JUNIPER NETWORKS

Security on the QFX Series

Release
13.2X52

Published: 2014-12-18

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

Security on the QFX Series
13.2X52

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- QFabric System

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

Table 1 on page xvii 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 xvii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

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

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

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

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

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

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

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Firewall Filters

Overview of Firewall Filters

Firewall filters provide rules that define whether to accept or discard packets that are transiting an interface. If a packet is accepted, you can configure additional actions to perform on the packet, such as class-of-service (CoS) marking (grouping similar types of traffic together and treating each type of traffic as a class with its own level of service priority) and traffic policing (controlling the maximum rate of traffic sent or received). You configure firewall filters to determine whether to accept or discard a packet before it enters or exits any of these:

- Port
- VLAN
- Layer 3 (routed) interface
- Routed VLAN interface (RVI)

An *ingress* firewall filter is applied to packets that are entering an interface or VLAN, and an *egress* firewall filter is applied to packets that are exiting an interface or VLAN.

NOTE: Firewall filters are sometimes called *access control lists* (ACLs).

Firewall Filter Types

The following firewall filter types are supported:

- Port (Layer 2) firewall filter—Port firewall filters apply to Layer 2 traffic transiting system ports.
- VLAN firewall filter—VLAN firewall filters provide access control for packets that enter a VLAN, are bridged within a VLAN, or leave a VLAN.
- Router (Layer 3) firewall filter—You can apply a router firewall filter in both ingress and egress directions on IPv4 or IPv6 Layer 3 (routed) interfaces, routed VLAN interfaces (RVI) and a loopback interface, which filters traffic sent to the switch itself or generated by the switch. (You apply a filter to a loopback interface in the input direction to protect the switch from unwanted traffic. You also might want to apply a filter to a loopback interface in the output direction so that you can set the forwarding class and DSCP bit value for packets that originate on the switch itself. This feature gives you very fine control over the classification of CPU generated packets. For example, you might want to assign different DSCP values and forwarding classes to traffic generated by different routing protocols so the traffic for those protocols can be treated in a differentiated manner by other devices. You can apply a filter to a loopback interface in the output direction starting with Junos OS 13.2X51-D15.)

  NOTE: You can apply a firewall filter to a management interface (for example, me0) on a QFX and EX4600 standalone switch. You cannot apply a firewall filter to a management interface on a QFX3000-G or QFX3000-M system.

- MPLS filter—You can apply a firewall filter to an MPLS interface

To apply a firewall filter:

1. Configure the firewall filter.
2. Apply the firewall filter to a port, VLAN, or router interface.

NOTE: You can apply only one firewall filter to a port, VLAN, or interface for a given direction. For example, for interface ge-0/0/6.0, you can apply one filter for the ingress direction and one for the egress direction.

Firewall Filter Components

In a firewall filter, you first define the family address type (ethernet-switching, inet (for IPv4), inet6 (for IPv6), or mpls) and then define one or more terms that specify the filtering criteria and the action to take if a match occurs.

Each term consists of the following components:

- Match conditions—Specify values that a packet must contain to be considered a match. You can specify values for most fields in the IP, TCP, UDP, or ICMP headers. You can also match on interface names.
- Action—Specifies what to do if a packet matches the match conditions. A filter can accept, discard, or reject a matching packet and then perform additional actions, such as counting, classifying, and policing. If no action is specified for a term, the default is to accept the matching packet.

Firewall Filter Processing

If there are multiple terms in a filter, the order of the terms is important. If a packet matches the first term, the switch executes the action defined by that term, and no other terms are evaluated. If the switch does not find a match between the packet and the first term, it compares the packet to the next term. If no match occurs between the packet and the second term, the system continues to compare the packet to each successive term in the filter until a match is found. If the packet does not match any terms in the filter, the switch discards the packet by default.

Related Documentation

- Understanding Firewall Filter Planning on page 27
- Understanding Firewall Filter Processing Points for Bridged and Routed Packets on page 32
- Understanding How Firewall Filters Are Evaluated on page 5
- Understanding Firewall Filter Match Conditions on page 8
- Overview of Policers on page 35
- Configuring Firewall Filters on page 121

Understanding How Firewall Filters Are Evaluated

A firewall filter consists of one or more terms, and the order of the terms within a filter is important. Before you configure firewall filters, you should understand how switches evaluate the terms within a filter and how packets are evaluated against the terms.

When a firewall filter consists of a single term, the filter is evaluated as follows:

- If the packet matches all the conditions, the action in the **then** statement is taken.
- If the packet matches all the conditions, and no action is specified in the **then** statement, the default action **accept** is taken.

- If the packet does not match all the conditions, the switch discards it.

When a firewall filter consists of more than one term, the filter is evaluated sequentially:

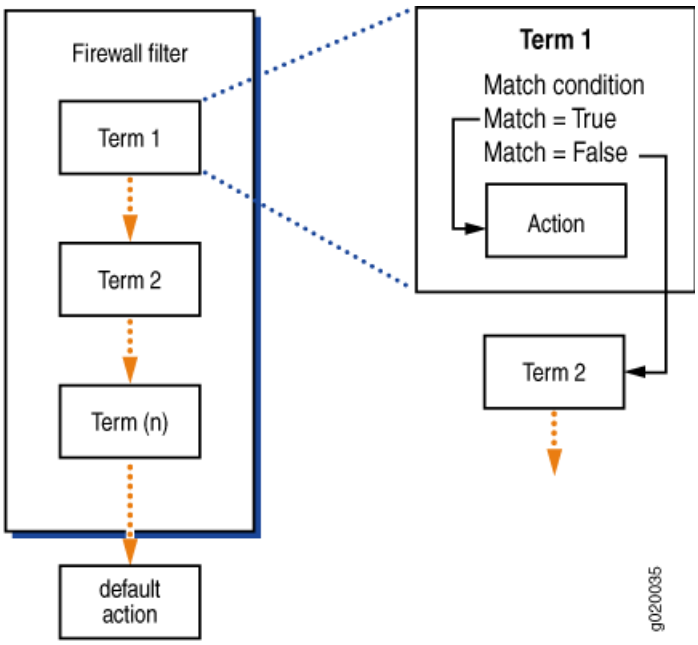
1. The packet is evaluated against the conditions in the **from** statement in the first term.
2. If the packet matches all the conditions in the term, the action in the **then** statement is taken and the evaluation ends. Subsequent terms in the filter are not evaluated.
3. If the packet does not match all the conditions in the term, the packet is evaluated against the conditions in the **from** statement in the second term.

   This process continues until the packet matches all the conditions in the **from** statement in one of the subsequent terms or there are no more terms in the filter.
4. If a packet passes through all the terms in the filter without a match, the switch discards it.

NOTE: **The order of conditions in a from statement is not important because a packet must match all the conditions to be considered a match.**

Figure 1 on page 6 shows how switches evaluate the terms within a firewall filter.

Figure 1: Evaluation of Terms Within a Firewall Filter



If you do not include a **from** statement in a term, all packets will match the term and be processed by the **then** statement. If a term does not contain a **then** statement or if an action has not been configured in the **then** statement, the term accepts any matching packets.

Every firewall filter contains an implicit **deny** statement at the end of the filter, which is equivalent to the following explicit filter term:

```
term implicit-rule {
  then discard;
}
```

Consequently, a packet that does not match any of the terms in a firewall filter is discarded. If you configure a filter that has no terms, all packets that pass through the filter are discarded.

NOTE: **Firewall filtering is supported on packets that are at least 64 bytes long.**

Related Documentation

- Overview of Firewall Filters on page 3
- Understanding Firewall Filter Match Conditions on page 8
- Overview of Policers on page 35
- Configuring Firewall Filters on page 121

Understanding How Firewall Filters Control Packet Flows

A switch supports firewall filters that allow you to control flows of data packets and local packets. *Data packets* transit a switch as they are forwarded from a source to a destination. *Local packets* are destined for or sent by a Routing Engine (they do not transit a switch). Local packets usually contain routing protocol data, data for IP services such as Telnet or SSH, or data for administrative protocols such as the Internet Control Message Protocol (ICMP).

Firewall filters affect packet flows entering into or exiting from a switch as follows:

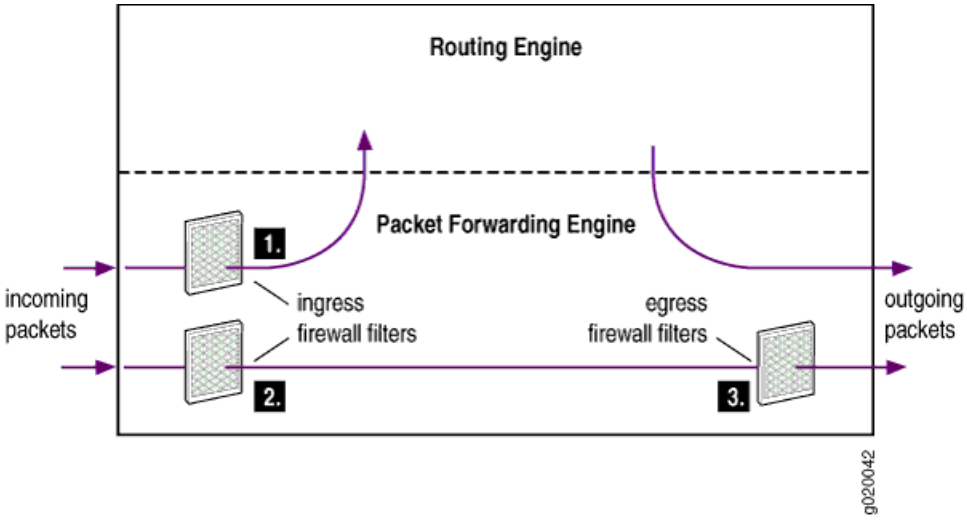
- Ingress firewall filters affect the flow of data packets that are received on switch interfaces. When a switch receives a data packet, the Packet Forwarding Engine in the system that contains the ingress interface determines where to forward the packet by looking in its Layer 2 or Layer 3 forwarding table for the best route to the destination. Data packets are forwarded to an egress interface. Locally destined packets are forwarded to the Routing Engine.
- Egress firewall filters affect data packets that are transiting a switch but do not affect packets sent by the Routing Engine. These filters are applied by the Packet Forwarding Engine in the system that contains the egress interface.

Figure 2 on page 8 illustrates the application of ingress and egress firewall filters to control the flow of packets through a switch:

1. Ingress firewall filter applied to locally destined packets that are received on switch interfaces and are destined for the Routing Engine.

2. Ingress firewall filter applied to data packets that are received on switch interfaces and will transit the switch.
3. Egress firewall filter applied to data packets that are transiting the switch.

Figure 2: Application of Firewall Filters to Control Packet Flow



Related Documentation

- Understanding Firewall Filter Processing Points for Bridged and Routed Packets on page 32
- Understanding How Firewall Filters Are Evaluated on page 5
- Configuring Firewall Filters on page 121

Understanding Firewall Filter Match Conditions

Before you define terms for firewall filters, you must understand how the conditions in a term are handled and how to specify interface, numeric, address, and bit-field filter match conditions to achieve the desired filter results.

- Filter Match Conditions on page 8
- Numeric Filter Match Conditions on page 9
- Interface Filter Match Conditions on page 9
- IP Address Filter Match Conditions on page 10
- MAC Address Filter Match Conditions on page 10
- Bit-Field Filter Match Conditions on page 11

Filter Match Conditions

In the **from** statement of a firewall filter term, you specify the conditions that the packet must match for the action in the **then** statement to be taken. All conditions must match for the action to be implemented. The order in which you specify match conditions is not important, because a packet must match all the conditions in a term for a match to occur.

If you specify multiple values for the same condition, a match on any one of those values matches that condition. For example, if you specify multiple IP source addresses using the **source-address** statement, a packet that contains any one of those IP source addresses matches the condition. In some cases you can specify multiple values for the same condition by enclosing the possible values in square brackets, as in:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set protocol (icmp | udp)
```

In other cases you must enter multiple statements, as in:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-address 10.1.1.1
user@switch# set source-address 10.1.1.2
```

If you specify no match conditions in a term, that term matches all packets.

NOTE: Unlike traditional Junos OS firewall filters, you cannot use except in a condition statement to negate the condition.

Numeric Filter Match Conditions

You can specify numeric filter match conditions that are identified by a numeric value, such as port and protocol numbers. For numeric filter match conditions, you specify the condition and a single value that a field in a packet must contain to be considered a match.

You can specify the numeric value in one of the following ways:

- Single number—A match occurs if the value of the field matches the number. For example, to match Telnet traffic:

  ```
  [edit firewall family family-name filter filter-name term term-name from]
  user@switch# set source-port 23
  ```

- Text synonym for a single number—A match occurs if the value of the field matches the number that corresponds to the synonym. For example, to match Telnet traffic:

  ```
  [edit firewall family family-name filter filter-name term term-name from]
  user@switch# set source-port telnet
  ```

- To specify multiple values for the same match condition in a filter term, enter each value in its own match statement. For example, a match occurs in the following term if the value of the source port in the packet is 22 or 23.

  ```
  [edit firewall family family-name filter filter-name term term-name from]
  user@switch# set source-port 22
  user@switch# set source-port 23
  ```

Interface Filter Match Conditions

You can specify an interface filter match condition to match an interface on which a packet is received or transmitted. For example, if you apply a filter to a VLAN you might want the filter to match on some interfaces that participate in the VLAN and not match

on other interfaces in the VLAN. When you specify the name of the interface, you must include a logical unit.

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/0/6.0
```

In this example, the final character (**0**) specifies the logical unit. You can include the wildcard (*****) as part of the interface name. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/*/6.0
user@switch# set interface ge-0/1/*.0
user@switch# set interface ge-0/0/6.*
```

Note that you must specify a value or a wildcard for the logical unit.

IP Address Filter Match Conditions

You can specify an address filter match condition to match an IP source or destination address or prefix in a packet. Specify the address or prefix type and the address or prefix itself. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-address 10.2.1.0/24;
```

If you omit the prefix length, it defaults to **/32**. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-address 10
[edit firewall family family-name filter filter-name term term-name from]
user@switch# show
destination-address {
10.0.0.0/32;
}
```

To specify more than one IP address or prefix in a filter term, enter each address or prefix in its own match statement. For example, a match occurs in the following term if the source address of a packet matches either of the following prefixes:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-address 10.1.0.0/16
user@switch# set source-address 10.2.0.0/16
```

MAC Address Filter Match Conditions

You can specify a MAC address filter match condition to match a source or destination MAC address. You specify the address type and value that a packet must contain to be considered a match.

You can specify the MAC address as six hexadecimal bytes in any of the following formats:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 00:11:22:33:44:55
```

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 0011.2233.4455
```

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 001122334455
```

Regardless of the formats you use, the system resolves the address to the standard format, in this case 00:11:22:33:44:55.

To specify more than one MAC address in a filter term, enter each MAC address in its own match statement. For example, a match occurs in the following term if the value of the MAC source address matches either of the following addresses:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-mac-address 00:11:22:33:44:55
user@switch# set source-mac-address 00:11:22:33:20:15
```

Bit-Field Filter Match Conditions

You can specify bit-field filter match conditions to match particular bits within certain fields in Ethernet frames and IP, TCP, UDP, and ICMP headers. You usually specify the field and the bit within the field that must be set in a packet to be considered a match.

In most cases you can use a keyword to specify the bit you want to match on. For example, to match on a TCP SYN packet you can enter **syn**, as in:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags syn
```

You can also enter **0x02** because the SYN bit is the third least-significant bit of the 8-bit tcp-flags field:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags 0x02
```

To match multiple bit-field values, use the logical operators, which are described in Table 3 on page 11. The operators are listed in order from highest precedence to lowest precedence. Operations are evaluated from left to right.

Table 3: Actions for Firewall Filters

Logical Operators	Description
!	Negation
&	Logical AND
|	Logical OR

If you use a logical operator, enclose the values in quotation marks and do not include any spaces. For example, the following statement matches the second packet of a TCP handshake:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "syn&ack"
```

To negate a match, precede the value with an exclamation point. For example, the following statement matches only the initial packet of a TCP handshake:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "syn&!ack"
```

You can use text synonyms to specify some common bit-field matches. For example, the following statement also matches the initial packet of a TCP handshake:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-initial
```

Related Documentation

- Overview of Firewall Filters on page 3
- Understanding How a Firewall Filter Tests a Protocol on page 26
- Firewall Filter Match Conditions and Actions on page 12
- Configuring Firewall Filters on page 121

Firewall Filter Match Conditions and Actions

Each term in a firewall filter consists of *match conditions* and an *action*. Match conditions are the fields and values that a packet must contain to be considered a match. You can define single or multiple match conditions in *match statements*. You can also include no match statement, in which case the term matches all packets.

When a packet matches a filter, a switch takes the action specified in the term. In addition, you can specify action modifiers to count, mirror, rate-limit, and classify packets. If no match conditions are specified for the term, the switch accepts the packet by default.

This topic describes the various match conditions, actions, and action modifiers that you can define in a firewall filter.

- Table 4 on page 12 describes the match conditions you can specify when configuring a firewall filter. Some of the numeric range and bit-field match conditions allow you to specify a text synonym. To see a list of all the synonyms for a match condition, type **?** at the appropriate place in a statement.
- Table 5 on page 23 shows the actions that you can specify in a term.
- Table 6 on page 24 shows the action modifiers you can use to count, mirror, rate-limit, and classify packets.

Table 4: Supported Match Conditions for Firewall Filters

Match Condition	Description	Direction and Interface
arp-type	ARP request packet or ARP reply packet.	Egress and ingress ports.
destination-address ***ip-address***	IP destination address field, which is the address of the final destination node.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.
destination-mac-address ***mac-address***	Destination media access control (MAC) address of the packet.	Ingress ports, VLANs and IPv4 (inet) interfaces. Egress ports and VLANs.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
destination-port *value*	TCP or UDP destination port field. Typically, you specify this match in conjunction with the **protocol** match statement. For the following well-known ports you can specify text synonyms (the port numbers are also listed): **afs (1483), bgp (179), biff (512), bootpc (68), bootps (67),** **cmd (514), cvspserver (2401),** **dhcp (67), domain (53),** **eklogin (2105), ekshell (2106), exec (512),** **finger (79), ftp (21), ftp-data (20),** **http (80), https (443),** **ident (113), imap (143),** **kerberos-sec (88), klogin (543), kpasswd (761), krb-prop (754), krbupdate (760), kshell (544),** **ldap (389), login (513),** **mobileip-agent (434), mobilip-mn (435), msdp (639),** **netbios-dgm (138), netbios-ns (137), netbios-ssn (139), nfsd (2049), nntp (119), ntalk (518), ntp (123),** **pop3 (110), pptp (1723), printer (515),** **radacct (1813),radius (1812), rip (520), rkinit (2108),** **smtp (25), snmp (161), snmptrap (162), snpp (444), socks (1080), ssh (22), sunrpc (111), syslog (514),** **tacacs-ds (65), talk (517), telnet (23), tftp (69), timed (525),** **who (513),** **xdmcp (177),** **zephyr-clt (2103), zephyr-hm (2104)**	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
destination-port range-optimize *range*	Match a range of TCP or UDP port ranges while using the available memory more efficiently. Using this condition allows you to configure more firewall filters than if you configure individual destination ports. (Not supported with filter-based forwarding.)	Egress and ingress IPv4 (inet) interfaces.
destination-prefix-list *prefix-list*	IP destination prefix list field. You can define a list of IP address prefixes under a prefix-list alias for frequent use. Define this list at the **[edit policy-options]** hierarchy level.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces and IPv6 (inet6) interfaces.
dot1q-tag *number*	802.1Q VLAN ID field in the Ethernet frame. The tag values can be 1–4094.	Ingress ports and VLANs. Egress ports and VLANs (*Number* must be the VLAN ID of the VLAN you want to match).
dot1q-user-priority *number*	802.1Q priority field in the Ethernet frame (used for class-of-service priorities). Values can be 0–7. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): • **best-effort (0)**—Best effort • **background (1)**—Background • **standard (2)**—Standard or spare • **excellent-load (3)**—Excellent load • **controlled-load (4)**—Controlled load • **video (5)**—Video • **voice (6)**—Voice • **network-control (7)**—Network control reserved traffic	Ingress ports and VLANs. Egress ports and VLANs.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
dscp *value*	Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most-significant 6 bits of this byte form the DSCP. You can specify DSCP in hexadecimal, binary, or decimal form. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): • **be**—best effort (default) • **ef (46)**—as defined in RFC 3246, *An Expedited Forwarding PHB*. • **af11 (10)**, **af12 (12)**, **af13 (14)**; **af21 (18)**, **af22 (20)**, **af23 (22)**; **af31 (26)**, **af32 (28)**, **af33 (30)**; **af41 (34)**, **af42 (36)**, **af43 (38)** These four classes, with three drop precedences in each class, for a total of 12 code points, are defined in RFC 2597, *Assured Forwarding PHB*. • **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **cs5**	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
ether-type ***value***	Ethernet type field of a packet. The EtherType value specifies what protocol is being transported in the Ethernet frame. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): • **aarp (0x80F3)**—EtherType value AARP • **appletalk (0x809B)**—EtherType value AppleTalk • **arp (0x0806)**—EtherType value ARP • **fcoe (0x8906)**—EtherType value FCoE • **fip (0x8914)**—EtherType value FIP • **ipv4 (0x0800)**—EtherType value IPv4 • **ipv6 (0x08DD)**—EtherType value IPv6 • **mpls-multicast (0x8848)**—EtherType value MPLS multicast • **mpls-unicast (0x8847)**—EtherType value MPLS unicast • **oam (0x88A8)**—EtherType value OAM • **ppp (0x880B)**—EtherType value PPP • **pppoe-discovery (0x8863)**—EtherType value PPPoE Discovery Stage • **pppoe-session (0x8864)**—EtherType value PPPoE Session Stage • **sna (0x80D5)**—EtherType value SNA	Ingress ports and VLANs. Egress ports and VLANs.
exp	Match on MPLS EXP bits.	Ingress MPLS interfaces. Egress MPLS interfaces.
fragment-flags ***value***	IP fragmentation flags. In place of the numeric value, you can specify one of the following text synonyms (the hexadecimal values are also listed): • **is-fragment** • **dont-fragment (0x4000)** • **more-fragments (0x2000)** • **reserved (0x8000)**	Ingress ports and VLANs.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
icmp-code *value*	ICMP code field. Because the meaning of the value depends upon the associated **icmp-type**, you must specify a value for **icmp-type** along with a value for **icmp-code**. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated: • *IPv4:* parameter-problem—**ip-header-bad (0)**, **required-option-missing (1)** • *IPv6:* parameter-problem—**ip6-header-bad (0)**, **unrecognized-next-header (1)**, **unrecognized-option (2)** • **redirect**—**redirect-for-network (0)**, **redirect-for-host (1)**, **redirect-for-tos-and-net (2)**, **redirect-for-tos-and-host (3)** • **time-exceeded**—**ttl-eq-zero-during-reassembly (1)**, **ttl-eq-zero-during-transit (0)** • *IPv4:* unreachable—**network-unreachable (0)**, **host-unreachable (1)**, **protocol-unreachable (2)**, **port-unreachable (3)**, **fragmentation-needed (4)**, **source-route-failed (5)**, **destination-network-unknown (6)**, **destination-host-unknown (7)**, **source-host-isolated (8)**, **destination-network-prohibited (9)**, **destination-host-prohibited (10)**, **network-unreachable-for-TOS (11)**, **host-unreachable-for-TOS (12)**, **communication-prohibited-by-filtering (13)**, **host-precedence-violation (14)**, **precedence-cutoff-in-effect (15)** • *IPv6:* unreachable—**address-unreachable (3)**, **administratively-prohibited (1)**, **no-route-to-destination (0)**, **port-unreachable (4)**	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
hop-limit*value*	Match the the specified hop limit or set of hop limits. Specify a single value or a range of values from 0 through 255.	Ingress and egress IPv6 (inet6) interfaces.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
icmp-type ***value***	ICMP message type field. Typically, you specify this match in conjunction with the **protocol** match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): *IPv4:* **echo-reply (0)**, **destination unreachable (3)**, **source-quench (4)**, **redirect (5)**, **echo-request (8)**, **IPv4 (inet)-advertisement (9)**, **IPv4 (inet)-solicit (10)**, **time-exceeded (11)**, **parameter-problem (12)**, **timestamp (13)**, **timestamp-reply (14)**, **info-request (15)**, **info-reply (16)**, **mask-request (17)**, **mask-reply (18)** *IPv6:* **destination-unreachable (1)**, **packet-too-big (2)**, **time-exceeded (3)**, **parameter-problem (4)**, **echo-request (128)**, **echo-reply (129)**, **membership-query (130)**, **membership-report (131)**, **membership-termination (132)**, **router-solicit (133)**, **router-advertisement (134)**, **neighbor-solicit (135)**, **neighbor-advertisement (136)**, **redirect (137)**, **router-renumbering (138)**, **node-information-request (139)**, **node-information-reply (140)** See also **icmp-code** ***variable***.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
interface ***interface-name***	Interface on which the packet is received, including the logical unit. You can include the wildcard character (*) as part of an interface name or logical unit. NOTE: An interface from which a packet is sent cannot be used as a match condition.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces and IPv6 (inet6) interfaces.
ip-destination-address *address*	IPv4 address that is the final destination node address for the packet.	Ingress ports and VLANs.
ip6-destination-address *address*	IPv6 address that is the final destination node address for the packet.	Ingress ports and VLANs. (You cannot simultaneously apply a filter with this match criterion to a Layer 2 port and VLAN that includes that port.)
ip-options	Specify **any** to create a match if anything is specified in the options field in the IP header.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
ip-precedence *ip-precedence-field*	IP precedence field. In place of the numeric field value, you can specify one of the following text synonyms (the field values are also listed): **critical-ecp** (0xa0), **flash** (0x60), **flash-override** (0x80), **immediate** (0x40), **internet-control** (0xc0), **net-control** (0xe0), **priority** (0x20), or **routine** (0x00).	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
ip-protocol *number*	IP protocol field.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
ip-source-address *address*	IPv4 address of the source node sending the packet.	Ingress ports and VLANs.
ip6-source-address *address*	IPv6 address of the source node sending the packet.	Ingress ports and VLANs. (You cannot simultaneously apply a filter with this match criterion to a Layer 2 port and VLAN that includes that port.)
ip-version *address*	IP version of the packet. Use this condition to match IPv4 or IPv6 header fields in traffic that arrives on a Layer 2 port or VLAN interface.	Ingress ports and VLANs.
is-fragment	Using this condition causes a match if the More Fragments flag is enabled in the IP header or if the fragment offset is not zero.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
l2-encap-type llc-non-snap	Match on logical link control (LLC) layer packets for non-Subnet Access Protocol (SNAP) Ethernet Encapsulation type.	Ingress ports and VLANs. Egress ports and VLANs.
label	Match on MPLS label bits.	Ingress MPLS interfaces. Egress MPLS interfaces.
learn-vlan-id *number*	VLAN identifier used for MAC learning.	Ingress ports and VLANs. Egress ports and VLANs.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
next-header	IPv4 or IPv6 protocol value. In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed): **hop-by-hop (0)**,**icmp (1)**, **icmp6 (58)**, **igmp (2)**, **ipip (4)**, **tcp (6)**, **egp (8)**, **udp (17)**, **ipv6 (41)**, **routing (43)**, **fragment (44)**,**rsvp (46)**, **gre (47)**, **esp (50)**, **ah (51)**, **icmp6 (58)**, **no-next-header (59)**, **dstopts (60)**, **ospf (89)**, **pim (103)**, **vrrp (112)**, **sctp (132)**	Ingress ports, VLANs, and IPv6 (inet6) interfaces. Egress IPv6 (inet6) interfaces.
packet-length	Packet length in bytes. You must enter a value between 0 and 65535.	Ingress ports, VLANs, IPv4 (inet), and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
payload-protocol	IPv4 or IPv6 protocol value. In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed): **hop-by-hop (0)**,**icmp (1)**, **icmp6 (58)**, **igmp (2)**, **ipip (4)**, **tcp (6)**, **egp (8)**, **udp (17)**, **ipv6 (41)**, **routing (43)**, **fragment (44)**,**rsvp (46)**, **gre (47)**, **esp (50)**, **ah (51)**, **icmp6 (58)**, **no-next-header (59)**, **dstopts (60)**, **ospf (89)**, **pim (103)**, **vrrp (112)**, **sctp (132)**	Ingress ports, VLANs, and IPv6 (inet6) interfaces. Egress IPv6 (inet6) interfaces.
precedence *value*	IP precedence bits in the type-of-service (ToS) byte in the IP header. (This byte can also used for the DiffServ DSCP.) In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed): • **routine (0)** • **priority (1)** • **immediate (2)** • **flash (3)** • **flash-override (4)** • **critical-ecp (5)** • **internet-control (6)** • **net-control (7)**	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
protocol *type*	IPv4 or IPv6 protocol value. In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed): **hop-by-hop (0)**,**icmp (1)**, **icmp6**, **igmp (2)**, **ipip (4)**, **tcp (6)**, **egp (8)**, **udp (17)**, **ipv6 (41)**, **routing (43)**, **fragment (44)**,**rsvp (46)**, **gre (47)**, **esp (50)**, **ah (51)**, **icmp6 (58)**, **no-next-header (59)**, **dstopts (60)**, **ospf (89)**, **pim (103)**, **vrrp (112)**, **sctp (132)**	Ingress ports, VLANs and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
rat-type *tech-type-value*	Match the radio-access technology (RAT) type specified in the 8-bit Tech-Type field of Proxy Mobile IPv4 (PMIPv4) access technology type extension. The technology type specifies the access technology through which the mobile device is connected to the access network. Specify a single value, a range of values, or a set of values. You can specify a technology type as a numeric value from 0 through 255 or as a system keyword. • Numeric value 1 matches IEEE 802.3. • Numeric value 2 matches IEEE 802.11a/b/g. • Numeric value 3 matches IEEE 802.16e • Numeric value 4 matches IEEE 802.16m. • Text string **eutran** matches 4G. • Text string **geran** matches 2G. • Text string **utran** matches 3G. •	Egress and ingress IPv4 (inet) interfaces.
sample	Sample the packet traffic. Apply this option only if you have enabled traffic sampling.	Egress and ingress IPv4 (inet) interfaces.
source-address *ip-address*	IP source address field, which is the address of the node that sent the packet.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
source-mac-address *mac-address*	Source media access control (MAC) address of the packet.	Ingress ports and VLANs. Egress ports and VLANs.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
source-port *value*	TCP or UDP source port. Typically, you specify this match in conjunction with the **protocol** match statement. In place of the numeric field, you can specify one of the text synonyms listed under **destination-port**.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
source-port range-optimize *range*	Match a range of TCP or UDP port ranges while using the available memory more efficiently. Using this condition allows you to configure more firewall filters than if you configure individual source ports. (Not supported with filter-based forwarding.)	Egress and ingress IPv4 (inet) interfaces.
source-prefix-list *prefix-list*	IP source prefix list. You can define a list of IP address prefixes under a prefix-list alias for frequent use. Define this list at the **[edit policy-options]** hierarchy level.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
tcp-established	Match packets of an established TCP connection. This condition matches packets other than those used to set up a TCP connection—that is, three-way handshake packets are not matched. When you specify **tcp-established**, a switch does not implicitly verify that the protocol is TCP. You must also specify the **protocol tcp** match condition.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
tcp-flags *value*	One or more TCP flags: • **ack (0x10)** • **fin (0x01)** • **push (0x08)** • **rst (0x04)** • **syn (0x02)** • **urgent (0x20)**	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
tcp-initial	Match the first TCP packet of a connection. A match occurs when the TCP flag **SYN** is set and the TCP flag **ACK** is not set. When you specify **tcp-initial**, a switch does not implicitly verify that the protocol is TCP. You must also specify the **protocol tcp** match condition.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.

Table 4: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
traffic-class	8-bit field that specifies the class-of-service (CoS) priority of the packet. The traffic-class field is used to specify a DiffServ code point (DSCP) value. This field was previously used as the type-of-service (ToS) field in IPv4, and, the semantics of this field (for example, DSCP) are identical to those of IPv4. You can specify one of the following text synonyms (the field values are also listed): **af11 (10)**, **af12 (12)**, **af13 (14)**, **af21 (18)**, **af22 (20)**, **af23 (22)**, **af31 (26)**, **af32 (28)**, **af33 (30)**, **af41 (34)**, **af42 (36)**, **af43 (38)**, **cs0 (0)**, **cs1 (8)**, **cs2 (16)**, **cs3 (24)**, **cs4 (32)**, **cs5 (40)**, **cs6 (48)**, **cs7 (56)**, **ef (46)**	Ingress ports, VLANs, and IPv6 (inet6) interfaces. Egress IPv6 (inet6) interfaces.
ttl *value*	IP Time-to-live (TTL) field in decimal. The value can be 1-255.	Ingress IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
user-vlan-1p-priority *value*	Match on the IEEE 802.1p user priority bits in the customer VLAN tag (the inner tag in a dual-tag frame with 802.1Q VLAN tags). Specify a single value or multiple values from 0 through 7.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
user-vlan-id *number*	Match the first VLAN identifier that is part of the payload.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
vlan (*vlan-name* **|** *vlan-id* **)**	VLAN names or ID.	Ingress ports and VLANs. Egress ports and VLANs.

Use **then** statements to define actions that should occur if a packet matches all conditions in a **from** statement. Table 5 on page 23 shows the actions that you can specify in a term. (If you do not include a **then** statement, the system accepts packets that match the filter.)

Table 5: Actions for Firewall Filters

Action	Description
accept	Accept a packet. This is the default action for packets that match a term.
discard	Discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.

Table 5: Actions for Firewall Filters *(continued)*

Action	Description
reject ***message-type***	Discard a packet and send a "destination unreachable" ICMPv4 message (type 3). To log rejected packets, configure the **syslog** action modifier. You can specify one of the following message types: **administratively-prohibited (default), bad-host-tos, bad-network-tos, host-prohibited, host-unknown, host-unreachable, network-prohibited, network-unknown, network-unreachable, port-unreachable, precedence-cutoff, precedence-violation, protocol-unreachable, source-host-isolated, source-route-failed,** or **tcp-reset**. If you specify **tcp-reset**, the system sends a TCP reset if the packet is a TCP packet; otherwise nothing is sent. If you do not specify a message type, the ICMP notification "destination unreachable" is sent with the default message "communication administratively filtered." NOTE: The **reject** action is supported on ingress interfaces only.
routing-instance *instance-name*	Forward matched packets to a virtual routing instance.
vlan *VLAN-name*	Forward matched packets to a specific VLAN. NOTE: The **vlan** action is supported on ingress interfaces only.

You can also specify the action modifiers listed in Table 6 on page 24 to count, mirror, rate-limit, and classify packets.

Table 6: Action Modifiers for Firewall Filters

Action Modifier	Description
analyzer ***analyzer-name***	(Non-ELS platforms) Mirror traffic (copy packets) to an analyzer configured at the **[edit ethernet-switching-options analyzer]** hierarchy level. You can specify port mirroring for ingress port, VLAN, and IPv4 (inet) firewall filters only.
count ***counter-name***	Count the number of packets that match the term.
decapsulate [gre | ***routing-instance*****]**	De-encapsulate GRE packets or forward de-encapsulated GRE packets to the specified routing instance

Table 6: Action Modifiers for Firewall Filters *(continued)*

Action Modifier	Description
dscp *value*	Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most-significant 6 bits of this byte form the DSCP. You can specify DSCP in hexadecimal, binary, or decimal form. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): • **be**—best effort (default) • **ef (46)**—as defined in RFC 3246, *An Expedited Forwarding PHB*. • **af11 (10)**, **af12 (12)**, **af13 (14)**; **af21 (18)**, **af22 (20)**, **af23 (22)**; **af31 (26)**, **af32 (28)**, **af33 (30)**; **af41 (34)**, **af42 (36)**, **af43 (38)** These four classes, with three drop precedences in each class, for a total of 12 code points, are defined in RFC 2597, *Assured Forwarding PHB*. • **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **cs5**
forwarding-class *class*	Classify the packet in one of the following forwarding classes: • **best-effort** • **fcoe** • **mcast** • **network-control** • **no-loss** NOTE: To configure a forwarding class, you must also configure loss priority.
log	Log the packet's header information in the Routing Engine. To view this information, enter the **show firewall log** operational mode command. NOTE: The **log** action modifier is supported on ingress interfaces only.
loss-priority (low | medium-low | medium-high | high)	Set the packet loss priority (PLP). NOTE: The **loss-priority** action modifier is supported on ingress interfaces only. NOTE: The **loss-priority** action modifier is not supported in combination with the **policer** action.
policer *policer-name*	Send packets to a policer (for the purpose of applying rate limiting). You can specify a policer for ingress port, VLAN, IPv4 (inet), IPv6 (inet6), and MPLS filters. NOTE: The **policer** action modifier is not supported in combination with the **loss-priority** action.

Table 6: Action Modifiers for Firewall Filters *(continued)*

Action Modifier	Description
port-mirror	(ELS platforms) Mirror traffic (copy packets) to an output interface configured in a port-mirroring instance at the **[edit forwarding-options port-mirroring]** hierarchy level. You can specify port mirroring for ingress port, VLAN, and IPv4 (inet) firewall filters only.
port-mirror-instance *port-mirror-instance-name*	(ELS platforms) Mirror traffic to a port-mirroring instance configured at the **[edit forwarding-options port-mirroring]** hierarchy level. You can specify port mirroring for ingress port, VLAN, and IPv4 (inet) firewall filters only.
syslog	Log an alert for this packet. NOTE: The **syslog** action modifier is supported on ingress interfaces only.
three-color-policer *three-color-policer-name*	Send packets to a three-color policer (for the purpose of applying rate limiting). You can specify a three-color policer for ingress and egress port, VLAN, IPv4 (inet), IPv6 (inet6), and MPLS filters. NOTE: The **policer** action modifier is not supported in combination with the **loss-priority** action.

Related Documentation

- Understanding Firewall Filter Match Conditions on page 8
- Understanding How Firewall Filters Are Evaluated on page 5
- Understanding How a Firewall Filter Tests a Protocol on page 26
- Overview of Policers on page 35
- *Understanding Port Mirroring*
- Configuring Firewall Filters on page 121

Understanding How a Firewall Filter Tests a Protocol

When examining match conditions in a firewall filter, a switch tests only the fields that you specify. It does not implicitly test any fields that you do not explicitly configure. For example, if you specify a match condition of **source-port ssh**, there is no implied test to determine if the protocol is TCP. In this case, the switch considers any packet that has a value of **22** (decimal) in the 2-byte field that follows a *presumed* IP header to be a match. To ensure that the term matches on TCP packets, you also specify a **protocol tcp** match condition.

For the following match conditions, you should explicitly specify the protocol match condition in the same term:

- **destination-port**—Specify **protocol tcp** or **protocol udp**.
- **icmp-code**—Specify **protocol icmp** and **icmp-type**.
- **icmp-type**—Specify **protocol tcp** or **protocol udp**.
- **source-port**—Specify **protocol tcp** or **protocol udp**.
- **tcp-flags**—Specify **protocol tcp**.

Related Documentation

- Overview of Firewall Filters on page 3
- Understanding Firewall Filter Match Conditions on page 8
- Configuring Firewall Filters on page 121

Understanding Firewall Filter Planning

Before you create a firewall filter and apply it, determine what you want the filter to accomplish and how to use its match conditions and actions to achieve your goals. It is important that you understand how packets are matched, the default and configured actions of the firewall filter, and where to apply the firewall filter.

You can apply no more than one firewall filter per port, VLAN, or router interface per direction (input and output). For example, for a given port you can apply at most one filter in the input direction and one filter in the output direction. You should try to be conservative in the number of terms (rules) that you include in each firewall filter, because a large number of terms requires longer processing time during a commit operation and can make testing and troubleshooting more difficult.

Before you configure and apply firewall filters, answer the following questions for each of them:

1. What is the purpose of the filter?

   For example, the system can drop packets based on header information, rate-limit traffic, classify packets into forwarding classes, log and count packets, or prevent denial-of-service attacks.

2. What are the appropriate match conditions? Determine the packet header fields that the packet must contain for a match. Possible fields include:

   - Layer 2 header fields—Source and destination MAC addresses, 802.1Q tag, Ethernet type, or VLAN.
   - Layer 3 header fields—Source and destination IP addresses, protocols, and IP options (IP precedence, IP fragmentation flags, or TTL type).
   - TCP header fields—Source and destination ports and flags.
   - ICMP header fields—Packet type and code.

3. What are the appropriate actions to take if a match occurs?

   The system can accept, discard, or reject packets.

4. What additional action modifiers might be required?

   For example, you can configure the system to mirror (copy) packets to a specified port, count matching packets, apply traffic management, or police packets.

5. On what port, router interface, or VLAN should the firewall filter be applied?

   Start with the following basic guidelines:

   - If packets entering or leaving a Layer 2 interface (port) need to be filtered, apply the filter at the **[edit family ethernet switching filter]** hierarchy level. This is a port filter.
   - If packets entering or leaving any port in a specific VLAN need to be filtered, use a VLAN filter.
   - If packets entering or leaving a Layer 3 (routed) interface or routed VLAN interface (RVI) need to be filtered, use a router firewall filter. Apply the filter to the interface at the **[edit family inet]** hierarchy level. You can also apply a router firewall filter on a loopback interface.

   Before you choose the interface or VLAN on which to apply a firewall filter, understand how that placement can affect traffic flow to other interfaces. In general, apply a filter close to the source device if the filter matches on source or destination IP addresses, IP protocols, or protocol information—such as ICMP message types, and TCP or UDP port numbers. However, you should apply a filter close to the destination device if the filter matches *only* on a source IP address. When you apply a filter too close to the source device, the filter could prevent that source device from accessing other services that are available on the network.

   NOTE: **Egress firewall filters do not affect the flow of locally generated control packets from the Routing Engine.**

6. In which direction should the firewall filter be applied?

   You typically configure different actions for traffic entering an interface than you configure for traffic exiting an interface.

7. How many filters should I create?

   See "Planning the Number of Firewall Filters to Create" on page 29 for information about how many firewall filters you can apply.

Related Documentation

- Overview of Firewall Filters on page 3
- Overview of Policers on page 35
- Understanding How Firewall Filters Are Evaluated on page 5
- Planning the Number of Firewall Filters to Create on page 29
- Configuring Firewall Filters on page 121

Planning the Number of Firewall Filters to Create

Understanding How Many Firewall Filters Are Supported

QFX3500, QFX3600, QFX5100, and EX4600 switches, QFabric Node devices, and VCF members support the maximum numbers of firewall filter terms per type of attachment point shown in Table 7 on page 29.

Table 7: Supported Firewall Filter Numbers

Filter Type	QFX3500, QFX3600	QFX5100, EX4600
Ingress	768	1536
Egress	1024	1024

These totals are applied in aggregate. For example, on the QFX3500 and QFX3600 you can apply a total of 768 terms in all your port filters, Layer 3 filters, and VLAN filters that are applied in the input direction and 1024 terms in port filters, Layer 3 filters, and VLAN filters that are applied in the output direction.

NOTE: If you want to create more than 512 egress VLAN filters, your first VLAN ID should be 6 and the subsequent VLAN IDs should increase by 1. For example, to create 1024 egress VLAN filters, the first VLAN ID would be 6, the second ID would be 7, and the sequence would continue through VLAN ID 1029. Similarly, if you want to create fewer than 512 egress VLAN filters but want the total number of terms in those filters to exceed 512, you should number your VLAN IDs in the same manner. If you do not use this approach to create your VLAN IDs, the total number of allowed terms or filters will be less than 1024 and might be 512.

The ternary content addressable memory (TCAM) for firewall filters is divided into slices that accommodate 256 terms, and all the terms in a memory slice must be in filters of the same type and applied in the same direction. A memory slice is reserved as soon as you commit a filter. For example, if you create a port filter and apply it in the input direction, a memory slice is reserved that will only store ingress port filters. If you create and apply only one ingress port filter and that filter has only one term, the rest of this slice is unused and is unavailable for other filter types.

Continuing with the above example, assume that you create and apply 256 ingress port filters with one term each so that one memory slice is filled. This leaves two more memory slices available for ingress filters. (Remember that the maximum number of ingress terms is 768.) If you then create and apply an ingress Layer 3 filter with one term, another memory slice is reserved for ingress Layer 3 filters. As before, the rest of the slice is unused and is unavailable for different filter types. At this point there is one memory slice available for any ingress filter type.

Now assume that you create and apply a VLAN ingress filter. The final memory slice is reserved for VLAN ingress filters. Memory allocation for ingress filters (once again assuming one term per filter) is as follows:

- Slice 1: Filled with 256 ingress port filters. You cannot commit any more ingress port filters.
- Slice 2: Contains one ingress Layer 3 filter with one term. You can commit 255 more terms in ingress Layer 3 filters.
- Slice 3: Contains one ingress VLAN filter with one term. You can commit 255 more terms in ingress VLAN filters.

Here is another example. Assume that you create 257 ingress port filters with one term per filter—that is, you create one more term than a single memory slice can accommodate. When you apply the filters and commit the configuration, the filter memory allocation is:

- Slice 1: Filled with 256 ingress port filters. You cannot apply any more ingress port filters.
- Slice 2: Contains one ingress port filter. You can apply 255 more terms in ingress port filters.
- Slice 3: This slice is unassigned. You can create and apply 256 terms in ingress filters of any type (port, Layer 3, or VLAN), but all the filters must be of the same type.

Egress Filters

All of the preceding principles also apply to egress filters, but four memory slices are used because IPv4 Layer 3 filters and IPv6 Layer 3 filters are stored in separate slices. The memory slices for egress filters are the same size as those for ingress filters, so the maximum number of egress filter terms is therefore 1024.

Avoid Configuring too Many Filters

If you violate any of these restrictions and commit a configuration that is not in compliance, Junos OS rejects the excessive filters. For example, if you configure 300 ingress port filters and 300 ingress Layer 3 filters and try to commit the configuration, Junos OS does the following (again assuming one term per filter):

- Accepts the 300 ingress port filters (storing them in two memory slices).
- Accepts the first 256 ingress Layer 3 filters it processes (storing them in the third memory slice).
- Rejects the remaining 44 ingress Layer 3 filters.

NOTE: In this situation, be sure to delete excessive filters (for example, the remaining 44 ingress Layer 3 filters) from the configuration before you reboot the device. If you reboot a device that has a noncompliant configuration, you cannot predict which filters are installed after the reboot. Using the example above, the 44 ingress Layer 3 filters that were originally rejected might be installed, and 44 of the port filters that were originally accepted might be rejected.

Policers can Limit Egress Filters

The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters.

Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms, 1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.
- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
  - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
  - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

You can prevent this problem from occurring by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.
- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.

Planning for Filter-Specific Policers

You can configure policers to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps. However, the behavior of a filter-specific policer is affected by how the firewall filter terms that reference the policer are stored in ternary content addressable memory (TCAM). If you create a filter-specific policer and reference it in multiple firewall filter terms, the policer allows more traffic than expected if the terms are stored in different TCAM slices. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms that are stored in three separate memory slices, the total bandwidth allowed by the filter is 3 Gbps, not 1 Gbps.

To prevent this unexpected behavior from occurring, use the information about TCAM slices presented above to organize your configuration file so that all the firewall filter terms that reference a given filter-specific policer are stored in the same TCAM slice.

Planning for Filter-Based Forwarding

You can use firewall filters in conjunction with virtual routing instances to specify different routes for packets to travel in their networks. To set up this feature—called filter-based forwarding—you specify a filter and match criteria and then specify the virtual routing instance to send packets to. Filters used in this way also consume memory in an additional TCAM. See *Understanding FIP Snooping, FBF, and MVR Filter Scalability* for more information. The section *FBF Filter VFP TCAM Consumption* in this topic specifically addresses the number of supported filters when using filter-based forwarding.

Related Documentation

- Overview of Firewall Filters on page 3
- Understanding How Firewall Filters Are Evaluated on page 5
- Understanding Firewall Filter Planning on page 27
- Configuring Firewall Filters on page 121
- *Understanding Filter-Based Forwarding*

Understanding Firewall Filter Processing Points for Bridged and Routed Packets

You apply firewall filters at multiple processing points in the forwarding path. At each processing point, the action to be taken on a packet is determined by the configuration of the filter and the results of the lookup in the forwarding or routing table.

For both bridged (Layer 2) unicast packets and routed (Layer 3) unicast packets, firewall filters are applied in the prescribed order shown below (assuming that each filter is present and a packet is accepted by each one).

Bridged packets:

1. Ingress port filter
2. Ingress VLAN filter
3. Egress VLAN filter
4. Egress port filter

Routed packets:

1. Ingress port firewall filter
2. Ingress VLAN firewall filter (Layer 2 CoS)
3. Ingress router firewall filter (Layer 3 CoS)
4. Egress router firewall filter
5. Egress VLAN firewall filter
6. Egress port filter

NOTE: MAC learning occurs before filters are applied, so switcheslearn the MAC addresses of packets that are dropped by ingress filters.

Related Documentation

- Overview of Firewall Filters on page 3
- Understanding How Firewall Filters Control Packet Flows on page 7
- Configuring Firewall Filters on page 121

Applying Firewall Filters to Interfaces

For a firewall filter to work, you must apply it to at least one interface. To do this, include the **filter** statement when configuring a logical interface at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
user@switch# set interface-name unit logical-unit-number family family-name filter (input | output) filter-name
```

In the **input** statement, specify a firewall filter to be evaluated when packets are received on the interface. Input filters applied to a loopback interface affect only traffic destined for the Routing Engine.

In the **output** statement, specify a filter to be evaluated when packets exit the interface.

NOTE: When you create a loopback interface, it is important to apply an ingress filter to it so the Routing Engine is protected. We recommend that when you apply a filter to the loopback interface lo0, you include the apply-groups statement. Doing so ensures that the filter is automatically inherited on every loopback interface, including lo0 and other loopback interfaces.

Related Documentation

- Configuring Firewall Filters on page 121

CHAPTER 2

Policers

Overview of Policers

A switch polices traffic by limiting the input or output transmission rate of a class of traffic according to user-defined criteria. Policing (or rate-limiting) traffic allows you to control the maximum rate of traffic sent or received on an interface and to provide multiple priority levels or classes of service.

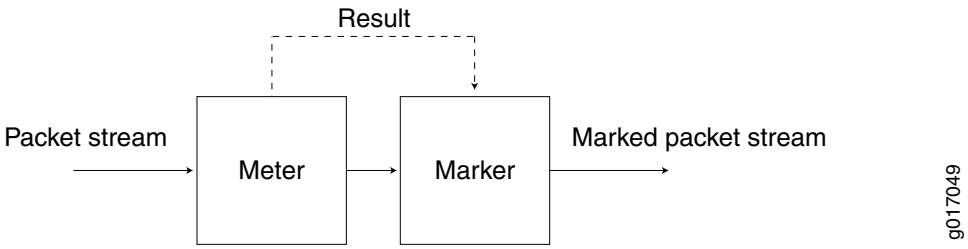
Policer Overview

You use policers to apply limits to traffic flow and set consequences for packets that exceed these limits—usually applying a higher loss priority—so that if packets encounter downstream congestion, they can be discarded first. Policers apply only to unicast packets.

Policers provide two functions: metering and marking. A policer meters (measures) each packet against traffic rates and burst sizes that you configure. It then passes the packet

and the metering result to the marker, which assigns a packet loss priority that corresponds to the metering result. Figure 3 on page 36 illustrates this process.

Figure 3: Flow of Tricolor Marking Policer Operation



After you name and configure a policer, you use it by specifying it as an action in one or more firewall filters.

Policer Types

A switch supports three types of policers:

- Single-rate two-color marker—A two-color policer (or "policer" when used without qualification) meters the traffic stream and classifies packets into two categories of packet loss priority (PLP) according to a configured bandwidth and burst-size limit. You can mark packets that exceed the bandwidth and burst-size limit with a specified PLP or simply discard them.

  You can specify this type of policer in an ingress or egress firewall.

  NOTE: **A two-color policer is most useful for metering traffic at the port (physical interface) level.**

- Single-rate three-color marker—This type of policer is defined in RFC 2697, *A Single Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on one rate—the configured committed information rate (CIR) as well as the committed burst size (CBS) and the excess burst size (EBS). The CIR specifies the average rate at which bits are admitted to the switch. The CBS specifies the usual burst size in bytes and the EBS specifies the maximum burst size in bytes. The EBS must be greater than or equal to the CBS, and neither can be 0.

  You can specify this type of policer in an ingress or egress firewall.

  NOTE: **A single-rate three-color marker (TCM) is most useful when a service is structured according to packet length and not peak arrival rate.**

- Two-rate three-color marker—This type of policer is defined in RFC 2698, *A Two Rate Three Color Marker*, as part of an assured forwarding per-hop-behavior classification system for a Differentiated Services environment. This type of policer meters traffic based on two rates—the CIR and peak information rate (PIR) along with their associated burst sizes, the CBS and peak burst size (PBS). The PIR specifies the maximum rate

at which bits are admitted to the network and must be greater than or equal to the CIR.

You can specify this type of policer in an ingress or egress firewall.

NOTE: A two-rate three-color policer is most useful when a service is structured according to arrival rates and not necessarily packet length.

See Table 8 on page 37 for information about how metering results are applied for each of these policer types.

Policer Actions

Policer actions are implicit or explicit and vary by policer type. *Implicit* means that Junos OS assigns the loss priority automatically. Table 8 on page 37 describes the policer actions.

Table 8: Policer Actions

Policer	Marking	Implicit Action	Configurable Action
Single-rate two-color	Green (conforming)	Assign low loss priority	None
	Red (nonconforming)	None	Discard
Single-rate three-color	Green (conforming)	Assign low loss priority	None
	Yellow (above the CIR and CBS)	Assign medium-high loss priority	None
	Red (above the EBS)	Assign high loss priority	Discard
Two-rate three-color	Green (conforming)	Assign low loss priority	None
	Yellow (above the CIR and CBS)	Assign medium-high loss priority	None
	Red (above the PIR and PBS)	Assign high loss priority	Discard

NOTE: If you specify a policer in an egress firewall filter, the only supported action is discard.

Policer Colors

Single-rate and two-rate three-color policers can operate in two modes:

- Color-blind—In color-blind mode, the three-color policer assumes that all packets examined have not been previously marked or metered. In other words, the three-color policer is "blind" to any previous coloring a packet might have had.
- Color-aware—In color-aware mode, the three-color policer assumes that all packets examined have been previously marked or metered. In other words, the three-color policer is "aware" of the previous coloring a packet might have had. In color-aware mode, the three-color policer can increase the PLP of a packet but cannot decrease it. For example, if a color-aware three-color policer meters a packet with a medium PLP marking, it can raise the PLP level to high but cannot reduce the PLP level to low.

Filter-Specific Policers

You can configure policers to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps. However, the behavior of a filter-specific policer is affected by how the firewall filter terms that reference the policer are stored in TCAM. If you create a filter-specific policer and reference it in multiple firewall filter terms, the policer allows more traffic than expected if the terms are stored in different TCAM slices. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms that are stored in three separate memory slices, the total bandwidth allowed by the filter is 3 Gbps, not 1 Gbps.

To prevent this unexpected behavior from occurring, use the information about TCAM slices presented in "Planning the Number of Firewall Filters to Create" on page 29 to organize your configuration file so that all the firewall filter terms that reference a given filter-specific policer are stored in the same TCAM slice.

Suggested Naming Convention for Policers

We recommend that you use the naming convention ***policertypeTCM#-color type*** when configuring three-color policers and ***policer#*** when configuring two-color policers. TCM stands for three-color marker. Because policers can be numerous and must be applied correctly to work, a simple naming convention makes it easier to apply the policers properly. For example, the first single-rate, color-aware three-color policer configured would be named **srTCM1-ca**. The second two-rate, color-blind three-color configured would be named **trTCM2-cb**. The elements of this naming convention are explained below:

- sr (single-rate)
- tr (two-rate)
- TCM (tricolor marking)
- 1 or 2 (number of marker)

- ca (color-aware)
- cb (color-blind)

Policer Counters

Each policer that you configure includes an implicit counter that counts the number of packets that exceed the rate limits that are specified for the policer. If you use the same policer in multiple terms—either within the same filter or in different filters—the implicit counter counts all the packets that are policed in all of these terms. If you want to obtain separate packet counts for each term, use these options:

- Configure a unique policer for each term.
- Configure only one policer, but use a unique, explicit counter in each term.

Policer Algorithms

Policing uses the *token-bucket algorithm*, which enforces a limit on average bandwidth while allowing bursts up to a specified maximum value. It offers more flexibility than the *leaky bucket algorithm* in allowing a certain amount of bursty traffic before it starts discarding packets.

How Many Policers are Supported?

You can configure and commit the following numbers of policers on QFX3500 and QFX3600 devices when they are operating as standalone switches:

- Two-color policers used in ingress firewall filters: 767
- Three-color policers used in ingress firewall filters: 767
- Two-color policers used in egress firewall filters: 1022
- Three-color policers used in egress firewall filters: 512

Policers can Limit Egress Firewall Filters

The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters.

Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms,

1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.

- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
  - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
  - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

You can prevent this problem by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.
- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.

Related Documentation

- Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 41
- Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 43
- Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 41
- Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 43
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128

Understanding Policers with Link Aggregation Groups

If you apply a policer to a link aggregation group (LAG) on a QFX3500 switch or node, the policer applies to all the interfaces in the LAG in aggregate. For example, if you configure a policer to rate-limit at 1 Gbps and apply the policer (by using a firewall filter) to a LAG that has two member interfaces on a single switch or node, the total allowed throughput for both members is 1 Gbps.

If you apply a policer to a LAG that has members on different nodes in a QFabric network Node group or redundant server Node group, the configured rate applies to the interface on each node. For example, if you configure a policer to rate-limit at 1 Gbps and apply the policer to a LAG that has one member on server node A and one member on server node B, the allowed throughput for each member is 1 Gbps, for a total allowed throughput of 2 Gbps.

Related Documentation

- Overview of Policers on page 35
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128

Understanding Color-Blind Mode for Single-Rate Tricolor Marking

With the color-blind mode of single-rate tricolor marking, all packets are evaluated against the CBS. If a packet exceeds the CBS, it is evaluated against the EBS. In color-blind mode, the policer supports three loss priorities only: low, medium-high, and high.

Packets that exceed the CBS but are below the EBS are marked yellow (medium-high). Packets that exceed the EBS are marked red (high), as shown in Table 9 on page 41.

Table 9: Color-Blind Mode TCM Color-to-PLP Mapping

Color	PLP	Meaning
Green	**low**	Conforming.
Yellow	**medium-high**	Packet exceeds the CIR and CBS but does not exceed the EBS.
Red	**high**	Packet exceeds the EBS.

Related Documentation

- Overview of Policers on page 35
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 127

Understanding Color-Aware Mode for Single-Rate Tricolor Marking

In color-aware mode, the treatment the packet receives depends on its classification. Marking can increase a preassigned PLP but cannot decrease it.

Summary of PLP Changes

Table 10 on page 41 shows how a packet's incoming priority can be modified with single-rate marking.

Table 10: Color-Aware Mode Single-Rate PLP Mapping

Incoming PLP	Packet Metered Against	Possible Cases	Outgoing PLP
low	CIR, CBS, and EBS	Conforming	**low**
		Packet exceeds the CIR and CBS but does not exceed the EBS.	**medium-high**
		Packet exceeds the EBS.	**high**

Table 10: Color-Aware Mode Single-Rate PLP Mapping *(continued)*

Incoming PLP	Packet Metered Against	Possible Cases	Outgoing PLP
medium-low	EBS only	Packet does not exceed the EBS.	**medium-low**
		Packet exceeds the EBS.	**high**
medium-high	EBS only	Packet does not exceed the EBS.	**medium-high**
		Packet exceeds the EBS.	**high**
high	Not metered by the policer.	All cases.	**high**

The following sections describe single-rate color-aware PLP mapping in more detail.

Effect on Green Packets (Low PLP)

Packets belonging to the green class have already been marked by a classifier with low PLP. The marking policer can leave the PLP unchanged or increase it to medium-high or high, so these packets are therefore metered against both the CBS and the EBS. For example, if a behavior aggregate or multifield classifier marks a packet with low PLP and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CIR, packets remain marked as low PLP.
- If bursts exceed the CBS but not the EBS, some of the packets are marked as medium-high PLP, and some of the packets remain marked as low PLP.
- If bursts exceed the EBS, some of the packets are marked as high PLP, and some of the packets remain marked as low PLP.

Effect on Yellow Packets (Medium PLP)

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the PLP unchanged or increase it to high, so these packets are therefore metered against the EBS only. For example, if a behavior aggregate or multifield classifier marks a packet with medium-low PLP and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CBS, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the CBS but less than the EBS, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the EBS, some of the packets are marked as high PLP and some remain marked as medium-low PLP.

If a BA or multifield classifier marks a packet with medium-high PLP and the two-rate TCM policer is in color-aware mode, the policer assigns output loss priority as follows:

- If the rate of traffic flow is less than the CBS, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the CBS but less than the EBS, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the EBS, some of the packets are marked as high PLP and some remain marked as medium-high PLP.

Effect on Red Packets (High PLP)

Packets belonging to the red class have already been marked by a classifier with high PLP. Because the policer cannot decrease the PLP, it does not change it, and these packets are not metered against the CBS or the EBS.

Related Documentation

- Overview of Policers on page 35
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 127

Understanding Color-Blind Mode for Two-Rate Tricolor Marking

With the color-blind mode of two-rate tricolor marking, all packets are evaluated against the committed information rate (CIR). If a packet exceeds the CIR, it is evaluated against the peak information rate (PIR). Packets that exceed the CIR but are below the PIR are marked yellow (medium-high). Packets that exceed the PIR are marked red (high).

Table 11: Color-Blind Mode TCM Color-to-PLP Mapping

Color	PLP	Meaning
Green	**low**	Packet does not exceed the CIR.
Yellow	**medium-high**	Packet exceeds the CIR but does not exceed the PIR.
Red	**high**	Packet exceeds the PIR.

Related Documentation

- Overview of Policers on page 35
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 127

Understanding Color-Aware Mode for Two-Rate Tricolor Marking

In color-aware mode, the treatment the packet receives depends on its classification. Marking can increase the preassigned PLP but cannot decrease it

Summary of PLP Changes

Table 12 on page 44 shows how a packet's incoming priority can be modified with two-rate marking.

Table 12: Color-Aware Mode Two-Rate PLP Mapping

Incoming PLP	Packet Metered Against	Possible Cases	Outgoing PLP
low	CIR and PIR	Packet does not exceed the CIR.	**low**
		Packet exceeds the CIR but not the PIR.	**medium-high**
		Packet exceeds the PIR.	**high**
medium-low	PIR only	Packet does not exceed the PIR.	**medium-low**
		Packet exceeds the PIR.	**high**
medium-high	PIR only	Packet does not exceed the PIR.	**medium-high**
		Packet exceeds the PIR.	**high**
high	Not metered by the policer.	All cases.	**high**

The following sections describe color-aware two-rate PLP mapping in more detail.

Effect on Green Packets (Low PLP)

Packets belonging to the green class have already been marked by a classifier with low PLP. The marking policer can leave the packet's PLP unchanged or increase the PLP to medium-high or high. These packets are therefore metered against both the CIR and the PIR. For example, if a behavior aggregate or multifield classifier marks a packet with low PLP and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CIR, the packets remain marked as low PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, some of the packets are marked as medium-high PLP and some of the packets remain marked as low PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP and some of the packets remain marked as low PLP.

Effect on Yellow Packets (Medium PLP)

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the PLP unchanged or increase it to high. These packets are therefore metered against the PIR only. For example, if a behavior aggregate (BA) or multifield classifier marks a packet with medium-low PLP and the two-rate TCM policer is in color-aware mode, the policer assigns output loss priority as follows:

- If the rate of traffic flow is less than the CIR, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP and some of the packets remain marked as medium-low PLP.

If a BA or multifield classifier marks a packet with medium-high PLP and the two-rate TCM policer is in color-aware mode, the policer assigns output loss priority as follows:

- If the rate of traffic flow is less than the CIR, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP and some of the packets remain marked as medium-high PLP.

Effect on Red Packets (High PLP)

Packets belonging to the red class have already been marked by a classifier with high PLP. Because the policer cannot decrease the PLP, it does not change it, and these packets are not metered against the CIR or the PIR.

Related Documentation

- Overview of Policers on page 35
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 127

CHAPTER 3

Port Security

Overview of Access Port Protection

Port security features can protect a switch against various types of attacks. Protection methods against some common attacks are:

Mitigation of Ethernet Switching Table Overflow Attacks

In an overflow attack on an Ethernet switching table, an intruder sends so many requests from new MAC addresses that the table cannot learn all the addresses. The attack forces the switch to send broadcast messages when it needs to send traffic to addresses for which it lacks MAC addresses. In addition to generating unnecessary traffic, the attacker might be able to sniff the broadcast packets.

To mitigate such attacks, you can configure a limit for learned MAC addresses or allow only specific MAC addresses. Use the MAC limit feature to control the total number of MAC addresses that can be added to the Ethernet switching table for the specified interface or interfaces. By setting the MAC addresses that are explicitly allowed, you

ensure that the addresses of network devices whose network access is critical are guaranteed to be included in the Ethernet switching table.

Mitigation of Rogue DHCP Server Attacks

By default, all access ports are untrusted, and all trunk ports are trusted with regard to DHCP. Trusted ports allow DHCP servers to provide IP addresses and other information to requesting devices. If someone connects an unauthorized DHCP server to a trusted port, the unauthorized server can start issuing IP addresses and configuration information to the network's DHCP clients. The information provided to the clients by this server can disrupt their network access. The unauthorized server might also assign itself as the default gateway device for the network. An attacker can then sniff the network traffic and perpetrate a man-in-the-middle attack—that is, it misdirects traffic intended for a legitimate network device to a device of its choice.

To mitigate this problem, set the interface to which the unauthorized server is connected as untrusted. That action blocks all ingress DHCP server messages from that interface.
.

NOTE: The switch logs all DHCP server packets that are received on untrusted ports. For example:

5 untrusted DHCPOFFER received, interface xe-:0/0/2.0[65], vlan v1[10] server ip/mac 12.12.12.1/00:00:00:00:01:12 offer ip/client mac 12.12.12.253/00:AA:BB:CC:DD:01

You can use these messages to detect unauthorized DHCP servers on the network.

NOTE: If you attach a DHCP server to an access port, you must configure the port as trusted.

Protection Against ARP Spoofing Attacks

In ARP spoofing, an attacker sends faked ARP messages on the network. The attacker associates its own MAC address with the IP address of a network device connected to the switch. Any traffic sent to that IP address is instead sent to the attacker. Now the attacker can create various types of problems, including sniffing the packets that were meant for another host and perpetrating man-in-the middle attacks. (In a man-in-the-middle attack, the attacker intercepts messages between two hosts, reads them, and perhaps alters them, all without the original hosts knowing that their communications have been compromised.)

To protect against ARP spoofing on your switch, enable both DHCP snooping and dynamic ARP inspection (DAI). DHCP snooping builds and maintains the DHCP snooping table. That table contains the MAC addresses, IP addresses, lease times, binding types, VLAN information, and interface information for the untrusted interfaces on the switch. DAI uses the information in the DHCP snooping table to validate ARP packets. Invalid ARP

packets are blocked, and when they are blocked, a system log message is recorded that includes the type of ARP packet and the sender's IP address and MAC address.

See "Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks" on page 106.

Protection Against DHCP Snooping Database Alteration Attacks

In an attack designed to alter the DHCP snooping database, an intruder introduces a DHCP client on one of the switch's untrusted access interfaces that has a MAC address identical to that of a client on another untrusted port. The intruder acquires the DHCP lease, which results in changes to the entries in the DHCP snooping table. Subsequently, what would have been valid ARP requests from the legitimate client are blocked.

To protect against this type of alteration of the DHCP snooping database, configure MAC addresses that are explicitly allowed on the interface. See "Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks" on page 111.

Protection Against DHCP Starvation Attacks

In a DHCP starvation attack, an attacker floods an Ethernet LAN with DHCP requests from spoofed (counterfeit) MAC addresses so that trusted DHCP servers cannot keep up with requests from legitimate DHCP clients. The address space of those servers is completely used up, so they can no longer assign IP addresses and lease times to clients. DHCP requests from those clients are either dropped—that is, the result is a denial of service (DoS)—or directed to a rogue DHCP server set up by the attacker to imitate a legitimate DHCP server.

To protect the switch from DHCP starvation attacks, use the MAC limiting feature. Specify the maximum number of MAC addresses that the switch can learn on the access interfaces to which DHCP clients connect. The DHCP server or servers can then supply only the specified number of IP addresses over each of those interfaces. If a DHCP starvation attack occurs after the maximum number of IP addresses has been assigned, the attack fails.

Related Documentation

- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Configuring MAC Limiting on page 134
- Verifying That MAC Limiting Is Working Correctly on page 240
- Understanding DHCP Option 82 for Port Security on page 64
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 88
- Understanding DAI for Port Security on page 59

Port Security Overview

Ethernet LANs are vulnerable to attacks such as address spoofing (forging) and Layer 2 denial of service (DoS) on network devices. Port security features help protect the access ports on your switch against the loss of information and productivity that can result from such attacks.

Juniper Networks Junos operating system (Junos OS) provides features to help secure ports on the switch. Ports can be categorized as either trusted or untrusted. You apply policies appropriate to each category to protect ports against various types of attacks.

Basic port security features are enabled in the switch's default configuration. You can configure additional features with minimal configuration steps.

Depending on the particular feature, you can configure the feature either on VLANs or interfaces.

Port security features supported on switches are:

- DHCP snooping—Filters and blocks ingress Dynamic Host Configuration Protocol (DHCP) server messages on untrusted ports; builds and maintains an IP address to MAC address binding (IP-MAC binding) database, which is called the DHCP snooping database.

  NOTE: **DHCP snooping is not enabled in the default switch configurations. DHCP snooping is enabled on a per-VLAN basis. The details of enabling DHCP snooping depend on the particular switch.**

- DHCPv6 snooping—DHCP snooping for IPv6.
- DHCP option 82—Also known as the DHCP Relay Agent information option. This DHCPv4 feature helps protect the switch against attacks such as spoofing of IP addresses and media access control (MAC) addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.
- DHCPv6 option 37—Option 37 is the DHCP for IPv6 (DHCPv6) equivalent of option 82 and is enabled by default when DHCPv6 snooping is enabled on a VLAN.
- Dynamic ARP inspection (DAI)—Prevents Address Resolution Protocol (ARP) spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable DAI on a VLAN.
- IPv6 Neighbor Discovery inspection—Prevents IPv6 address spoofing attacks. Neighbor Discovery requests and replies are compared against entries in the DHCPv6 snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable Neighbor Discovery inspection on a VLAN.

- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. With IP source guard enabled, the source IP address in the packet sent from an untrusted access interface is validated against the source MAC address in the DHCP snooping database. The packet is forwarded if the source IP-MAC binding is valid; if the binding is not valid, the packet is discarded. You enable IP source guard on a VLAN. EX Series switches support IPv6 source guard also.

  NOTE: **IP source guard is not supported.**

- MAC limiting—Protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You can enable MAC limiting on an interface.
- MAC move limiting—(Not supported on EX9200) Tracks MAC movement and detects MAC spoofing on access ports. You enable this feature on a VLAN.
- Persistent MAC learning—Also known as sticky MAC. Persistent MAC learning enables interfaces to retain dynamically learned MAC addresses across switch reboots You enable this feature on an interface.
- RA Guard—Examines incoming Router Advertisement (RA) messages and decides whether to forward or block them based on statically-configured IPv6/MAC address bindings. If the content of the RA message does not match the bindings, the message is dropped.
- Trusted DHCP server—Configuring the DHCP server on a trusted port protects against rogue DHCP servers sending leases. You enable this feature on an interface (port). By default, access ports are untrusted, and trunk ports are trusted. (Access ports are the switch ports that connect to Ethernet endpoints such as user PCs and laptops, servers, and printers. Trunk ports are the switch ports that connect an Ethernet switch to other switches or to routers.)

Related Documentation

- *Security Features for EX Series Switches Overview*
- Understanding DHCP Snooping for Port Security on page 52
- *Understanding DHCP Snooping for Port Security*
- *Understanding IPv6 Neighbor Discovery Inspection*
- Understanding DAI for Port Security on page 59
- *Understanding IP Source Guard for Port Security on EX Series Switches*
- *Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches*
- *Understanding DHCP Option 82 for Port Security on EX Series Switches*

Understanding DHCP Snooping for Port Security

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. When DHCP snooping is enabled, the system snoops the DHCP messages to view DHCP lease information and build and maintain a database of valid IP address to MAC address (IP-MAC) bindings called the DHCP snooping database. Only clients with valid bindings are allowed access to the network.

DHCP Snooping Basics

Dynamic Host Configuration Protocol (DHCP) allocates IP addresses dynamically, *leasing* addresses to devices so that the addresses can be reused when no longer needed. Hosts and end devices that require IP addresses obtained through DHCP must communicate with a DHCP server across the LAN.

DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server (the server is connected to a trusted network port).

By default, all trunk ports on the switch are trusted and all access ports are untrusted for DHCP snooping.

When DHCP snooping is enabled, the lease information from the switch is used to create the DHCP snooping database, a mapping of IP address to MAC-address pairs.

NOTE: **DHCP snooping is disabled in the default switch configuration. You must explicitly enable DHCP snooping by setting examine-dhcp at the [edit ethernet-switching-options secure-access-port] hierarchy level.**

Entries in the DHCP database are updated in these events:

- When a DHCP client releases an IP address (sends a DHCPRELEASE message), the associated mapping entry is deleted from the database.
- If you move a network device from one VLAN to another, typically the device needs to acquire a new IP address. Therefore, its entry in the database, including the VLAN ID, is updated.

- When the lease time (timeout value) assigned by the DHCP server expires, the associated entry is deleted from the database.

TIP: By default, the IP-MAC bindings are lost when the switch is rebooted and DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the **dhcp-snooping-file** statement to store the database file either locally or remotely.

You can configure the switch to snoop DHCP server responses only from particular VLANs. Doing this prevents spoofing of DHCP server messages.

You configure DHCP snooping per VLAN, not per interface (port). DHCP snooping is disabled by default.

DHCP Snooping Process

The basic process of DHCP snooping consists of the following steps:

NOTE: When DHCP snooping is enabled for a VLAN, all DHCP packets sent from that network devices in that VLAN are subjected to DHCP snooping. The final IP-MAC binding occurs when the DHCP server sends DHCPACK to the DHCP client.

1. The network device sends DHCPDISCOVER packet to request IP address.
2. The switch forwards the packet to the DHCP server.
3. The server sends a DHCPOFFER packet to offer an address. If the DHCPOFFER packet is from a trusted interface, the switch forwards the packet to the DHCP client.
4. The network device sends a DHCPREQUEST packet to accept the IP address. The switch adds an IP-MAC placeholder binding to the database. The entry is considered a placeholder until a DHCPACK packet is received from the server. Until then, the IP address could still be assigned to some other host.
5. The server sends a DHCPACK packet to assign the IP address or a DHCPNAK packet to deny the address request.
6. The switch updates the DHCP database in accordance with the type of packet received:
   - Upon receipt of a DHCPACK packet, the switch updates lease information for the IP-MAC binding in its database.
   - Upon receipt of a DHCPNACK packet, the switch deletes the placeholder.

NOTE: The DHCP database is updated only after the DHCPREQUEST packet has been sent.

For general information about the messages that the DHCP client and DHCP server exchange during the assignment of an IP address for the client, see the *Junos OS System Basics Configuration Guide*.

DHCP Server Access

A switch's access to the DHCP server can be configured in three ways:

- Switch, DHCP Clients, and DHCP Server Are All on the Same VLAN on page 54
- Switch Acts as DHCP Server on page 55
- Switch Acts as Relay Agent on page 56

Switch, DHCP Clients, and DHCP Server Are All on the Same VLAN

When the switch, DHCP clients, and DHCP server are *all members of the same VLAN*, the DHCP server can be connected to the switch in one of two ways:

- The server is directly connected to the same switch as the one connected to the DHCP clients (the hosts, or network devices, that are requesting IP addresses from the server). The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. See Figure 4 on page 54.
- The server is connected to an intermediary switch (Switch 2) that is connected through a trunk port to the switch (Switch 1) that the DHCP clients are connected to. Switch 2 is being used as a transit switch. The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. See Figure 5 on page 55—in the figure, **ge-0/0/11** is a trusted trunk port.

Figure 4: DHCP Server Connected Directly to Switch

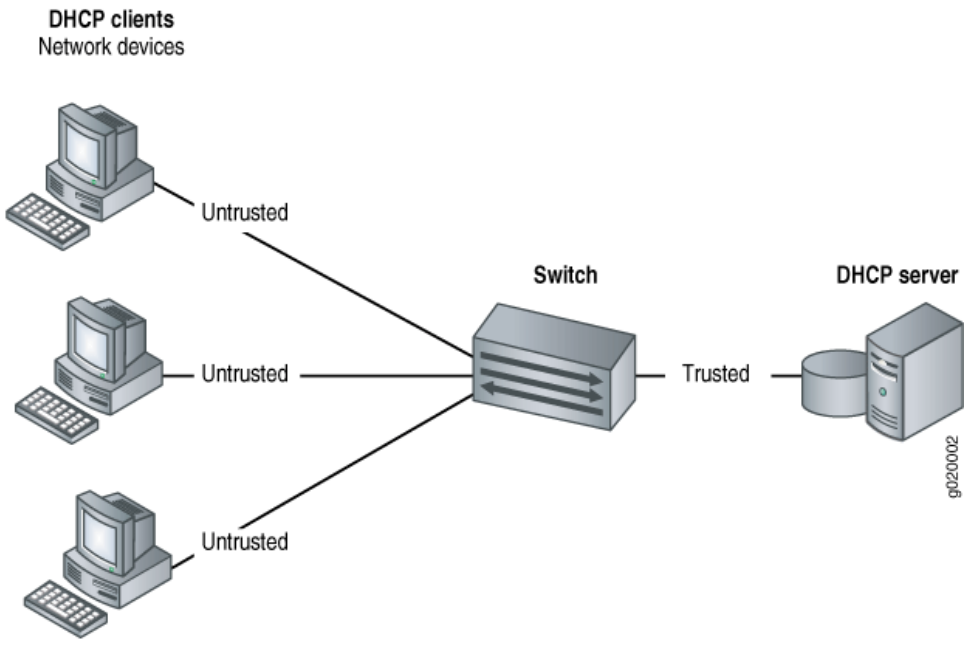
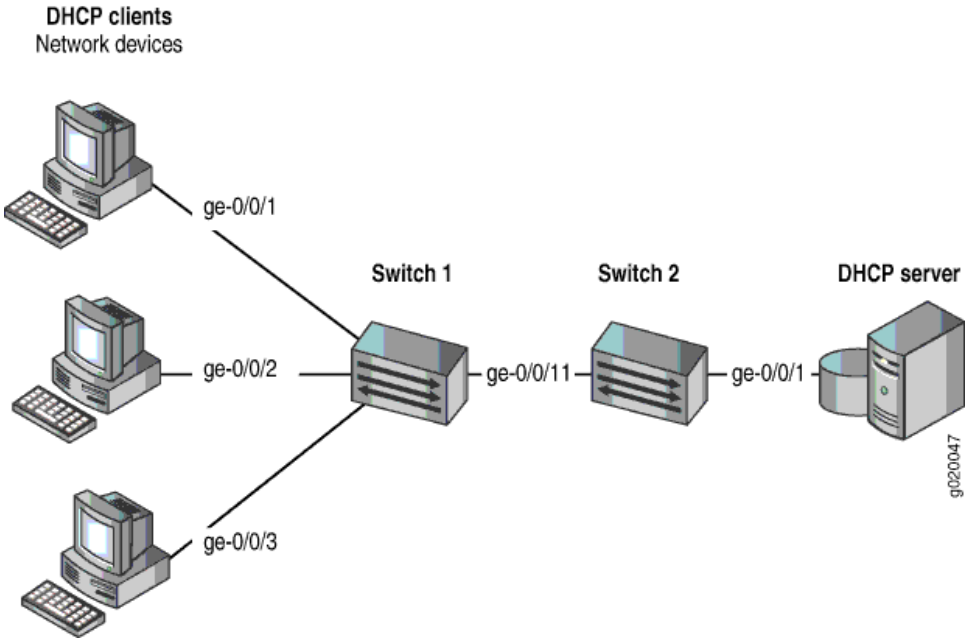


Figure 5: DHCP Server Connected Directly to Switch 2, with Switch 2 Connected to Switch 1 Through a Trusted Trunk Port

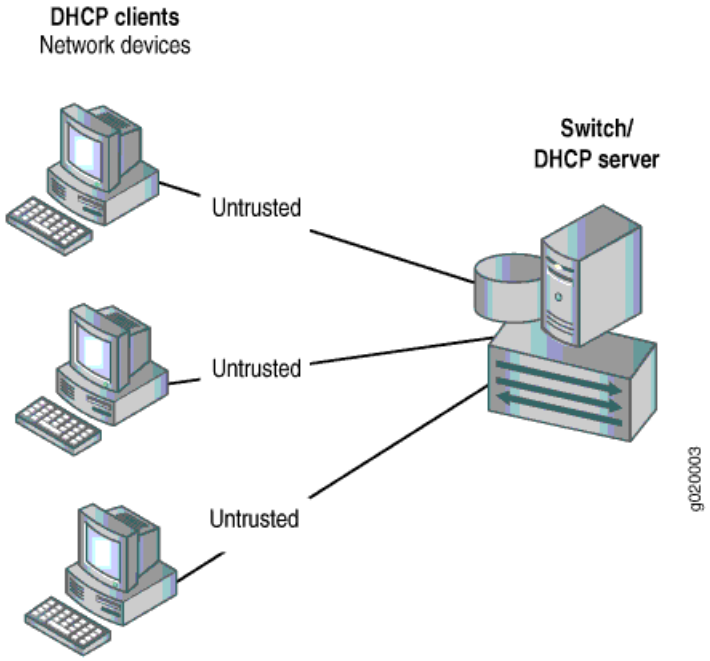


Switch Acts as DHCP Server

NOTE: The switch cannot act as a DHCP server.

The switch itself is configured as a DHCP server; this is known as a “local” configuration. See Figure 6 on page 56.

Figure 6: Switch Is the DHCP Server



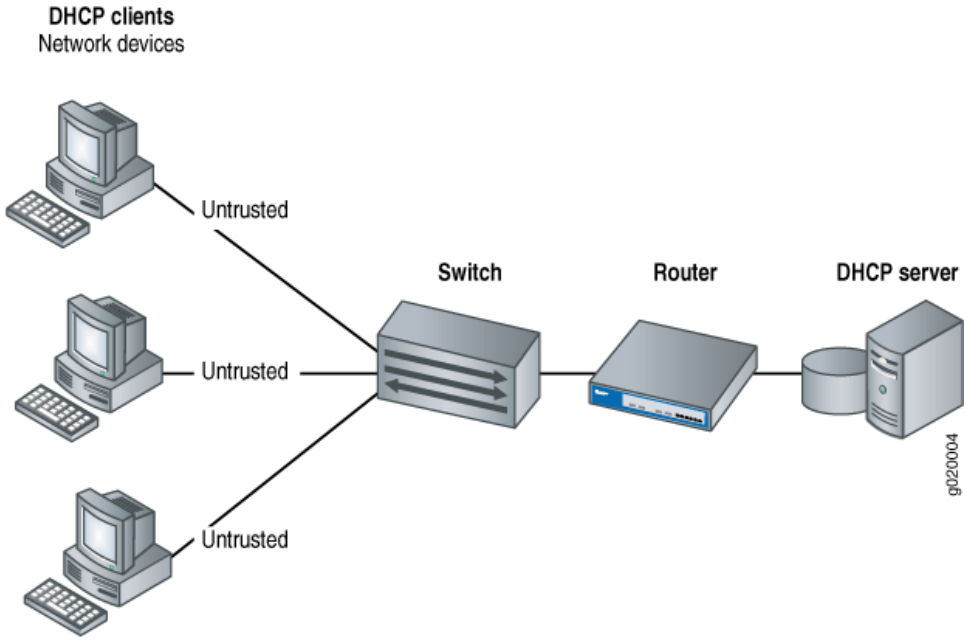
Switch Acts as Relay Agent

The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. The Layer 3 interfaces on the switch are configured as routed VLAN interfaces (RVIs,) or integrated routing and bridging interfaces (IRBs). The trunk interfaces are trusted by default.

These two scenarios illustrate the switch acting as a relay agent:

- The DHCP server and clients are in different VLANs.
- The switch is connected to a router that is in turn connected to the DHCP server. See Figure 7 on page 57.

Figure 7: Switch Acting as Relay Agent Through Router to DHCP Server



DHCP Snooping Table

The software creates a DHCP snooping information table that displays the content of the DHCP snooping database. The table shows current IP-MAC bindings, as well as lease time, type of binding, names of associated VLANs, and associated interface.

To display the DHCP snooping database, issue the operational mode command show dhcp snooping binding.

Static IP Address Additions to the DHCP Snooping Database

You can add specific static IP addresses to the database as well as have the addresses dynamically assigned through DHCP snooping. To add static IP addresses, you supply the IP address, the MAC address of the device, the interface on which the device is connected, and the VLAN with which the interface is associated. No lease time is assigned to the entry. The statically configured entry never expires.

Snooping DHCP Packets That Have Invalid IP Addresses

If you enable DHCP snooping on a VLAN and then devices on that VLAN send DHCP packets that request invalid IP addresses, these invalid IP addresses will be stored in the DHCP snooping database until they are deleted when their default timeout is reached. To eliminate this unnecessary consumption of space in the DHCP snooping database, the switch drops the DCHP packets that request invalid IP addresses, preventing the snooping of these packets. The invalid IP addresses are:

- 0.0.0.0
- 128.0.*x.x*
- 191.255.*x.x*

- 192.0.0.*x*
- 223.255.255.*x*
- 224.*x.x.x*
- 240.*x.x.x* to 255.255.255.255

Prioritizing Snooped Packets

NOTE: **Prioritizing snooped packets is not supported on the QFX Series and the EX4600 switch.**

You can use class-of-service (CoS) forwarding classes and queues to prioritize DHCP snooped packets for a specified VLAN. This type of configuration places the DHCP snooped packets for that VLAN in the desired egress queue, so that the security procedure does not interfere with the transmittal of high-priority traffic. For additional information, see *Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic*.

Related Documentation

- Port Security Overview on page 50
- Understanding Trusted DHCP Servers for Port Security on page 64
- *Understanding DHCP Option 82 for Port Security on EX Series Switches*
- *Understanding DHCP Services for Switches*
- *DHCP/BOOTP Relay for Switches Overview*
- Example: Configuring Basic Port Security Features on page 79
- Enabling DHCP Snooping (CLI Procedure) on page 140
- *Enabling DHCP Snooping (J-Web Procedure)*
- *Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure)*

Understanding DAI for Port Security

Dynamic ARP inspection (DAI) protects switches against ARP spoofing.

DAI inspects Address Resolution Protocol (ARP) packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP spoofing (also known as ARP poisoning or ARP cache poisoning). ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. When an attacker tries to use a forged ARP packet to spoof an address, the switch compares the address with entries in the database. If the media access control (MAC) address or IP address in the ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped.

ARP packets are sent to the Routing Engine and are rate-limited to protect the switch from CPU overload.

Address Resolution Protocol

Sending IP packets on a multi-access network requires mapping an IP address to an Ethernet MAC address.

Ethernet LANs use ARP to map MAC addresses to IP addresses.

The switch maintains this mapping in a cache that it consults when forwarding packets to network devices. If the ARP cache does not contain an entry for the destination device, the host (the DHCP client) broadcasts an ARP request for that device's address and stores the response in the cache.

ARP Spoofing

ARP spoofing is one way to initiate man-in-the-middle attacks. The attacker sends an ARP packet that spoofs the MAC address of another device on the LAN. Instead of the switch sending traffic to the proper network device, the switch sends the traffic to the device with the spoofed address that is impersonating the proper device. If the impersonating device is the attacker's machine, the attacker receives all the traffic from the switch that must have gone to another device. The result is that traffic from the switch is misdirected and cannot reach its proper destination.

One type of ARP spoofing is gratuitous ARP, which is when a network device sends an ARP request to resolve its own IP address. In normal LAN operation, gratuitous ARP messages indicate that two devices have the same MAC address. They are also broadcast when a network interface card (NIC) in a device is changed and the device is rebooted, so that other devices on the LAN update their ARP caches. In malicious situations, an attacker can poison the ARP cache of a network device by sending an ARP response to

the device that directs all packets destined for a certain IP address to go to a different MAC address instead.

To prevent MAC spoofing through gratuitous ARP and through other types of spoofing, the switches examine ARP responses through DAI.

Dynamic ARP Inspection

DAI examines ARP requests and responses on the LAN and validates ARP packets. The switch intercepts ARP packets from an access port and validates them against the DHCP snooping database. If no IP-MAC entry in the database corresponds to the information in the ARP packet, DAI drops the ARP packet and the local ARP cache is not updated with the information in that packet. DAI also drops ARP packets when the IP address in the packet is invalid. ARP probe packets are not subjected to dynamic ARP inspection. The switch always forwards such packets.

Junos OS for EX Series switches and the QFX Series uses DAI for ARP packets received on access ports because these ports are untrusted by default. Trunk ports are trusted by default, and therefore ARP packets bypass DAI on them.

You configure DAI for each VLAN, not for each interface (port). By default, DAI is disabled for all VLANs.

If you set an interface to be a DHCP trusted port, it is also trusted for ARP packets.

NOTE:

- If your switch uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, see *Enabling a Trusted DHCP Server (CLI Procedure)* for information about configuring an access interface to be a DHCP trusted port. .
- If your switch is not using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, see "Enabling a Trusted DHCP Server (CLI Procedure)" on page 144 for information about configuring an access interface to be a DHCP trusted port.

For packets directed to the switch to which a network device is connected, ARP queries are broadcast on the VLAN. The ARP responses to those queries are subjected to the DAI check.

For DAI, all ARP packets are trapped to the PFE. To prevent CPU overloading, ARP packets destined for the Routing Engine are rate-limited.

If the DHCP server goes down and the lease time for an IP-MAC entry for a previously valid ARP packet runs out, that packet is blocked.

Prioritizing Inspected Packets

NOTE: **Prioritizing inspected packets is not supported on the QFX Series and the EX4600 switch.**

You can use class-of-service (CoS) forwarding classes and queues to prioritize DAI packets for a specified VLAN. This type of configuration places inspected packets for that VLAN in the egress queue, that you specify, ensuring that the security procedure does not interfere with the transmission of high-priority traffic.

Related Documentation

- Port Security Overview on page 50
- Understanding DHCP Snooping for Port Security on page 52
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 99
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 106
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing*
- *Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic*
- Enabling Dynamic ARP Inspection (CLI Procedure) on page 142
- *Enabling Dynamic ARP Inspection (CLI Procedure)*
- *Enabling Dynamic ARP Inspection (J-Web Procedure)*

Understanding MAC Limiting and MAC Move Limiting for Port Security

MAC limiting protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You enable this feature on Layer 2 interfaces (ports). MAC move limiting detects MAC movement and MAC spoofing on access interfaces. You enable this feature on VLANs.

- MAC Limiting on page 61
- MAC Move Limiting on page 62
- Actions for MAC Limiting on page 62
- MAC Addresses That Exceed the MAC Limit or MAC Move Limit on page 63

MAC Limiting

MAC limiting sets a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface or on all the Layer 2 access interfaces on the switch. Junos OS provides two MAC limiting methods:

- Maximum number of MAC addresses—You configure the maximum number of dynamic MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses can be ignored, dropped, or logged. You can also specify that the interface be shut down or temporarily disabled.
- Allowed MAC addresses—You configure specific “allowed” MAC addresses for the access interface. Any MAC address that is not in the list of configured addresses is not learned, and the switch logs an appropriate message. Allowed MAC binds MAC addresses to a VLAN so that the address does not get registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.

NOTE: If you do not want the system to log messages about invalid MAC addresses received by an interface that has been configured for allowed MAC addresses, disable the logging by configuring the no-allowed-mac-log statement.

You configure MAC limiting per interface, not per VLAN. You can specify the maximum number of dynamic MAC addresses that can be learned on a single Layer 2 access interface (including tagged-access interfaces) or on all Layer 2 access interfaces.

MAC Move Limiting

MAC move limiting causes the switch to track the number of times a MAC address can move to a new interface (port). It can help to prevent MAC spoofing, and it can also detect and prevent loops.

If a MAC address moves more than the configured number of times within 1 second, the switch performs the configured action. You can configure MAC move limiting to apply to all VLANs or to a specific VLAN.

CAUTION: Mac move limiting does not work properly on a QFX5100 switch used as a Node device in a QFabric system. Do not use this feature on a QFX5100 switch in a QFabric system.

Actions for MAC Limiting

You can choose to have one of the following actions performed when the limit of MAC addresses or the limit of MAC moves is exceeded:

- **drop**—Drop the packet and generate a system log entry. This is the default.
- **log**—Do not drop the packet but generate a system log entry.
- **none**—Take no action.
- **shutdown**—Disable the interface and generate an alarm. If you configure the switch with the port-error-disable statement, the disabled interface recovers automatically

upon expiration of the specified timeout. If this is not configured, you can bring up the disabled interfaces by running the **clear ethernet-switching port-error** command.

See descriptions of results of these various action settings in "Verifying That MAC Limiting Is Working Correctly" on page 240.

If you set a MAC limit to apply to all interfaces on the switch, you can override that setting for a particular interface by specifying action **none**. See "Configuring the none Action to Override a MAC Limit Applied to All Interfaces (CLI Procedure)" on page 138

MAC Addresses That Exceed the MAC Limit or MAC Move Limit

If you have configured the **port-error-disable** statement, you can view which interfaces are temporarily disabled because the MAC limit or MAC move limit was exceeded. Use the **show ethernet-switching interfaces** command.

The log messages that indicate the MAC limit or MAC move limit has been exceeded include the offending MAC addresses.

Related Documentation

- Port Security Overview on page 50
- Configuring MAC Limiting on page 134
- Configuring MAC Move Limiting (CLI Procedure) on page 136
- Verifying That MAC Limiting Is Working Correctly on page 240
- Verifying That MAC Move Limiting Is Working Correctly on page 243
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 88
- Example: Configuring Basic Port Security Features on page 79
- **no-allowed-mac-log on page 205**

Understanding Trusted and Untrusted Ports

By default, all access ports are untrusted and all trunk ports are trusted in regard to DHCP. Trusted ports allow DHCP servers to provide IP addresses and other information to requesting devices. Untrusted ports drop traffic from DHCP servers to prevent unauthorized servers from providing any configuration information to clients.

If you attach a DHCP server to an access port, you must configure the port as trusted. Before you do so, ensure that the server is physically secure—that is, that access to the server is monitored and controlled.

Related Documentation

- Understanding DHCP Snooping for Port Security on page 52
- Example: Configuring Basic Port Security Features on page 79
- Enabling a Trusted Port for DHCP on page 145

Understanding Trusted DHCP Servers for Port Security

Any interface on the switch that connects to a DHCP server can be configured as a trusted port. Configuring a DHCP server on a trusted port protects against rogue DHCP servers sending leases.

Ensure that the DHCP server interface is physically secure—that is, that access to the server is monitored and controlled at the site—before you configure the port as trusted.

Related Documentation

- Understanding DHCP Snooping for Port Security on page 52
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 95
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing*
- Enabling a Trusted DHCP Server (CLI Procedure) on page 144
- *Enabling a Trusted DHCP Server (CLI Procedure)*
- *Enabling a Trusted DHCP Server (J-Web Procedure)*

Understanding DHCP Option 82 for Port Security

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Hosts on untrusted access interfaces on Ethernet LAN switches send requests for IP addresses in order to access the Internet. The switch forwards or relays these requests to DHCP servers, and the servers send offers for IP address leases in response. Attackers can use these messages to perpetrate address spoofing and starvation.

Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client. The Juniper Networks Junos operating system (Junos OS) implementation of DHCP option 82 supports RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

This topic covers:

- DHCP Option 82 Processing on page 64
- Suboption Components of Option 82 on page 65
- Configurations That Support Option 82 on page 66

DHCP Option 82 Processing

If DHCP option 82 is enabled on the switch, then when a DHCP client that is connected to the switch on an untrusted interface sends a DHCP request, the switch inserts information about the client's network location into the packet header of that request.

The switch then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or another parameter for the client. See "Suboption Components of Option 82" on page 65 for details about option 82 information.

You can enable DHCP option 82 on a single VLAN or on all VLANs on the switch. You can also configure it on Layer 3 interfaces (in routed VLAN interfaces, or RVIs) when the switch is functioning as a relay agent.

When option 82 is enabled on the switch, then this sequence of events occurs when a DHCP client sends a DHCP request:

1. The switch receives the request and inserts the option 82 information in the packet header.
2. The switch forwards or relays the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response back to the switch. It does not alter the option 82 information.
4. The switch strips the option 82 information from the response packet.
5. The switch forwards the response packet to the client.

NOTE: To use the DHCP option 82 feature, you must ensure that the DHCP server is configured to accept option 82. If it is not configured to accept option 82, then when it receives requests containing option 82 information, it does not use the information in setting parameters and it does not echo the information in its response message.

Suboption Components of Option 82

When configuring DHCP option 82, you can use the following suboptions:

- circuit ID—Identifies the circuit (interface and/or VLAN) on the switch on which the request was received. The circuit ID contains the interface name and/or VLAN name, with the two elements separated by a colon—for example, **xe-0/0/10:vlan1**. If the request packet is received on a Layer 3 interface, the circuit ID is just the interface name—for example, **xe-0/0/10**.

  Use the **prefix** option to add an optional prefix to the circuit ID. If you enable the **prefix** option, the hostname for the switch is used as the prefix; for example, **switch1:xe-0/0/10:vlan1**..

  You can also specify that the interface description be used rather than the interface name and that the VLAN ID be used rather than the VLAN name.

- remote ID—Identifies the host. By default, the remote ID is the MAC address of the switch. You can specify that the remote ID be the hostname of the switch, the interface description, or a character string of your choice. You can also add an optional prefix to the remote ID.

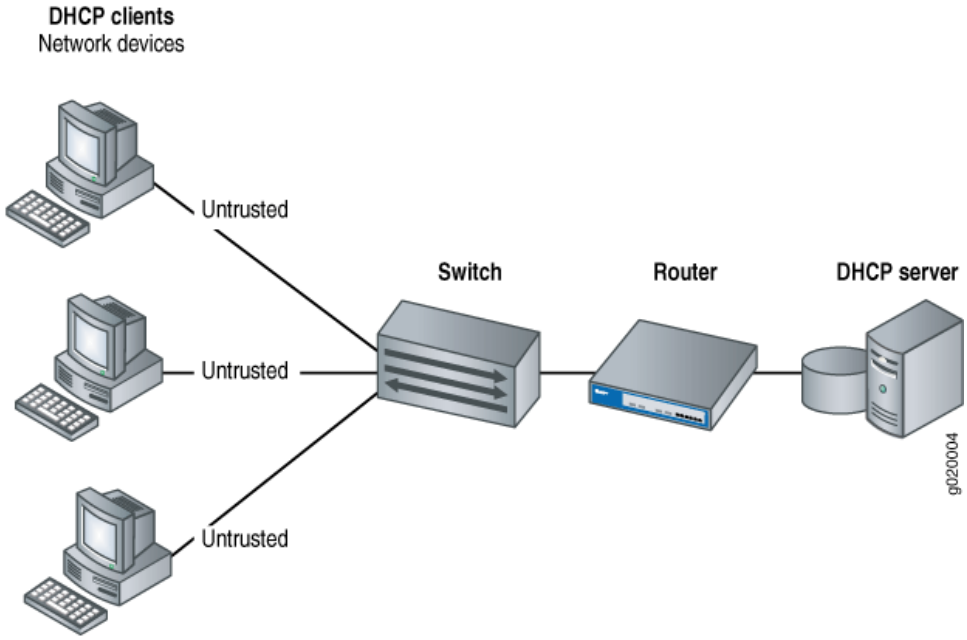
- vendor ID—Identifies the vendor of the host. If you specify the **vendor-id** option but do not enter a value, the default value **Juniper** is used. To specify a value, you type a character string.

Configurations That Support Option 82

You can use option 82 with the following configurations:

- The DHCP client and the DHCP server are on the same VLAN. In this case the switch forwards the requests from the clients on untrusted access interfaces to the server on a trusted interface. For this configuration, you set DHCP option 82 at the **[edit ethernet-switching-options secure-access-port vlan]** hierarchy level.
- The DHCP client or the DHCP server is connected to the switch through a Layer 3 interface and the switch is configured to relay DHCP requests. Figure 8 on page 66 illustrates a scenario for the switch-as-relay-agent; in this instance, the switch relays requests through a router to the server.

Figure 8: Switch Relays DHCP Requests to Server



For the configuration shown in Figure 8 on page 66, you set DHCP option 82 at the **[edit forwarding-options helpers bootp]** hierarchy level.

Related Documentation

- Overview of Access Port Protection on page 47
- *DHCP and BOOTP Relay Overview*
- **dhcp-option82 on page 189**
- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114

- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149

Understanding Static ARP Entries

You can create explicit mappings between IP addresses and MAC addresses, which are called static ARP table entries. Unlike dynamically learned ARP entries, static entries do not age out. You might want to create static ARP entries in a troubleshooting situation or if your device is unable to learn a MAC address dynamically for any reason.

Related Documentation

- Configuring Static ARP Entries on page 139
- *arp*

CHAPTER 4

Device Security

Understanding Storm Control

A traffic storm occurs when broadcast packets prompt receiving devices to broadcast packets in response. This prompts further responses, creating a snowball effect. The switch is flooded with packets, which creates unnecessary traffic that leads to poor performance or even a complete loss of service by some clients. Storm control causes a device to monitor traffic levels and take a specified action when a specified traffic level—called the *storm control level*—is exceeded, thus preventing packets from proliferating and degrading service. You can configure devices to drop broadcast and unknown unicast packets, shut down interfaces, or temporarily disable interfaces when the storm control level is exceeded.

Storm control is enabled by default on ELS platforms and disabled by default on non-ELS platforms. If storm control is enabled, the default level is 80 percent of the available bandwidth for ingress traffic. You can change the storm control level by configuring it as a specific bandwidth value. (The **level** configuration statement, which allows you to configure the storm control level as a percentage of the combined broadcast and unknown unicast streams, is deprecated and might be removed from future releases. We recommend that you phase out its use and replace it with the **bandwidth** statement.)

NOTE: Storm control is not enabled by default on MX platforms.

NOTE: When you configure storm control bandwidth, the value you configure is rounded off internally to the closest multiple of 64 Kbps, and the rounded-off value represents the bandwidth that is actually enforced. For example, if you configure a bandwidth limit of 150 Kbps, storm control enforces a bandwidth limit of 128 Kbps.

NOTE: On an FCoE-FC gateway, storm control must be disabled on all Ethernet interfaces that belong to an FCoE VLAN to prevent FCoE traffic from being dropped. Configuring storm control on an Ethernet interface that is included in an FCoE-FC gateway may have undesirable effects, including FCoE packet loss. After disabling storm control on all interfaces, enable storm control on any interfaces that are not part of an FCoE-FC gateway on which you want to use storm control. However, on an FCoE transit switch, you can enable storm control on interfaces that carry FCoE traffic.

CAUTION: The Junos OS allows you to configure a storm control value that exceeds the bandwidth of the interface. If you configure an interface this way, storm control does not drop broadcast or unknown unicast packets even if they consume all the available bandwidth.

To recognize a storm, you must be able to identify when traffic has reached an abnormal level. Suspect a storm when operations begin timing out and network response times slow down. Users might be unable to access expected services. Monitor the percentage of broadcast and unknown unicast traffic in the network when it is operating normally. This data can then be used as a benchmark to determine when traffic levels are too high. You can then configure storm control to set the level at which you want to drop broadcast and unknown unicast traffic.

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on page 87
- Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure) on page 138
- *Disabling Storm Control on FCoE Interfaces on an FCoE-FC Gateway*
- action-shutdown on page 224
- interface (Storm Control) on page 228
- port-error-disable on page 208
- storm-control on page 232

PART 2

Configuration

CHAPTER 5

Firewall and Policer Configuration Examples

Example: Using Two-Color Policers and Prefix Lists

If you provide specific amounts of bandwidth to internal or external customers, you can use policing to make sure that customers do not consume more bandwidth than they should receive. For example, you might connect many customers to one 10-Gbps interface and want to ensure that none of them congest the interface by using more bandwidth than they have been allotted.

You could accomplish this by creating a two-color policer similar to the following for each customer:

```
firewall {
    policer Limit-Customer-1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 150m;
        }
        then discard;
    }
```

Creating a policer for each customer is clearly not a scalable solution, however. As an alternative, you can create prefix lists that group classes of customers and then create policers for each prefix list. For example, you could create prefix lists such as **Class-A-Customer-Prefixes**, **Class-B-Customer-Prefixes**, and **Class-C-Customer-Prefixes** (at the **[edit policy-options]** hierarchy level) and create the following corresponding policers:

```
firewall {
    policer Class-A {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 150m;
        }
        then discard;
    }
```

```
    policer Class-B {
      if-exceeding {
        bandwidth-limit 75m;
        burst-size-limit 100m;
      }
      then discard;
    }
    policer Class-C {
      if-exceeding {
        bandwidth-limit 50m;
        burst-size-limit 75m;
      }
      then discard;
    }
}
```

You must create filter terms that specify the prefix lists in their **from** statements and the corresponding policers in their **then** statements similar to the following:

```
firewall
    family inet {
        filter Class-A-Customers {
            term term-1 {
                from {
                    destination-prefix-list {
                        Class-A-Customer-Prefixes;
                    }
                }
                then policer Class-A;
            }
        }
        filter Class-B-Customers {
            term term-1 {
                from {
                    destination-prefix-list {
                        Class-B-Customer-Prefixes;
                    }
                }
                then policer Class-B;
            }
        }
        filter Class-C-Customers {
            term term-1 {
                from {
                    destination-prefix-list {
                        Class-C-Customer-Prefixes;
                    }
                }
                then policer Class-C;
            }
        }
    }
```

Here are the steps to create this firewall configuration:

1. Create the first policer:

```
[edit firewall]
user@switch# set policer Class-A if-exceeding bandwidth-limit 100m burst-size-limit 150m
user@switch# set policer Class-A then discard
```

2. Create the second policer:

```
[edit firewall]
user@switch# set policer Class-B if-exceeding bandwidth-limit 75m burst-size-limit 100m
user@switch# set policer Class-B then discard
```

3. Create the third policer:

```
[edit firewall]
user@switch# set policer Class-C if-exceeding bandwidth-limit 50m burst-size-limit 75m
user@switch# set policer Class-C then discard
```

4. Create a filter for class A customers:

```
[edit firewall]
user@switch# edit family inet filter Class-A-Customers
```

5. Configure the filter to send packets matching the **Class-A-Customer-Prefixes** prefix list to the **Class-A** policer:

```
[edit firewall family inet filter Class-A-Customers]
user@switch# set term term-1 from source-prefix-list Class-A-Customers
user@switch# set term term-1 then policer Class-A
```

6. Create a filter for class B customers:

```
[edit firewall]
user@switch# edit family inet filter Class-B-Customers
```

7. Configure the filter to send packets matching the **Class-B-Customer-Prefixes** prefix list to the **Class-B** policer:

```
[edit firewall family inet filter Class-B-Customers]
user@switch# set term term-1 from source-prefix-list Class-B-Customers
user@switch# set term term-1 then policer Class-B
```

8. Create a filter for class C customers:

```
[edit firewall]
user@switch# edit family inet filter Class-C-Customers
```

9. Configure the filter to send packets matching the **Class-C-Customer-Prefixes** prefix list to the **Class-C** policer:

```
[edit firewall family inet filter Class-C-Customers]
user@switch# set term term-1 from source-prefix-list Class-C-Customers
user@switch# set term term-1 then policer Class-C
```

10. Apply the filters you created to the appropriate interfaces in the output direction.

NOTE: Note that the implicit deny statement in this filter will block traffic from any source that does not match one of the prefix lists. If you want the filter to allow this traffic, you must include an explicit term for this purpose.

Related Documentation

- Overview of Policers on page 35
- Applying Firewall Filters to Interfaces on page 33

- *prefix-list*

Example: Using Policers to Manage Oversubscription

You might want to use a policer when an interface is oversubscribed and you want to control what will happen if congestion occurs. For example, you might have servers connected to a switch as listed in Table 13 on page 76.

Table 13: Servers Connected to Switch

Server Type	Connection	IP Address
Network application server	1-gigabit interface	10.0.0.1
Authentication server	1-gigabit interface	10.0.0.2
Database server	10-gigabit interface	10.0.0.3

In this example, users access services provided by the network application server, which requests information from the database server as appropriate. When it receives a request from a user, the network application server first contacts the authentication server to verify the user's credentials. When a user is authenticated and the network application server provides the requested service, all the packets sent from the database server to the application server must transit the 1-Gigabit Ethernet interface connected to the application server twice—once on ingress to the application server and again on egress to the user.

The sequence of events for a user session is as follows:

1. A user connects to the application server and requests a service.
2. The application server requests the user's credentials and relays them to the authentication server.
3. If the authentication server verifies the credentials, the application server initiates the requested service.
4. The application server requests the files necessary to meet the user's request from the database server.
5. The database server sends the requested files to the application server.
6. The application server includes the requested files in its response to the user.

Traffic from the database server to the application server might congest the 1-gigabit interface to which that the application server is connected. This congestion might prevent the server from responding to requests from users and creating new sessions for them. You can use policing to make sure that this does not occur.

To create this firewall configuration, perform the following steps on the database server:

1. Create a policer to drop traffic from the database server to the application server if it exceeds certain limits:

   ```
   [edit firewall]
   user@switch# set policer Database-Egress-Policer if-exceeding bandwidth-limit 400
   burst-size-limit 500m
   user@switch# set policer Database-Egress-Policer then discard
   ```

2. Create a filter to examine traffic from the database server to the application server:

   ```
   [edit firewall]
   user@switch# edit family inet filter Database-Egress-Filter
   ```

3. Configure the filter to apply the policer to traffic egressing the database server and destined for the application server:

   ```
   [edit firewall family inet filter Database-Egress-Filter]
   user@switch# set term term-1 from destination-address 10.0.0.1
   user@switch# set term term-1 then policer Database-Egress-Policer
   ```

4. If required, configure a term to allow traffic from the database server to other destinations (otherwise the traffic will be dropped by the implicit deny statement):

   ```
   [edit firewall family inet filter Database-Egress-Filter]
   user@switch# set term term-2 then accept
   ```

   Note that omitting a **from** statement causes the term to match all packets, which is the desired behavior.

5. Install the egress filter as an output filter on the database server interface that is connected the application server:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/3 unit 0 family inet filter output Database-Egress-Filter
   ```

Here is how the final configuration would appear:

```
firewall {
    policer Database-Egress-Policer {
        if-exceeding {
            bandwidth-limit 400;
            burst-size-limit 500m;
        }
        then discard;
    }
    family inet {
        filter Database-Egress-Filter {
            term term-1 {
                from {
                    destination-address {
                        10.0.0.1/24;
                    }
                }
                then policer Database-Egress-Policer;
            }
            term term-2 {  # If required, include this term so that traffic from the database server
                to other destinations is allowed.
                then accept;
            }
        }
```

```
  }
]
```

Related Documentation

- Overview of Policers on page 35

CHAPTER 6

Port Security Configuration Examples

Example: Configuring Basic Port Security Features

You can configure DHCP snooping, dynamic ARP inspection (DAI), MAC limiting, persistent MAC learning, and MAC move limiting on the access ports of switches to protect the switches and the Ethernet LAN against address spoofing and Layer 2 denial-of-service (DoS) attacks. You can also configure a trusted DHCP server and specific (allowed) MAC addresses for the switch interfaces.

This example describes how to configure basic port security features on a switch:

Requirements

This example uses the following hardware and software components:

- One EX Series or QFX Series.
- Junos OS Release 11.4 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure basic port security features, be sure you have:

- Connected the DHCP server to the switch.
- Configured a VLAN on the switch. See the task for your platform:
  - *Configuring VLANs for EX Series Switches (CLI Procedure)*
  - *Configuring VLANs* for the QFX Series

NOTE: In this example, the DHCP server and its clients are all members of a single VLAN on the switch.

Overview and Topology

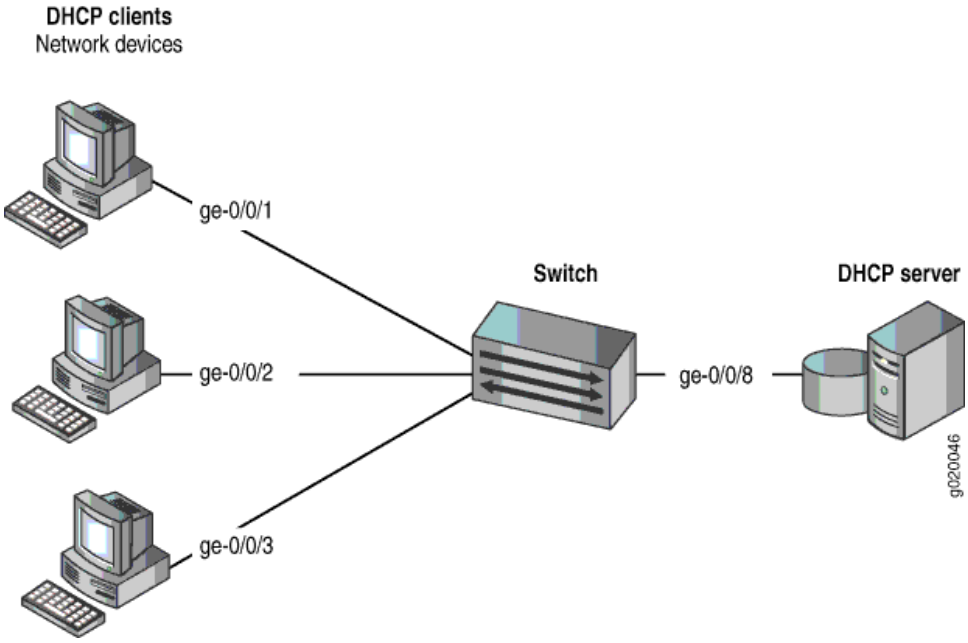
Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. To protect the devices from such attacks, you can configure:

- DHCP snooping to validate DHCP server messages
- DAI to protect against MAC spoofing
- MAC limiting to constrain the number of MAC addresses the switch adds to its MAC address cache
- MAC move limiting to help prevent MAC spoofing
- Persistent MAC learning (sticky MAC) to constrain the MAC addresses that can be learned on an interface to the first ones learned, even after a reboot of the switch
- Trusted DHCP server configured on a trusted port to protect against rogue DHCP servers sending leases

This example shows how to configure these security features on a switch connected to a DHCP server.

The setup for this example includes the VLAN **employee-vlan** on the switch. Figure 9 on page 81 illustrates the topology for this example.

Figure 9: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 14 on page 81.

Table 14: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX Series or QFX series switch
VLAN name and ID	**employee-vlan**, tag **20**
VLAN subnets	**192.0.2.16/28** **192.0.2.17** through **192.0.2.30** **192.0.2.31** is subnet's broadcast address
Interfaces in **employee-vlan**	**ge-0/0/1**, **ge-0/0/2**, **ge-0/0/3**, **ge-0/0/8**
Interface for DHCP server	**ge-0/0/8**

In this example, the switch is initially configured with the default port security setup. In the default switch configuration:

- Secure port access is activated on the switch.
- DHCP snooping and DAI are disabled on all VLANs.
- All access ports are untrusted, and all trunk ports are trusted for DHCP snooping.

In the configuration tasks for this example, you set the DHCP server as trusted; you enable DHCP snooping, DAI, and MAC move limiting on a VLAN; you set a value for a MAC limit on some interfaces; you configure some specific (allowed) MAC addresses on an interface; and you configure persistent MAC learning on an interface.

Configuration

To configure basic port security on a switch whose DHCP server and client ports are in a single VLAN:

CLI Quick Configuration

To quickly configure basic port security on the switch, copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/1 mac-limit 4
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88
set interface ge-0/0/2 mac-limit 4
set interface ge-0/0/1 persistent-learning
set interface ge-0/0/8 dhcp-trusted
set vlan employee-vlan arp-inspection
set vlan employee-vlan examine-dhcp
set vlan employee-vlan mac-move-limit 5
```

Step-by-Step Procedure

Configure basic port security on the switch:

1. Enable DHCP snooping on the VLAN:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee-vlan examine-dhcp
   ```

2. Specify the interface (port) from which DHCP responses are allowed:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface ge-0/0/8 dhcp-trusted
   ```

3. Enable dynamic ARP inspection (DAI) on the VLAN:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee-vlan arp-inspection
   ```

4. Configure a MAC limit of 4 and use the default action, **drop**. (Packets are dropped, and the MAC address is not added to the Ethernet switching table if the MAC limit is exceeded on the interfaces):

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface ge-0/0/1 mac-limit 4
   user@switch# set interface ge-0/0/2 mac-limit 4
   ```

5. Allow learned MAC addresses for a particular interface to persist across restarts of the switch and interface-down events by enabling persistent MAC learning:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface ge-0/0/1 persistent-learning
   ```

6. Configure a MAC move limit of **5** and use the default action, **drop**. (Packets are dropped, and the MAC address is not added to the Ethernet switching table if a MAC address has exceeded the MAC move limit):

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee-vlan mac-move-limit 5
   ```

7. Configure allowed MAC addresses:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
   user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
   ```

```
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88
```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/1.0 {
   mac-limit 4;
   persistent-learning;
}
interface ge-0/0/2.0 {
   allowed-mac [ 00:05:85:3a:82:80 00:05:85:3a:82:81 00:05:85:3a:82:83
      00:05:85:3a:82:85 00:05:85:3a:82:88 ];
   mac-limit 4;
}
interface ge-0/0/8.0 {
   dhcp-trusted;
}
vlan employee-vlan {
   arp-inspection
   examine-dhcp;
   mac-move-limit 5;
}
```

Verification

To confirm that the configuration is working properly:

- Verifying That DHCP Snooping Is Working Correctly on the Switch on page 83
- Verifying That DAI Is Working Correctly on the Switch on page 84
- Verifying That MAC Limiting, MAC Move Limiting, and Persistent MAC Learning Are Working Correctly on the Switch on page 85
- Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 86

Verifying That DHCP Snooping Is Working Correctly on the Switch

Purpose Verify that DHCP snooping is working on the switch.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp snooping binding
DHCP Snooping Information:
MAC Address         IP Address    Lease    Type     VLAN          Interface
-----------------   ----------    -----    ----     ----          ---------
00:05:85:3A:82:77    192.0.2.17    600    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:79    192.0.2.18    653    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:80    192.0.2.19    720    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:3A:82:81    192.0.2.20    932    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:3A:82:83    192.0.2.21   1230    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:27:32:88    192.0.2.22   3200    dynamic  employee-vlan   ge-0/0/2.0
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

If the DHCP server had been configured as untrusted, no entries would be added to the DHCP snooping database, and nothing would be shown in the output of the **show dhcp snooping binding** command.

Verifying That DAI Is Working Correctly on the Switch

Purpose Verify that DAI is working on the switch.

Action Send some ARP requests from network devices connected to the switch.

Display the DAI information:

```
user@switch> show arp inspection statistics
ARP inspection statistics:
Interface        Packets received  ARP inspection pass   ARP inspection failed
---------------  ----------------  --------------------  ---------------------
ge-0/0/1.0                      7                     5                      2
ge-0/0/2.0                     10                    10                      0
ge-0/0/3.0                     12                    12                      0
```

Meaning The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

Verifying That MAC Limiting, MAC Move Limiting, and Persistent MAC Learning Are Working Correctly on the Switch

Purpose Verify that MAC limiting, MAC move limiting, and persistent MAC learning are working on the switch.

Action Suppose that two packets have been sent from hosts on **ge-0/0/1** and five packets from hosts on **ge-0/0/2**, with both interfaces set to a MAC limit of **4** with the default action **drop** and **ge-0/0/1** enabled for persistent MAC learning.

Display the MAC addresses learned:

```
user@switch> show ethernet-switching table
Ethernet-switching table:  7 entries, 4 learned, 2 persistent entries
  VLAN                MAC address         Type         Age    Interfaces

  employee-vlan       *                   Flood          -    All-members
  employee-vlan       00:05:85:3A:82:77   Persistent     0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:79   Persistent     0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:80   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:81   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:83   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:85   Learn          0    ge-0/0/2.0
```

Now suppose packets have been sent from two of the hosts on **ge-0/0/2** after they have been moved to other interfaces more than five times in 1 second, with **employee-vlan** set to a MAC move limit of **5** with the default action **drop**.

Display the MAC addresses in the table:

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

Ethernet-switching table:  7 entries, 2 learned, 2 persistent entries
  VLAN                MAC address         Type         Age    Interfaces

  employee-vlan       *                   Flood          -    All-members
  employee-vlan       00:05:85:3A:82:77   Persistent     0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:79   Persistent     0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:80   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:81   Learn          0    ge-0/0/2.0
  employee-vlan       *                   Flood          -    ge-0/0/2.0
  employee-vlan       *                   Flood          -    ge-0/0/2.0
```

Meaning The first sample output shows that with a MAC limit of **4** for each interface, the fifth MAC address on **ge-0/0/2** was not learned because it exceeded the MAC limit. The second sample output shows that MAC addresses for three of the hosts on **ge-/0/0/2** were not learned, because the hosts had been moved back more than five times in 1 second.

Interface ge-0/0/1.0 was enabled for persistent MAC learning, so the MAC addresses associated with this interface are of the type **persistent**.

Verifying That Allowed MAC Addresses Are Working Correctly on the Switch

Purpose Verify that allowed MAC addresses are working on the switch.

Action Display the MAC cache information after five allowed MAC addresses have been configured on interface **ge-0/0/2**:

```
user@switch> show ethernet-switching table
Ethernet-switching table:  5 entries, 4 learned
  VLAN                MAC address         Type         Age    Interfaces

  employee-vlan       00:05:85:3A:82:80   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:81   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:83   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:85   Learn          0    ge-0/0/2.0
  employee-vlan       *                   Flood          -    ge-0/0/2.0
```

Meaning Because the MAC limit value for this interface has been set to **4**, only four of the five configured allowed addresses are learned.

Related Documentation

- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 99
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 95
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 111
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 106
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 91
- *Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks*
- Configuring Port Security (CLI Procedure) on page 131
- *Configuring Port Security (J-Web Procedure)*
- *secure-access-port*
- **secure-access-port on page 212**
- **show arp inspection statistics on page 254**
- **show dhcp snooping binding on page 255**
- *show ethernet-switching table*
- *show ethernet-switching table*

Example: Configuring Storm Control to Prevent Network Outages

Using storm control can prevent problems caused by broadcast storms. You can configure storm control to rate-limit broadcast traffic and unknown unicast traffic at a specified level and to drop packets when the specified traffic level is exceeded, which prevents packets from proliferating and degrading service or causing a security issue. You can also configure the switch to shut down or temporarily disable an interface when the storm control limit is exceeded.

This example shows how to configure storm control:

NOTE: This example uses a Junos OS release that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Example: Configuring Storm Control to Prevent Network Outages*.

Requirements

This example uses the following hardware and software components:

- A switch
- Junos OS Release 11.1 or later

Overview and Topology

A traffic storm occurs when broadcast packets prompt receiving devices to broadcast packets in response. This prompts further responses, creating a snowball effect. The switch is flooded with packets, and the resulting unnecessary traffic leads to poor performance or even a complete loss of service by some clients. Storm control causes a device to monitor traffic levels and take a specified action when a specified traffic level—called the *storm control level*—is exceeded, thus preventing packets from proliferating and degrading service.

Storm control monitors the incoming broadcast traffic and unknown unicast traffic and compares it with the level that you specify. If broadcast traffic and unknown unicast traffic exceed the specified level, the switch drops packets for the controlled traffic types. On non-ELS systems, storm control is disabled by default on all interfaces. If you enable storm control, the default level is 80 percent of the available bandwidth.

This example shows how to configure the storm control level on interface **xe-0/0/0** by setting the level to a traffic rate of 5000000 Kbps, based on the total of the combined broadcast and unknown unicast streams. If broadcast traffic and unknown unicast traffic exceed these levels, the switch drops packets for the controlled traffic types.

Configuration

Step-by-Step Procedure

To configure storm control for a 10-Gigabit Ethernet interface to the equivalent of 50 percent of the available bandwidth:

- Specify the level of allowed broadcast traffic and unknown unicast traffic on a specific interface:

```
[edit ethernet-switching-options]
user@switch#  set storm-control interface xe-0/0/0 bandwidth 5000000
```

Results

Display the results of the configuration:

```
[edit ethernet-switching-options]
user@switch# show storm-control
interface xe-0/0/0 {
   bandwidth 5000000;
}
```

Related Documentation

- Understanding Storm Control on page 69
- Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure) on page 138
- action-shutdown on page 224
- interface (Storm Control) on page 228
- port-error-disable on page 208

Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks

In a DHCP starvation attack, an attacker floods an Ethernet LAN with DHCP requests from spoofed (counterfeit) MAC addresses. The switch's trusted DHCP server or servers cannot keep up with the requests and can no longer assign IP addresses and lease times to legitimate DHCP clients on the switch. Requests from those clients are either dropped or directed to a rogue DHCP server set up by the attacker.

This example describes how to configure MAC limiting, a port security feature, to protect the switch against DHCP starvation attacks:

CAUTION: Mac move limiting does not work properly on a QFX5100 switch used as a Node device in a QFabric system. Do not use this feature on a QFX5100 switch in a QFabric system.

- Requirements on page 89
- Overview and Topology on page 89
- Configuration on page 90
- Verification on page 91

Requirements

This example uses the following hardware and software components:

- One QFX3500 switch
- Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure MAC limiting, a port security feature, to mitigate DHCP starvation attacks, be sure you have:

- Connected the DHCP server to the switch.
- Configured the VLAN **employee-vlan** on the switch. See *Example: Setting Up Bridging with Multiple VLANs*.

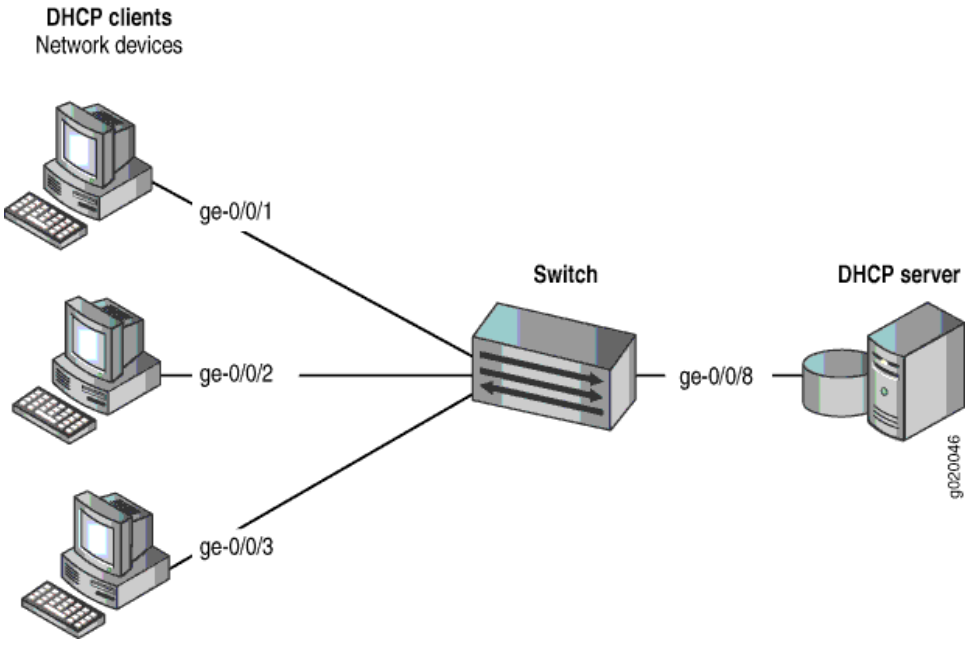
Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch against one common type of attack, a DHCP starvation attack.

This example shows how to configure port security features on a switch that is connected to a DHCP server.

The setup for this example includes the VLAN **employee-vlan** on the switch. Figure 10 on page 89 illustrates the topology for this example.

Figure 10: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 15 on page 90.

Table 15: Components of the Port Security Topology

Properties	Settings
Switch hardware	One QFX3500 switch
VLAN name and ID	**employee-vlan**
Interfaces in **employee-vlan**	**ge-0/0/1**, **ge-0/0/2**, **ge-0/0/3**, **ge-0/0/8**
Interface for DHCP server	**ge-0/0/8**

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- No MAC limit is set on any of the interfaces.
- DHCP snooping is disabled on the VLAN **employee-vlan**.
- All access interfaces are untrusted, which is the default setting.

Configuration

To configure the MAC limiting port security feature to protect the switch against DHCP starvation attacks:

CLI Quick Configuration

To quickly configure MAC limiting, copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 mac-limit 3 action drop
user@switch# set interface ge-0/0/2 mac-limit 3 action drop
```

Step-by-Step Procedure

Configure MAC limiting:

1. Configure a MAC limit of **3** on **ge-0/0/1** and specify that packets with new addresses be dropped if the limit has been exceeded on the interface:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface ge–0/0/1 mac-limit (Access Port Security) 3 action drop
   ```

2. Configure a MAC limit of **3** on **ge-0/0/2** and specify that packets with new addresses be dropped if the limit has been exceeded on the interface:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface ge-0/0/2 mac-limit 3 action drop
   ```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/1.0 {
    mac-limit 3 action drop;
}
interface ge-0/0/2.0 {
    mac-limit 3 action drop;
}
```

Verification

Confirm that the configuration is working properly.

Verifying That MAC Limiting Is Working Correctly on the Switch

Purpose Verify that MAC limiting is working on the switch.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the MAC addresses learned when DHCP requests are sent from hosts on **ge-0/0/1** and from hosts on **ge-0/0/2**, with both interfaces set to a MAC limit of **3** with the action **drop**:

```
user@switch> show ethernet-switching table
Ethernet-switching table:  7 entries, 6 learned
  VLAN           MAC address         Type         Age    Interfaces

  default        *                   Flood          -    ge-0/0/2.0
  default        00:05:85:3A:82:77   Learn          0    ge-0/0/1.0
  default        00:05:85:3A:82:79   Learn          0    ge-0/0/1.0
  default        00:05:85:3A:82:80   Learn          0    ge-0/0/1.0
  default        00:05:85:3A:82:81   Learn          0    ge-0/0/2.0
  default        00:05:85:3A:82:83   Learn          0    ge-0/0/2.0
  default        00:05:85:3A:82:85   Learn          0    ge-0/0/2.0
```

Meaning The sample output shows that with a MAC limit of **3** for each interface, the DHCP request for a fourth MAC address on **ge-0/0/2** was dropped because it exceeded the MAC limit.

Because only 3 MAC addresses can be learned on each of the two interfaces, attempted DHCP starvation attacks fail.

Related Documentation

- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Configuring MAC Limiting on page 134

Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks

In an Ethernet switching table overflow attack, an intruder sends so many requests from new MAC addresses that the Ethernet switching table fills up and then overflows, forcing the switch to broadcast all messages.

This example describes how to configure MAC limiting and allowed MAC addresses, two port security features, to protect the switch from Ethernet switching table attacks:

- Requirements on page 92
- Overview and Topology on page 92

Requirements

This example uses the following hardware and software components:

- One EX Series switch or QFX3500 switch
- Junos OS Release 9.0 or later for EX Series switches or Junos OS 12.1 or later for the QFX Series.
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure specific port security features to mitigate common access-interface attacks, be sure you have:

- Connected the DHCP server to the switch.
- Configured a VLAN on the switch. See the task for your platform:

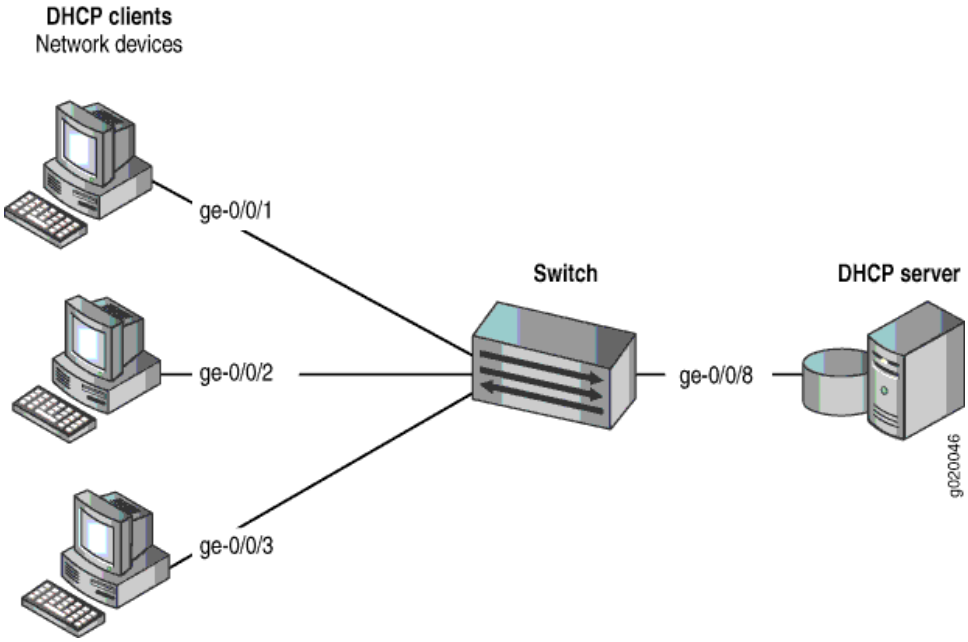
Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch from an attack on the Ethernet switching table that causes the table to overflow and thus forces the switch to broadcast all messages.

This example shows how to configure port security features on a switch connected to a DHCP server.

The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches* and *Example: Setting Up Bridging with Multiple VLANs* for the QFX Series. That procedure is not repeated here. Figure 11 on page 93 illustrates the topology for this example.

Figure 11: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 16 on page 93.

Table 16: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX Series switch or one QFX3500 switch
VLAN name and ID	**employee-vlan**, tag **20**
VLAN subnets	**192.0.2.16/28** **192.0.2.17** through **192.0.2.30** **192.0.2.31** is subnet's broadcast address
Interfaces in **employee-vlan**	**ge-0/0/1**, **ge-0/0/2**, **ge-0/0/3**, **ge-0/0/8**
Interface for DHCP server	**ge-0/0/8**

In this example, use the MAC limit feature to control the total number of MAC addresses that can be added to the Ethernet switching table for the specified interface. Use the allowed MAC addresses feature to ensure that the addresses of network devices whose network access is critical are guaranteed to be included in the Ethernet switching table.

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- No MAC limit is set on any of the interfaces.
- All access interfaces are untrusted, which is the default setting.

Configuration

To configure MAC limiting and some allowed MAC addresses to protect the switch against Ethernet switching table overflow attacks:

CLI Quick Configuration

To quickly configure MAC limiting, clear the MAC forwarding table, and configure some allowed MAC addresses, copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/1 mac-limit 4 action drop
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
exit
exit
clear ethernet-switching-table interface ge-0/0/1
```

Step-by-Step Procedure

Configure MAC limiting and some allowed MAC addresses:

1. Configure a MAC limit of **4** on **ge-0/0/1** and specify that incoming packets with different addresses be dropped once the limit is exceeded on the interface:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface ge-0/0/1 mac-limit (Access Port Security) 4 action drop
   ```

2. Clear the current entries for interface ge-0/0/1 from the MAC address forwarding table :

   ```
   user@switch# clear ethernet-switching-table interface ge-0/0/1
   ```

3. Configure the allowed MAC addresses on **ge-0/0/2**:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
   user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
   user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
   user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
   ```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/1.0 {
   mac-limit 4 action drop;
}
interface ge-0/0/2.0 {
   allowed-mac [ 00:05:85:3a:82:80 00:05:85:3a:82:81 00:05:85:3a:82:83 00:05:85
   :3a:82:85 ];
}
```

Verification

To confirm that the configuration is working properly:

- Verifying That MAC Limiting Is Working Correctly on the Switch on page 95

Verifying That MAC Limiting Is Working Correctly on the Switch

Purpose Verify that MAC limiting is working on the switch.

Action Display the MAC cache information after DHCP requests have been sent from hosts on **ge-0/0/1**, with the interface set to a MAC limit of **4** with the action **drop**, and after four allowed MAC addresses have been configured on interface **ge/0/0/2**:

```
user@switch> show ethernet-switching table
Ethernet-switching table:  5 entries, 4 learned
  VLAN              MAC address         Type         Age    Interfaces

  employee-vlan     00:05:85:3A:82:71   Learn          0    ge-0/0/1.0
  employee-vlan     00:05:85:3A:82:74   Learn          0    ge-0/0/1.0
  employee-vlan     00:05:85:3A:82:77   Learn          0    ge-0/0/1.0
  employee-vlan     00:05:85:3A:82:79   Learn          0    ge-0/0/1.0
  employee-vlan     *                   Flood          0    ge-0/0/1.0
  employee-vlan     00:05:85:3A:82:80   Learn          0    ge-0/0/2.0
  employee-vlan     00:05:85:3A:82:81   Learn          0    ge-0/0/2.0
  employee-vlan     00:05:85:3A:82:83   Learn          0    ge-0/0/2.0
  employee-vlan     00:05:85:3A:82:85   Learn          0    ge-0/0/2.0
  employee-vlan     *                   Flood          -    ge-0/0/2.0
```

Meaning The sample output shows that with a MAC limit of **4** for the interface, the DHCP request for a fifth MAC address on **ge-0/0/1** was dropped because it exceeded the MAC limit and that only the specified allowed MAC addresses have been learned on the **ge-0/0/2** interface.

Related Documentation

- Example: Configuring Basic Port Security Features on page 79
- *Configuring MAC Limiting (CLI Procedure)*
- Configuring MAC Limiting on page 134
- Configuring MAC Move Limiting (CLI Procedure) on page 136
- *Configuring MAC Limiting (J-Web Procedure)*

Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks

In a rogue DHCP server attack, an attacker has introduced a rogue server into the network, allowing it to give IP address leases to the network's DHCP clients and to assign itself as the gateway device.

This example describes how to configure a DHCP server interface as untrusted to protect the switch from a rogue DHCP server:

- Requirements on page 96
- Overview and Topology on page 96

Requirements

This example uses the following hardware and software components:

- One EX Series switch or one QFX3500 switch
- Junos OS Release 9.0 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure an untrusted DHCP server interface to mitigate rogue DHCP server attacks, be sure you have:

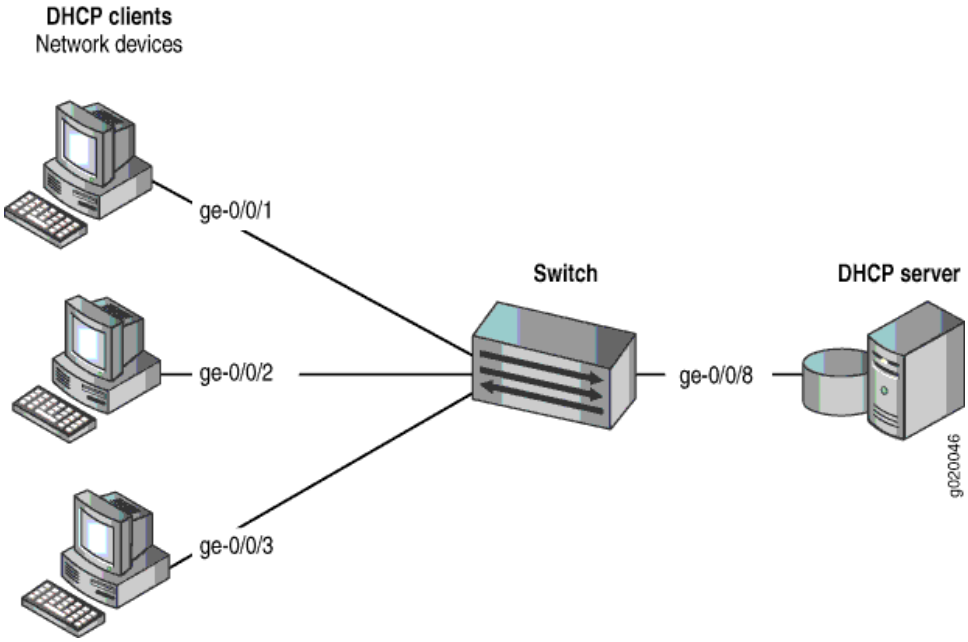
- Connected the DHCP server to the switch.
- Enabled DHCP snooping on the VLAN.
- Configured a VLAN on the switch. See the task for your platform:
  - *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
  - *Example: Setting Up Bridging with Multiple VLANs* for the QFX Series

Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch from rogue DHCP server attacks.

This example shows how to explicitly configure an untrusted interface on an EX3200-24P switch and a QFX3500 switch. Figure 12 on page 97 illustrates the topology for this example.

Figure 12: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 17 on page 97.

Table 17: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	**employee-vlan**, tag **20**
VLAN subnets	**192.0.2.16/28** **192.0.2.17** through **192.0.2.30** **192.0.2.31** is the subnet's broadcast address
Interfaces in **employee-vlan**	**ge-0/0/1**, **ge-0/0/2**, **ge-0/0/3**, **ge-0/0/8**
Interface for DHCP server	**ge-0/0/8**

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- DHCP snooping is enabled on the VLAN **employee-vlan**.
- The interface (port) where the rogue DHCP server has connected to the switch is currently trusted.

Configuration

To configure the DHCP server interface as untrusted because the interface is being used by a rogue DHCP server:

CLI Quick Configuration

To quickly set the rogue DHCP server interface as untrusted, copy the following command and paste it into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/8 no-dhcp-trusted
```

Step-by-Step Procedure

To set the DHCP server interface as untrusted:

- Specify the interface (port) from which DHCP responses are not allowed:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/8 no-dhcp-trusted
```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/8.0 {
    no-dhcp-trusted;
}
```

Verification

Confirm that the configuration is working properly.

Verifying That the DHCP Server Interface Is Untrusted

Purpose

Verify that the DHCP server is untrusted.

Action

1. Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.
2. Display the DHCP snooping information when the port on which the DHCP server connects to the switch is not trusted.

Meaning

There is no output from the command because no entries are added to the DHCP snooping database.

Related Documentation

- Example: Configuring Basic Port Security Features on page 79
- Enabling a Trusted DHCP Server (CLI Procedure) on page 144
- *Enabling a Trusted DHCP Server (J-Web Procedure)*
- *secure-access-port*
- secure-access-port on page 212
- show dhcp snooping binding on page 255

Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch

You can configure DHCP snooping, dynamic ARP inspection (DAI), and MAC limiting on the access interfaces of a switch to protect the switch and the Ethernet LAN against address spoofing and Layer 2 denial-of-service (DoS) attacks. To obtain the basic settings for these features, you can use the switch's default configuration for port security, configure the MAC limit, and enable DHCP snooping and DAI on a VLAN. You can configure these features when the DHCP server is connected to a switch that is different from the one to which the DHCP clients (network devices) are connected.

This example describes how to configure port security features on a switch whose hosts obtain IP addresses and lease times from a DHCP server connected to a second switch:

Requirements

This example uses the following hardware and software components:

- One EX Series switch or QFX3500 switch—*Switch 1* in this example.
- An additional EX Series switch or QFX3500 switch—*Switch 2* in this example. You do not configure port security on this second switch.
- Junos OS Release 9.0 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series.
- A DHCP server connected to Switch 2. You use the server to provide IP addresses to network devices connected to Switch 1.
- At least two network devices (hosts) that you connect to access interfaces on Switch 1. These devices are DHCP clients.

Before you configure DHCP snooping, DAI, and MAC limiting port security features, be sure you have:

- Connected the DHCP server to Switch 2.
- Configured a VLAN on Switch 1. See the task for your platform:
  - *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
  - *Example: Setting Up Bridging with Multiple VLANs* for the QFX Series

Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. To protect the devices from such attacks, you can configure:

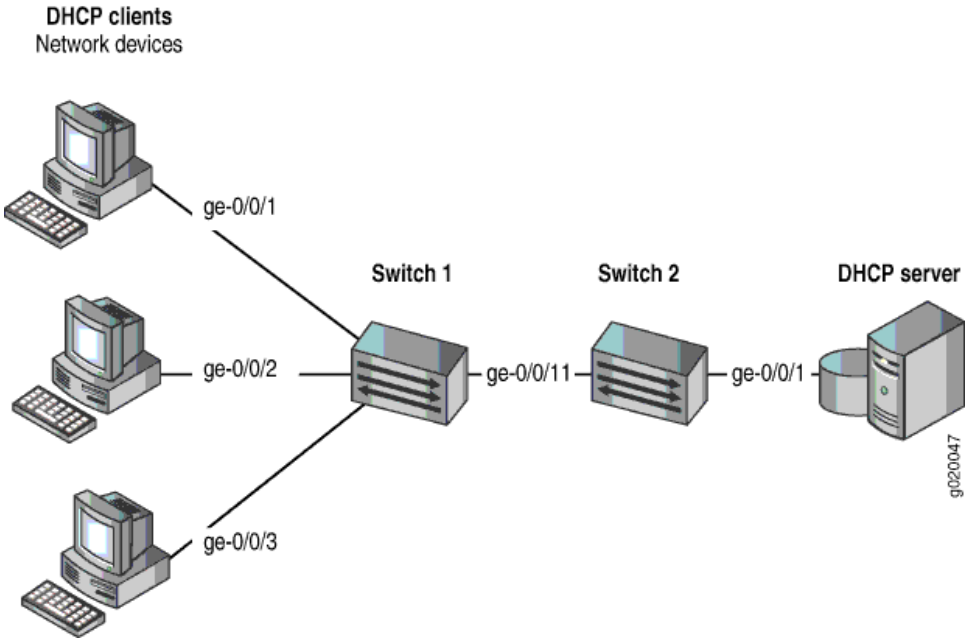
- DHCP snooping to validate DHCP server messages
- DAI to protect against ARP spoofing
- MAC limiting to constrain the number of MAC addresses the switch adds to its MAC address cache

This example shows how to configure these port security features on Switch 1. Switch 1 is connected to another switch (Switch 2), which is not configured with port security features. Switch 2 is connected to a DHCP server (see Figure 13 on page 100.) Network devices (hosts) that are connected to Switch 1 send requests for IP addresses (these network devices are DHCP clients). Those requests are transmitted from Switch 1 to Switch 2 and then to the DHCP server connected to Switch 2. Responses to the requests are transmitted along the reverse path of the one followed by the requests.

The setup for this example includes the VLAN **employee-vlan** on both switches.

Figure 13 on page 100 shows the network topology for the example.

Figure 13: Network Topology for Port Security Setup with Two Switches on the Same VLAN



The components of the topology for this example are shown in Table 18 on page 101.

Table 18: Components of Port Security Setup on Switch 1 with a DHCP Server Connected to Switch 2

Properties	Settings
Switch hardware	One EX Series switch or one QFX3500 switch (Switch 1), and an additional EX Series switch or QFX3500 switch (Switch 2)
VLAN name and ID	**employee-vlan**, tag **20**
VLAN subnets	**192.0.2.16/28** **192.0.2.17** through **192.0.2.30** **192.0.2.31** is subnet's broadcast address
Trunk interface on both switches	ge-0/0/11
Access interfaces on Switch 1	ge-0/0/1, ge-0/0/2, and ge-0/0/3
Access interface on Switch 2	ge-0/0/1
Interface for DHCP server	ge-0/0/1 on Switch 2

Switch 1 is initially configured with the default port security setup. In the default configuration on the switch:

- Secure port access is activated on the switch.
- The switch does not drop any packets, which is the default setting.
- DHCP snooping and DAI are disabled on all VLANs.
- All access interfaces are untrusted and trunk interfaces are trusted; these are the default settings.

In the configuration tasks for this example, you configure a VLAN on both switches.

In addition to configuring the VLAN, you enable DHCP snooping on Switch 1. In this example, you also enable DAI and a MAC limit of **5** on Switch 1.

Because the interface that connects Switch 2 to Switch 1 is a trunk interface, you do not need to configure this interface to be trusted. As noted above, trunk interfaces are automatically trusted, so DHCP messages coming from the DHCP server to Switch 2 and then on to Switch 1 are trusted.

Configuring a VLAN, Interfaces, and Port Security Features on Switch 1

CLI Quick Configuration

To quickly configure a VLAN, interfaces, and port security features, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans employee-vlan vlan-id 20
set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members 20
```

```
set ethernet-switching-options secure-access-port interface ge-0/0/1 mac-limit 5 action drop
set ethernet-switching-options secure-access-port vlan employee-vlan arp-inspection
set ethernet-switching-options secure-access-port vlan employee-vlan examine-dhcp
clear ethernet-switching table interface ge-0/0/1
```

Step-by-Step Procedure

To configure MAC limiting, a VLAN, and interfaces on Switch 1 and enable DAI and DHCP on the VLAN:

1. Configure the VLAN **employee-vlan** with VLAN ID **20**:

   ```
   [edit vlans]
   user@switch1# set employee-vlan vlan-id 20
   ```

2. Configure an interface on Switch 1 as a trunk interface:

   ```
   [edit interfaces]
   user@switch1# set ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
   ```

3. Associate the VLAN with interfaces ge-0/0/1, ge-0/0/2, ge-0/0/3, and ge-0/0/11:

   ```
   [edit interfaces]
   user@switch1# set ge-0/0/1 unit 0 family ethernet-switching vlan members 20
   user@switch1# set ge-0/0/2 unit 0 family ethernet-switching vlan members 20
   user@switch1# set ge-0/0/3 unit 0 family ethernet-switching vlan members 20
   user@switch1# set ge-0/0/11 unit 0 family ethernet-switching vlan members 20
   ```

4. Enable DHCP snooping on the VLAN:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch1# set vlan employee-vlan examine-dhcp
   ```

5. Enable DAI on the VLAN:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch1# set vlan employee-vlan arp-inspection
   ```

6. Configure a MAC limit of **5** on ge-0/0/1 and use the default action, **drop** (packets with new addresses are dropped if the limit is exceeded):

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch1# set interface ge-0/0/1 mac-limit 5 drop
   ```

7. Clear the existing MAC address table entries from interface ge-0/0/1:

   ```
   user@switch1# clear ethernet-switching table interface ge-0/0/1
   ```

Results

Display the results of the configuration:

```
[edit]
user@switch1# show
ethernet-switching-options {
  secure-access-port {
    interface ge-0/0/1.0{
      mac-limit 5 action drop;
    }
    vlan employee-vlan {
      arp-inspection;
      examine-dhcp;
    }
  }
}
interfaces {
  ge-0/0/1 {
    unit 0 {
      family ethernet-switching {
        vlan {
```

```
            members 20;
          }
        }
      }
    }
    ge-0/0/2 {
      unit 0 {
        family ethernet-switching {
          vlan {
            members 20;
          }
        }
      }
    }
    ge-0/0/3 {
      unit 0 {
        family ethernet-switching {
          vlan {
            port-mode trunk;
            members 20;
          }
        }
      }
    }
    ge-0/0/11 {
      unit 0 {
        family ethernet-switching {
          port-mode trunk;
          vlan {
            members 20;
          }
        }
      }
    }
  }
  vlans {
    employee-vlan {
      vlan-id 20;
    }
  }
```

Configuring a VLAN and Interfaces on Switch 2

To configure the VLAN and interfaces on Switch 2:

CLI Quick Configuration

To quickly configure the VLAN and interfaces on Switch 2, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans employee-vlan vlan-id 20
set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members 20
```

Step-by-Step Procedure

To configure the VLAN and interfaces on Switch 2:

1. Configure the VLAN **employee-vlan** with VLAN ID **20**:

```
[edit vlans]
user@switch1# set employee-vlan vlan-id 20
```

2. Configure an interface on Switch 2 as a trunk interface:

```
[edit interfaces]
user@switch2# set ge-0/0/11 unit 0 ethernet-switching port-mode trunk
```

3. Associate the VLAN with interfaces ge-0/0/1 and ge-0/0/11:

```
[edit interfaces]
user@switch2# set ge-0/0/1 unit 0 family ethernet-switching vlan members 20
user@switch2# set ge-0/0/11 unit 0 family ethernet-switching vlan members 20
```

Results Display the results of the configuration:

```
[edit]
user@switch2# show
interfaces {
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members 20;
                }
            }
        }
    }
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members 20;
                }
            }
        }
    }
}
vlans {
    employee-vlan {
        vlan-id 20;
    }
}
```

Verification

To confirm that the configuration is working properly.

- Verifying That DHCP Snooping Is Working Correctly on Switch 1 on page 104
- Verifying That DAI Is Working Correctly on Switch 1 on page 105
- Verifying That MAC Limiting Is Working Correctly on Switch 1 on page 105

Verifying That DHCP Snooping Is Working Correctly on Switch 1

Purpose Verify that DHCP snooping is working on Switch 1.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

issue the operational mode command **show dhcp snooping binding** to display the DHCP snooping information when the interface through which Switch 2 sends the DHCP server replies to clients connected to Switch 1 is trusted. The server has provided the IP addresses and leases:

```
user@switch1> show dhcp snooping binding
DHCP Snooping Information:
MAC Address         IP Address    Lease    Type     VLAN          Interface
-----------------   ----------    -----    ----     ----          ---------
00:05:85:3A:82:77    192.0.2.17    600    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:79    192.0.2.18    653    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:80    192.0.2.19    720    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:81    192.0.2.20    932    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:83    192.0.2.21   1230    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:90    192.0.2.20    932    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:3A:82:91    192.0.2.21   1230    dynamic  employee-vlan   ge-0/0/3.0
```

Meaning The output shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

Verifying That DAI Is Working Correctly on Switch 1

Purpose Verify that DAI is working on Switch 1.

Action Send some ARP requests from network devices connected to the switch.

Issue the operational mode command **show arp inspection statistics** to display the DAI information:

```
user@switch1> show arp inspection statistics
ARP inspection statistics:
Interface    Packets received  ARP inspection pass  ARP inspection failed
----------   ----------------  -------------------  ---------------------
ge-0/0/1.0                 7                    5                      2
ge-0/0/2.0                10                   10                      0
ge-0/0/3.0                18                   15                      3
```

Meaning The output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

Verifying That MAC Limiting Is Working Correctly on Switch 1

Purpose Verify that MAC limiting is working on Switch 1.

Action Issue the operational mode command **show ethernet-switching table** to display the MAC addresses that are learned when DHCP requests are sent from hosts on ge-0/0/1:

```
user@switch1> show ethernet-switching table

Ethernet-switching table:  6 entries, 5 learned
  VLAN                MAC address         Type         Age    Interfaces

  employee-vlan       00:05:85:3A:82:77   Learn          0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:79   Learn          0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:80   Learn          0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:81   Learn          0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:83   Learn          0    ge-0/0/1.0
  employee-vlan       *                   Flood          -    ge-0/0/1.0
```

Meaning The output shows that five MAC addresses have been learned for interface **ge-0/0/1**, which corresponds to the MAC limit of **5** set in the configuration. The last line of the output shows that a sixth MAC address request was dropped, as indicated by the asterisk (*) in the **MAC address** column.

Related Documentation

- Example: Configuring Basic Port Security Features on page 79
- Configuring Port Security (CLI Procedure) on page 131
- *Configuring Port Security (J-Web Procedure)*
- *secure-access-port*
- secure-access-port on page 212
- show arp inspection statistics on page 254
- show dhcp snooping binding on page 255
- *show ethernet-switching table*
- *show ethernet-switching table*

Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks

In an ARP spoofing attack, the attacker associates its own MAC address with the IP address of a network device connected to the switch. Traffic intended for that IP address is now sent to the attacker instead of being sent to the intended destination. The attacker can send faked, or “spoofed,” ARP messages on the LAN.

NOTE: When dynamic ARP inspection (DAI) is enabled, the switch logs the number of invalid ARP packets that it receives on each interface, along with the sender’s IP and MAC addresses. You can use these log messages to discover ARP spoofing on the network. ARP probe packets are not subjected to dynamic ARP inspection. The switch always forwards such packets.

This example describes how to configure DHCP snooping and dynamic ARP inspection (DAI), two port security features, to protect the switch against ARP spoofing attacks:

Requirements

This example uses the following hardware and software components:

- One EX Series switch or one QFX3500 switch
- Junos OS Release 11.4 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure DHCP snooping and DAI (two port security features) to mitigate ARP spoofing attacks, be sure you have:

- Connected the DHCP server to the switch.
- Configured a VLAN on the switch. See the task for your platform:
  - *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
  - *Example: Setting Up Bridging with Multiple VLANs* for the QFX Series

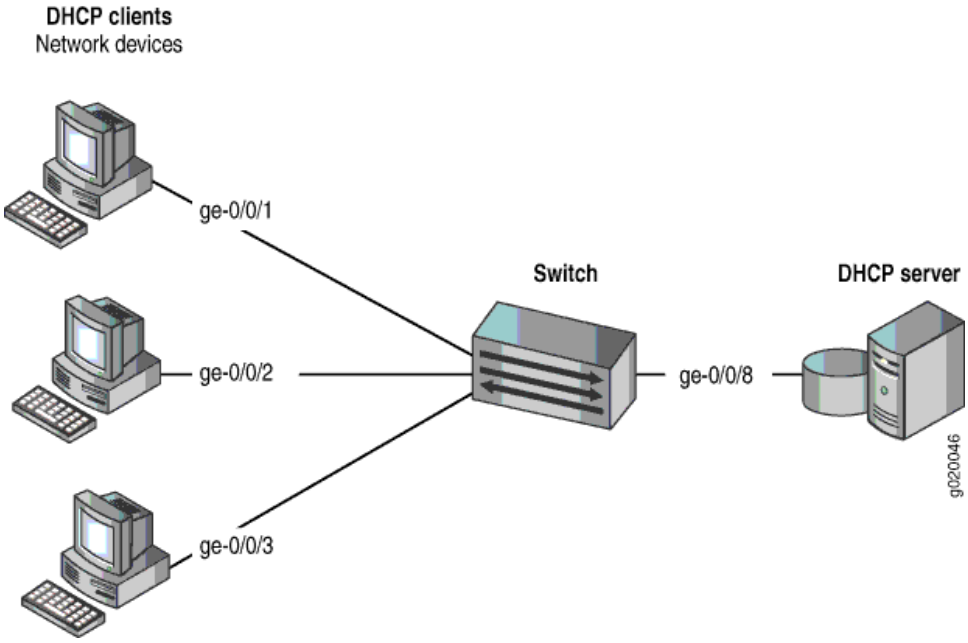
Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch against one common type of attack, an ARP spoofing attack.

In an ARP spoofing attack, the attacker sends faked ARP messages, thus creating various types of problems on the LAN—for example, the attacker might launch a man-in-the middle attack.

This example shows how to configure port security features on a switch that is connected to a DHCP server. The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches* and *Example: Setting Up Bridging with Multiple VLANs* for the QFX Series. That procedure is not repeated here.
Figure 14 on page 108 illustrates the topology for this example.

Figure 14: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 19 on page 108.

Table 19: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	**employee-vlan**, tag **20**
VLAN subnets	**192.0.2.16/28** **192.0.2.17** through **192.0.2.30** **192.0.2.31** is the subnet's broadcast address
Interfaces in **employee-vlan**	**ge-0/0/1**,**ge-0/0/2**, **ge-0/0/3**, **ge-0/0/8**
Interface for DHCP server	**ge-0/0/8**

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- DHCP snooping is disabled on the VLAN **employee-vlan**.
- All access ports are untrusted, which is the default setting.

Configuration

To configure DHCP snooping and dynamic ARP inspection (DAI) to protect the switch against ARP attacks:

CLI Quick Configuration

To quickly configure DHCP snooping and dynamic ARP inspection (DAI), copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/8 dhcp-trusted
user@switch# set vlan employee-vlan examine-dhcp
user@switch# set vlan employee-vlan arp-inspection
```

Step-by-Step Procedure

Configure DHCP snooping and dynamic ARP inspection (DAI) on the VLAN:

1. Set the **ge-0/0/8** interface as trusted:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface ge-0/0/8 dhcp-trusted
   ```

2. Enable DHCP snooping on the VLAN:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee-vlan examine-dhcp
   ```

3. Enable DAI on the VLAN:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee-vlan arp-inspection
   ```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/8.0 {
  dhcp-trusted;
}
vlan employee-vlan {
  arp-inspection;
  examine-dhcp;
}
```

Verification

Confirm that the configuration is working properly.

Verifying That DHCP Snooping Is Working Correctly on the Switch

Purpose

Verify that DHCP snooping is working on the switch.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the port on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp-snooping binding
DHCP Snooping Information:
MAC Address         IP Address    Lease    Type     VLAN            Interface
-----------------   ----------    -----    ----     ----            ---------
00:05:85:3A:82:77    192.0.2.17    600    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:79    192.0.2.18    653    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:80    192.0.2.19    720    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:3A:82:81    192.0.2.20    932    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:3A:82:83    192.0.2.21   1230    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:27:32:88    192.0.2.22   3200    dynamic  employee-vlan   ge-0/0/3.0
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

Verifying That DAI Is Working Correctly on the Switch

Purpose Verify that DAI is working on the switch.

Action Send some ARP requests from network devices connected to the switch.

Display the DAI information:

```
user@switch> show arp inspection statistics
ARP inspection statistics:
Interface        Packets received  ARP inspection pass   ARP inspection failed
---------------  ----------------  --------------------  ---------------------
ge-0/0/1.0                     7                     5                      2
ge-0/0/2.0                    10                    10                      0
ge-0/0/3.0                    12                    12                      0
```

Meaning The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

Related Documentation

- Example: Configuring Basic Port Security Features on page 79
- Enabling DHCP Snooping (CLI Procedure) on page 140
- *Enabling DHCP Snooping (J-Web Procedure)*
- Enabling Dynamic ARP Inspection (CLI Procedure) on page 142

- *Enabling Dynamic ARP Inspection (J-Web Procedure)*
- *secure-access-port*
- secure-access-port on page 212
- show arp inspection statistics on page 254
- show dhcp snooping binding on page 255

Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks

In one type of attack on the DHCP snooping database, an intruder introduces a DHCP client on an untrusted access interface with a MAC address identical to that of a client on another untrusted interface. The intruder then acquires the DHCP lease of that other client, thus changing the entries in the DHCP snooping table. Subsequently, what would have been valid ARP requests from the legitimate client are blocked.

This example describes how to configure allowed MAC addresses, a port security feature, to protect the switch from DHCP snooping database alteration attacks:

Requirements

This example uses the following hardware and software components:

- One EX Series switch or one QFX3500 switch
- Junos OS Release 11.4 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure specific port security features to mitigate common access-inteface attacks, be sure you have:

- Connected the DHCP server to the switch.
- Configured a VLAN on the switch. See the task for your platform:
  - *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
  - *Example: Setting Up Bridging with Multiple VLANs* for the QFX Series

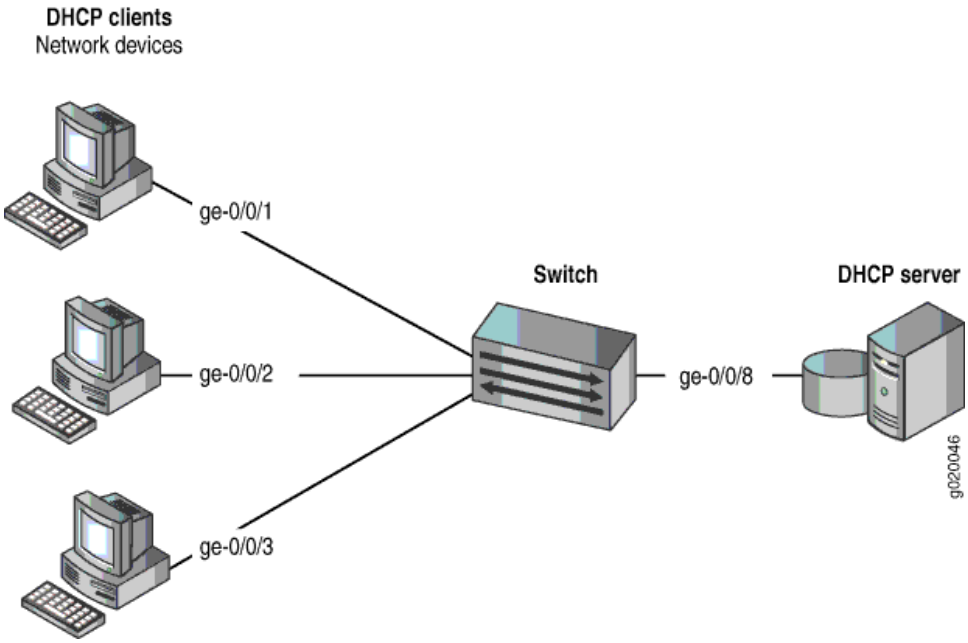
Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch from an attack on the DHCP snooping database that alters the MAC addresses assigned to some clients.

This example shows how to configure port security features on a switch that is connected to a DHCP server.

The setup for this example includes the VLAN **employee-vlan** on the switch. Figure 15 on page 112 illustrates the topology for this example.

Figure 15: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 20 on page 112.

Table 20: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	**employee-vlan**, tag **20**
VLAN subnets	**192.0.2.16/28** **192.0.2.17** through **192.0.2.30** **192.0.2.31** is the subnet's broadcast address
Interfaces in **employee-vlan**	**ge-0/0/1**, **ge-0/0/2**, **ge-0/0/3**, **ge-0/0/8**
Interface for DHCP server	**ge-0/0/8**

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- DHCP snooping is enabled on the VLAN **employee-vlan**.
- All access ports are untrusted, which is the default setting.

Configuration

To configure allowed MAC addresses to protect the switch against DHCP snooping database alteration attacks:

CLI Quick Configuration

To quickly configure some allowed MAC addresses on an interface, copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88
```

Step-by-Step Procedure

To configure some allowed MAC addresses on an interface:

Configure the five allowed MAC addresses on an interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88
```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/2.0 {
   allowed-mac [ 00:05:85:3a:82:80 00:05:85:3a:82:81 00:05:85:3a:82:83 00:05:85
   :3a:82:85 00:05:85:3a:82:88 ];
}
```

Verification

Confirm that the configuration is working properly.

- Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 113

Verifying That Allowed MAC Addresses Are Working Correctly on the Switch

Purpose

Verify that allowed MAC addresses are working on the switch.

Action Display the MAC cache information:

```
user@switch> show ethernet-switching table
Ethernet-switching table:  6 entries, 5 learned
  VLAN                MAC address         Type         Age    Interfaces

  employee-vlan       00:05:85:3A:82:80   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:81   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:83   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:85   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:88   Learn          0    ge-0/0/2.0
  employee-vlan       *                   Flood          -    ge-0/0/2.0
```

Meaning The output shows that the five MAC addresses configured as allowed MAC addresses have been learned and are displayed in the MAC cache. The last MAC address in the list, one that had not been configured as allowed, has not been added to the list of learned addresses.

Related Documentation

- Example: Configuring Basic Port Security Features on page 79
- *Configuring MAC Limiting (CLI Procedure)*
- *Configuring MAC Limiting (J-Web Procedure)*
- *secure-access-port*
- secure-access-port on page 212
- *show ethernet-switching table*
- *show ethernet-switching table*

Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.

This example describes how to configure DHCP option 82 on a switch with DHCP clients, DHCP server, and switch all on the same VLAN:

- Requirements on page 115
- Overview and Topology on page 115
- Configuration on page 116

Requirements

This example uses the following hardware and software components:

- One EX Series or QFX Series switch
- Junos OS Release 9.3 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure DHCP option 82 on the switch, be sure you have:

- Connected and configured the DHCP server.

  NOTE: **Your DHCP server must be configured to accept DHCP option 82. If it is not configured for DHCP option 82, it does not use the DHCP option 82 information in the requests sent to it when it formulates its reply messages.**

- Configured the **employee** VLAN on the switch and associated the interfaces on which the clients and the server connect to the switch with that VLAN. See the task for your platform:
  - *Configuring VLANs for EX Series Switches (CLI Procedure)*
  - *Configuring VLANs* for the QFX Series

Overview and Topology

If DHCP option 82 is enabled on the switch, then when a network device—a DHCP client—that is connected to the switch on an untrusted interface sends a DHCP request, the switch inserts information about the client's network location into the packet header of that request. The switch then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or other parameter for the client.

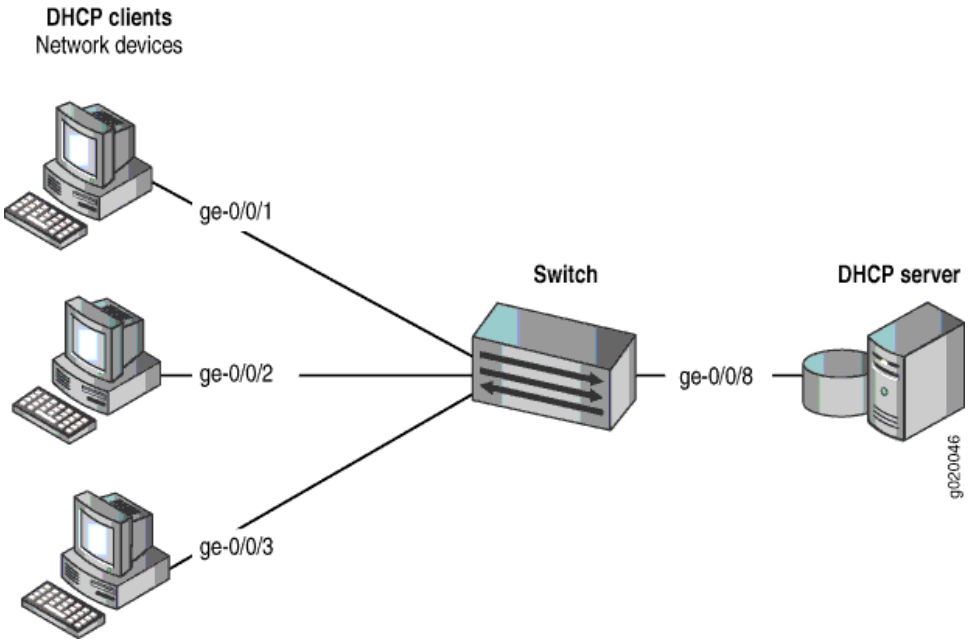
DHCP option 82 is enabled on an individual VLAN or on all VLANs on the switch.

When option 82 is enabled on the switch, then this sequence of events occurs when a DHCP client sends a DHCP request:

1. The switch receives the request and inserts the option 82 information in the packet header.
2. The switch forwards the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response back to the switch. It does not alter the option 82 information.
4. The switch strips the option 82 information from the response packet.
5. The switch forwards the response packet to the client.

Figure 16 on page 116 illustrates the topology for this example.

Figure 16: Network Topology for Configuring DHCP Option 82 on a Switch That Is on the Same VLAN as the DHCP Clients and the DHCP Server



In this example, you configure DHCP option 82 on the switch. The switch connects to the DHCP server on interface **ge-0/0/8**. The DHCP clients connect to the switch on interfaces **ge-0/0/1**, **ge-0/0/2**, and **ge-0/0/3**. The switch, server, and clients are all members of the **employee** VLAN.

Configuration

CLI Quick Configuration

To quickly configure DHCP option 82, copy the following commands and paste them into the switch terminal window:

```
set ethernet-switching-options secure-access-port vlan employee dhcp-option82
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 circuit-id prefix hostname
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 circuit-id use-vlan-id
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 remote-id
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 remote-id prefix mac
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 remote-id use-string employee-switch1
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 vendor-id
```

Step-by-Step Procedure

To configure DHCP option 82:

1. Specify DHCP option 82 for the **employee** VLAN:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee dhcp-option82
   ```

2. Configure a prefix for the circuit ID suboption (the prefix is always the hostname of the switch):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 circuit-id prefix hostname
```

3. Specify that the circuit ID suboption value contains the VLAN ID rather than the VLAN name (the default):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 circuit-id use-vlan-id
```

4. Specify that the remote ID suboption be included in the DHCP option 82 information:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id
```

5. Configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id prefix mac
```

6. Specify that the remote ID suboption value contain a character string (here, the string is **employee-switch1**):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id use-string employee-switch1
```

7. Configure a vendor ID suboption value, and use the default value. To use the default value, do not type a character string after the **vendor-id** option keyword:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 vendor-id
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
vlan employee {
  dhcp-option82 {
    circuit-id {
      prefix hostname;
      use-vlan-id;
    }
    remote-id {
      prefix mac;
      use-string employee-switch1;
    }
    vendor-id;
  }
}
```

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.
- *secure-access-port*
- secure-access-port on page 212

Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.

This example describes how to configure DHCP option 82 on a switch that is on the same VLAN with the DHCP clients but on a different VLAN from the DHCP server. in this example, the switch acts as a relay agent:

Requirements

This example uses the following hardware and software components:

- One EX4200-24P switch or one QFX3500 switch
- Junos OS Release 9.3 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure DHCP option 82 on the switch, be sure you have:

- Connected and configured the DHCP server.

  NOTE: **Your DHCP server must be configured to accept DHCP option 82. If it is not configured for DHCP option 82, it does not use the DHCP option 82 information in the requests sent to it when it formulates its reply messages.**

- Configured the **employee** VLAN on the switch and associated the interfaces on which the clients connect to the switch with that VLAN. See the task for your platform:
  - *Configuring VLANs for EX Series Switches (CLI Procedure)*
  - *Configuring VLANs* for the QFX Series
- Configured the **corporate** VLAN for the DHCP server.
- Configured the switch as a BOOTP relay agent. See *DHCP/BOOTP Relay for Switches Overview*.
- Configured the routed VLAN interface (RVI) to allow the switch to relay packets to the server and receive packets from the server. See *Configuring Routed VLAN Interfaces (CLI Procedure)* or *Configuring IRB Interfaces* for the QFX Series.

Overview and Topology

If DHCP option 82 is enabled on the switch, then when a network device—a DHCP client—that is connected to the switch on an untrusted interface sends a DHCP request, the switch inserts information about the client's network location into the packet header of that request. The switch then sends the request (in this setting, it relays the request) to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or other parameter for the client.

When option 82 is enabled on the switch, then this sequence of events occurs when a DHCP client sends a DHCP request:

1. The switch receives the request and inserts the option 82 information in the packet header.
2. The switch relays the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response back to the switch. It does not alter the option 82 information.
4. The switch strips the option 82 information from the response packet.
5. The switch forwards the response packet to the client.

In this example, you configure option 82 on the switch. The switch is configured as a BOOTP relay agent. The switch connects to the DHCP server through the routed VLAN interface (RVI) that you configured. The switch and clients are members of the **employee** VLAN. The DHCP server is a member of the **corporate** VLAN.

Configuration

To configure DHCP option 82:

CLI Quick Configuration

To quickly configure DHCP option 82, copy the following commands and paste them into the switch terminal window:

```
set forwarding-options helpers bootp dhcp-option82
set forwarding-options helpers bootp dhcp-option82 circuit-id prefix hostname
set forwarding-options helpers bootp dhcp-option82 circuit-id use-vlan-id
set forwarding-options helpers bootp dhcp-option82 remote-id
set forwarding-options helpers bootp dhcp-option82 remote-id prefix mac
set forwarding-options helpers bootp dhcp-option82 remote-id use-string employee-switch1
set forwarding-options helpers bootp dhcp-option82 vendor-id
```

Step-by-Step Procedure

To configure DHCP option 82:

1. Specify DHCP option 82 for the **employee** VLAN:

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82
   ```

2. Configure a prefix for the circuit ID suboption (the prefix is always the hostname of the switch):

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 circuit-id prefix hostname
   ```

3. Specify that the circuit ID suboption value contains the VLAN ID rather than the VLAN name (the default):

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 circuit-id use-vlan-id
```

4. Specify that the remote ID suboption be included in the DHCP option 82 information:

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id
```

5. Configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id prefix mac
```

6. Specify that the remote ID suboption value contains a character string (here, the string is **employee-switch1**):

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id use-string employee-switch1
```

7. Configure a vendor ID suboption value, and use the default value. To use the default value, do not type a character string after the **vendor-id** option keyword:

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 vendor-id
```

Results Check the results of the configuration:

```
[edit forwarding-options helpers bootp]
user@switch# show
dhcp-option82 {
    circuit-id {
        prefix hostname;
        use-vlan-id;
    }
    remote-id {
        prefix mac;
        use-string employee-switch1;
    }
    vendor-id;
}
```

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.
- *forwarding-options*

CHAPTER 7

Firewall and Policer Configuration Tasks

Configuring Firewall Filters

You can configure firewall filters in a switch to control traffic that enters switch ports or enters and exits VLANs and Layer 3 (routed) interfaces. To use a firewall filter, you must configure the filter and then apply it to a port, VLAN, or Layer 3 interface.

Configuring a Firewall Filter

To configure a firewall filter:

1. Configure the family address type, filter name, term name, and at least one match condition—for example, match on packets that contain a specific source address:

   ```
   [edit]
   user@switch#  set firewall family ethernet-switching filter ingress-port-filter term term-one from source-address 192.0.2.14
   ```

   For a firewall filter that is applied to a port or VLAN, specify the family address type **ethernet-switching**. For a firewall filter that is applied to a Layer 3 (routed) interface, specify the family address type **inet**.

   The filter and term names can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. Each filter name must be unique. A filter can contain one or more terms, and each term name must be unique within a filter.

2. Configure additional match conditions. For example, match on packets that contain a specific source port:

```
[edit firewall family ethernet-switching filter ingress-port-filter term
term-one from]
user@switch# set source-port 80
```

You can specify one or more match conditions in a single **from** statement. For a match to occur, the packet must match all the conditions in the term. The **from** statement is optional, but if included in a term, it cannot be empty. If you omit the **from** statement, all packets are considered to match.

3. If you want to apply a firewall filter to multiple interfaces and be able to see counters specific to each interface, configure the **interface-specific** option:

```
[edit firewall family ethernet-switching filter ingress-port-filter]
user@switch# set interface-specific
```

4. In each firewall filter term, specify the actions to take if the packet matches all the conditions in that term. You can specify an action and action modifiers:

   - To specify a filter action, for example, to discard packets that match the conditions of the filter term:

```
[edit firewall family ethernet-switching filter ingress-port-filter term
term-one then]
user@switch# set discard
```

     You can specify no more than one action (**accept**, **discard**, **reject**, **routing-instance**, or **vlan**) per term.

   - To specify action modifiers, for example, to count and classify packets to a forwarding class:

```
[edit firewall family ethernet-switching filter ingress-port-filter term
term-one then]
user@switch# set count counter-one
user@switch# set forwarding-class expedited-forwarding
user@switch# set loss-priority high
```

     You can specify any of the following action modifiers in a **then** statement:

     - **analyzer** ***analyzer-name***—Mirror port traffic to a specified analyzer, which you must configure at the **[ethernet-switching-options]** level.
     - **count** ***counter-name***—Count the number of packets that pass this filter term.

       NOTE: We recommend that you configure a counter for each term in a firewall filter, so that you can monitor the number of packets that match the conditions specified in each filter term.

       NOTE: On QFX3500 and QFX3600 switches, filters automatically count packets that have been dropped on ingress because of cyclic redundancy check (CRC) errors.

     - **forwarding-class** ***class***—Assign packets to a forwarding class.
     - **log**—Log the packet header information in the Routing Engine.
     - **loss-priority** ***priority***—Set the priority of dropping a packet.

- **policer** ***policer-name***—Apply rate-limiting to the traffic.
- **syslog**—Log an alert for this packet.

If you omit the **then** statement or do not specify an action, packets that match all the conditions in the **from** statement are accepted. However, you should always explicitly configure an action in the **then** statement. You can include no more than one action statement, but you can use any combination of action modifiers. For an action or action modifier to take effect, all conditions in the **from** statement must match.

NOTE: Implicit discard is also applicable to a firewall filter applied to the loopback interface, lo0.

Applying a Firewall Filter to a Port

To apply a firewall filter to an ingress port:

1. Provide a meaningful description of the firewall filter in the configuration of the port to which the filter will be applied:

   ```
   [edit]
   user@switch# set interfaces ge-0/0/6 description "filter to limit tcp traffic at trunk port for employee-vlan"
   ```

2. Apply the filter to the interface, specifying the unit number, family address type, the direction of the filter (for packets entering the port), and the filter name:

   ```
   [edit]
   user@switch# set ge-0/0/6 unit 0 family ethernet-switching filter input ingress-port-filter
   ```

   For firewall filters that are applied to ports, the family address type must be **ethernet-switching**.

NOTE: You can apply only one filter to a port for a given direction (ingress or egress).

Applying a Firewall Filter to a VLAN

To apply a firewall filter to a VLAN:

1. Provide a meaningful description of the firewall filter in the configuration of the VLAN to which the filter will be applied:

   ```
   [edit]
   user@switch# set vlans employee-vlan vlan-id 20 description "filter to block rogue devices on employee-vlan"
   ```

2. Apply firewall filters to filter packets that are entering or exiting the VLAN:

   - To apply a filter to match packets that are entering the VLAN:

     ```
     [edit]
     user@switch# set vlans employee-vlan vlan-id 20 filter input ingress-vlan-rogue-block
     ```

   - To apply a firewall filter to match packets that are exiting the VLAN:

```
[edit]
user@switch# set vlans employee-vlan vlan-id 20 filter output egress-vlan-filter
```

NOTE: You can apply only one filter to a VLAN for a given direction (ingress or egress).

Applying a Firewall Filter to a Layer 3 (Routed) Interface

To apply a firewall filter to a Layer 3 routed interface:

1. Provide a meaningful description of the firewall filter in the configuration of the interface to which the filter will be applied:

   ```
   [edit]
   user@switch# set interfaces ge-0/1/6 description "filter to count and monitor traffic on layer 3 interface"
   ```

2. You can apply firewall filters to filter packets that enter or exit a Layer 3 routed interface:

   - To apply a firewall filter to filter packets that enter a Layer 3 interface:

     ```
     [edit]
     user@switch# set interfaces ge-0/1/6 unit 0 family inet filter input ingress-router-filter
     ```

   - To apply a firewall filter to filter packets that exit a Layer 3 interface:

     ```
     [edit]
     user@switch# set interfaces ge-0/1/6 unit 0 family inet filter output egress-router-filter
     ```

     For firewall filters applied to Layer 3 routed interfaces, the family address type must be **inet**.

NOTE: You can apply only one filter to an interface for a given direction (ingress or egress).

Related Documentation

- Overview of Firewall Filters on page 3
- Firewall Filter Match Conditions and Actions on page 12
- Verifying That Firewall Filters Are Operational on page 238
- Monitoring Firewall Filter Traffic on page 235
- *Configuring Port Mirroring*

Applying Firewall Filters to Interfaces

For a firewall filter to work, you must apply it to at least one interface. To do this, include the **filter** statement when configuring a logical interface at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
```

`user@switch#` **set** *interface-name* **unit** *logical-unit-number* **family** *family-name* **filter (input | output)** *filter-name*

In the **input** statement, specify a firewall filter to be evaluated when packets are received on the interface. Input filters applied to a loopback interface affect only traffic destined for the Routing Engine.

In the **output** statement, specify a filter to be evaluated when packets exit the interface.

NOTE: When you create a loopback interface, it is important to apply an ingress filter to it so the Routing Engine is protected. We recommend that when you apply a filter to the loopback interface **lo0**, you include the **apply-groups** statement. Doing so ensures that the filter is automatically inherited on every loopback interface, including **lo0** and other loopback interfaces.

Related Documentation

- Configuring Firewall Filters on page 121

Assigning Forwarding Classes and Loss Priority

You can configure firewall filters to assign packet loss priority (PLP) and forwarding classes so that if congestion occurs, the marked packets can be dropped according to the priority you set. The valid match conditions are one or more of the six packet header fields: destination address, source address, IP protocol, source port, destination port, and DSCP. In other words, you can set the forwarding class and the PLP for each packet entering or an interface with a specific destination address, source address, IP protocol, source port, destination port, or DSCP.

NOTE: **Junos OS assigns forwarding classes and PLP on ingress only. Do not use a filter that assigns forwarding classes or PLP as an egress filter.**

When tricolor marking is enabled, a switch supports four PLP designations: **low**, **medium-low**, **medium-high**, and **high**. You can also specify any of the forwarding classes listed in Table 21 on page 126

Table 21: Unicast Forwarding Classes

Unicast Forwarding Class	For CoS Traffic Type
be	Best-effort traffic
no-loss	Guaranteed delivery for TCP traffic
fcoe	Guaranteed delivery for Fibre Channel over Ethernet (FCoE) traffic
nc	Network-control traffic

To assign forwarding classes in firewall filters:

1. Configure the family address type and filter name:

   ```
   [edit]
   user@switch# edit firewall family ethernet-switching filter ingress-filter
   ```

2. Configure the terms of the filter as appropriate, including the **forwarding-class** and **loss-priority** action modifiers. For example, each of the following terms in the filter examines various packet header fields and assigns the appropriate forwarding class and packet loss priority:

   - The term **corp-traffic** matches all IPv4 packets with a **10.1.1.0/24** source address and assigns the packets to forwarding class **no-loss** with a loss priority of **low**:

     ```
     [edit firewall family ethernet-switching filter ingress-filter]
     user@switch# set term corp-traffic from source-address 10.1.1.0/24;
     user@switch# set term corp-traffic then forwarding-class no-loss
     user@switch# set term corp-traffic then loss-priority low
     ```

   - The term **data-traffic** matches all IPv4 packets with a **10.1.2.0/24** source address and assigns the packets to forwarding class **be** (best effort) with a loss priority of **medium-high**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term data-traffic from source-address 10.1.2.0/24;
user@switch# set term data-traffic then forwarding-class be
user@switch# set term data-traffic then loss-priority medium-high
```

- Because the loss of network-generated packets can jeopardize proper network operation, the delay of these packets is preferable to discarding these packets. The term **network-traffic** assigns the packets with an IP precedence of **net-control** to forwarding class **nc** (network control) with a loss priority of **low**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term network-traffic from precedence net-control
user@switch# set term network-traffic then forwarding-class nc
user@switch# set term network-traffic then loss-priority low
```

- The last term **accept-traffic** matches any packets that did not match on any of the preceding terms and assigns the packets to forwarding class **be** with a loss priority of **high**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term accept-traffic then forwarding-class be
user@switch# set term accept-traffic then loss-priority high
```

3. Apply the filter **ingress-filter** to a port, VLAN, or Layer 3 interface. For information about applying the filter, see "Configuring Firewall Filters" on page 121. (Assigning forwarding classes and PLP is supported only on ingress filters.)

Related Documentation

- Configuring Firewall Filters on page 121
- Verifying That Firewall Filters Are Operational on page 238
- Monitoring Firewall Filter Traffic on page 235
- Overview of Policers on page 35
- *Understanding CoS Classifiers*
- *Understanding CoS Forwarding Classes*

Configuring Color-Blind Egress Policers for Medium-Low PLP

If you use color-blind mode and want to configure an egress policer that marks packets to have medium-low PLP, you must configure a single-rate two-color policer at the **[edit firewall policer *policer-name*]** hierarchy level, because color-blind mode does not support medium-low priority. For example:

1. Specify the name of the policer, the bandwidth limit in bits per second (bps) to control the traffic rate on an interface, and the maximum allowed burst size to control the amount of traffic bursting:

```
[edit]
user@switch# set firewall policer policer-name if-exceeding bandwidth-limit bytes
burst-size-limit bytes
```

2. Specify medium-low loss priority for matching packets:

```
[edit]
user@switch# set firewall policer policer-name then loss-priority medium-low;
```

3. Apply the filter to a port, VLAN, or Layer 3 interface.

Related Documentation

- Overview of Policers on page 35
- Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 41
- Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 43
- Configuring Firewall Filters on page 121
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128

Configuring Two-Color and Three-Color Policers to Control Traffic Rates

You can rate-limit traffic by configuring a policer and specifying it as an action modifier for a term in a firewall filter. By default, if you specify the same policer in multiple terms, Junos OS creates a separate policer instance for each term and applies rate limiting separately for each instance. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, each policer instance enforces a 1-Gbps limit. In this case, the total bandwidth allowed by the filter is 3 Gbps.

You can also configure a policer to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps.

NOTE: **You can include two-color policer actions on ingress firewall filters only. You can include three-color policer actions on ingress and egress filters.**

1. Configuring Two-Color Policers on page 128
2. Configuring Three-Color Policers on page 129
3. Specifying Policers in a Firewall Filter Configuration on page 129
4. Applying a Firewall Filter That Includes a Policer on page 130

Configuring Two-Color Policers

To configure a two-color policer:

1. Specify the name of the policer, the bandwidth limit to control the traffic rate on an interface, and the maximum allowed burst size to control the amount of traffic bursting:

   ```
   [edit firewall]
   user@switch# set policer policer-name <filter-specific> if-exceeding bandwidth-limit bps
   burst-size-limit bytes
   ```

   The policer name can contain letters, numbers, and hyphens (-) and can have as many as 64 characters.

   The range for the bandwidth limit is 32000 (32k) through 102,300,000,000 (102300m) bps.

To determine the value for the burst-size limit, multiply the bandwidth of the interface on which the filter is applied by the amount of time to allow a burst of traffic at that bandwidth to occur and divide the result by 8:

maximum burst size = (interface bandwidth) X (allowable time for burst) / (8 bits/byte)

The range for the burst-size limit is 1 through 2,147,450,880 bytes.

2. Specify the policer action to discard or assign a loss priority to packets that exceed the rate limits:

```
[edit firewall policer policer-name]
user@switch# set then (discard | loss-priority low | loss-priority high)
```

Configuring Three-Color Policers

To configure a three-color policer:

1. Specify the name of the policer and (optionally) whether to automatically discard packets with high loss priority (PLP):

```
[edit firewall]
user@switch# set three-color-policer policer-name
user@switch# set three-color-policer policer-name action loss-priority high then discard
```

2. Specify whether the three-color policer should be single-rate or two-rate and whether it should be color-aware or color-blind:

```
[edit firewall three-color-policer policer-name]
user@switch# set (single-rate | two-rate) (color-aware | color-blind)
```

3. For single-rate three-color policers, configure the CIR, CBS, and EBS:

```
[edit firewall three-color-policer policer-name single-rate]
user@switch# set committed-information-rate bps
user@switch# set committed-burst-size bytes
user@switch# set excess-burst-size bytes
```

4. For two-rate three-color policers, configure the CIR, CBS, PIR, and PBS:

```
[edit firewall three-color-policer policer-name single-rate]
user@switch# set committed-information-rate bps
user@switch# set committed-burst-size bytes
user@switch# set peak-information-rate bps
user@switch# set peak-burst-size bytes
```

Specifying Policers in a Firewall Filter Configuration

To use a two-color policer, configure a filter term that includes the action **policer**:

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

For example, the following commands apply a two-color policer to all packets sent from 192.0.2.0/24.

```
[edit firewall family family-name]
user@switch# set filter limit—hosts term term1 from source-address 192.0.2.0/24
user@switch# set filter limit—hosts term term1 then policer policer1
```

To use a three-color policer, configure a filter term that includes the action **three-color-policer**:

```
[edit firewall family name]
user@switch# set filter name term name from match-condition
```

```
user@switch# set filter name term name then three-color-policer (single-rate | two-rate) name
```

For example, the following commands apply a single-rate three-color policer to all packets received or sent by interface **ge-0/0/6** (depending on whether the filter is an ingress or egress filter).

```
[edit firewall family name]
user@switch# set filter srTCM term term-one from interface ge-0/0/6
user@switch# set filter srTCM term term-one then three-color-policer single-rate srTCM1-ca
```

You must specify whether the three-color policer is single-rate or two-rate, and this must match the policer itself. Otherwise, the configuration listing includes an error message indicating that the three-color policer you referenced in the filter does not exist.

Applying a Firewall Filter That Includes a Policer

A firewall filter that includes one or more policer action modifiers must be applied to a port, VLAN, or Layer 3 interface like any other filter. For information about applying firewall filters, see "Configuring Firewall Filters" on page 121.

NOTE: You can include two-color policer actions on ingress firewall filters only. You can include three-color policer actions on ingress and egress filters.

Related Documentation

- Configuring Firewall Filters on page 121
- Overview of Policers on page 35
- Verifying That Two-Color Policers Are Operational on page 246
- Verifying That Three-Color Policers Are Operational on page 246
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 127

CHAPTER 8

Port Security Configuration Tasks

Configuring Port Security (CLI Procedure)

Ethernet LANs are vulnerable to attacks such as address spoofing and Layer 2 denial of service (DoS) on network devices. Port security features such as DHCP snooping, DAI (dynamic ARP inspection), MAC limiting, MAC move limiting, and persistent MAC learning, as well as trusted DHCP server, help protect the access ports on the switch against the losses of information and productivity that can result from such attacks.

Depending on the particular feature, you can configure the port security feature either on:

- VLANs—A specific VLAN or all VLANs
- Interfaces—A specific interface or all interfaces

NOTE: If you configure one of the port security features on all VLANs or all interfaces, the switch software enables that port security feature on all VLANs and all interfaces that are not explicitly configured with other port security features.

However, if you do explicitly configure one of the port security features on a specific VLAN or on a specific interface, you must explicitly configure any additional port security features that you want to apply to that VLAN or interface. Otherwise, the switch software automatically applies the default values for the feature.

For example, if you disable DHCP snooping on all VLANs and decide to explicitly enable IP source guard only on a specific VLAN, you must also explicitly enable DHCP snooping on that specific VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

To configure port security features using the CLI:

- Enabling DHCP Snooping on page 132
- Enabling Dynamic ARP Inspection (DAI) on page 132
- Limiting Dynamic MAC Addresses on an Interface on page 133
- Enabling Persistent MAC Learning on an Interface on page 133
- Limiting MAC Address Movement on page 133
- Configuring Trusted DHCP Servers on an Interface on page 133

Enabling DHCP Snooping

You can configure DHCP snooping to allow the device to monitor DHCP messages received, ensure that hosts only use the IP addresses assigned to them, and allow access only to authorized DHCP servers.

To enable DHCP snooping:

- On a specific VLAN:

```
[edit vlans forwarding-options dhcp-security]
user@switch# set vlan default examine-dhcp
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all examine-dhcp
```

Enabling Dynamic ARP Inspection (DAI)

You can enable DAI to protect against ARP snooping. To enable DAI:

- On a single VLAN (here, the VLAN is **employee-vlan**):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan arp-inspection
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all arp-inspection
```

Limiting Dynamic MAC Addresses on an Interface

Limit the number of dynamic MAC addresses allowed on an interface and specify the action to take if the limit is exceeded—for example, set a MAC limit of **5** with an action of **drop**:

- On a single interface:

  ```
  [edit ethernet-switching-options secure-access-port]
  user@switch# set interface ge-0/0/1 mac-limit 5 action drop
  ```

- On all interfaces:

  ```
  [edit ethernet-switching-options secure-access-port]
  user@switch# set interface all mac-limit 5 action drop
  ```

You can also specify the actions **log** (do not drop the packet but generate an alarm, an SNMP trap, or a system log entry), **none** (no action), or **shutdown** (disable the interface and generate an alarm) to occur if the number of dynamic MAC addresses is exceeded.

Enabling Persistent MAC Learning on an Interface

You can configure learned MAC addresses to persist on an interface across restarts of the switch:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 persistent-learning
```

Limiting MAC Address Movement

You can limit the number of times a MAC address can move from its original interface in 1 second—for example, set a MAC move limit of **5** with an action of **drop** if the limit is exceeded:

- On a single VLAN (here, the VLAN is **employee-vlan**):

  ```
  [edit ethernet-switching-options secure-access-port]
  user@switch# set vlan employee-vlan mac-move-limit 5 action drop
  ```

- On all VLANs:

  ```
  [edit ethernet-switching-options secure-access-port]
  user@switch# set vlan all mac-move-limit 5 action drop
  ```

You can also specify the actions **log** (do not drop the packet but generate an alarm, an SNMP trap, or a system log entry), **none** (no action), or **shutdown** (disable the interface or VLAN and generate an alarm) to occur if the MAC address moves more than the specified number of times in 1 second.

Configuring Trusted DHCP Servers on an Interface

Configure a trusted DHCP server on an interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 dhcp-trusted
```

Related Documentation

- *Configuring Port Security (J-Web Procedure)*
- *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 99
- Monitoring Port Security on page 237
- Port Security Overview on page 50
- *secure-access-port*
- secure-access-port on page 212

Configuring MAC Limiting

To configure MAC limiting on a specific interface or on all interfaces:

1. To limit the number of dynamic MAC addresses, set a MAC limit of **5**.

   The action is not specified, so the switch performs the default action **drop** if the limit is exceeded:

   - On a single interface (here, the interface is **xe-0/0/1**):

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set interface xe-0/0/1 mac-limit (Access Port Security) 5
     ```

   - On all interfaces:

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set interface all mac-limit 5
     ```

   CAUTION: Do not set the MAC limit to 1. The first learned MAC address is often inserted into the forwarding database automatically. (For instance, the first MAC address inserted into the forwarding database for routed VLAN interfaces is the MAC address of the RVI. For Aggregated Ethernet bundles using LACP, the first MAC address inserted into the forwarding database in the forwarding table is the source address of the protocol packet.) The switch therefore fails to learn MAC addresses other than the automatic addresses when the MAC limit is set to 1, and this causes problems with MAC learning and forwarding.

2. To specify allowed MAC addresses:

   - On a single interface (here, the interface is **xe-0/0/2**):

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set interface xe-0/0/2 allowed-mac 00:05:85:3A:82:80
     user@switch# set interface xe-0/0/2 allowed-mac 00:05:85:3A:82:81
     user@switch# set interface xe-0/0/2 allowed-mac 00:05:85:3A:82:83
     ```

   - On all interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all allowed-mac 00:05:85:3A:82:80
user@switch# set interface all allowed-mac 00:05:85:3A:82:81
user@switch# set interface all allowed-mac 00:05:85:3A:82:83
```

Related Documentation

- Port Security Overview on page 50
- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Overview of Access Port Protection on page 47
- Verifying That MAC Limiting Is Working Correctly on page 240
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 91
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 88
- **no-allowed-mac-log on page 205**

Configuring MAC Move Limiting (CLI Procedure)

When MAC move limiting is configured, MAC address movements are tracked by the switch and, if a MAC address changes more than the configured number of times within 1 second, the changes to MAC addresses are dropped, logged, ignored, or the interface is shut down.

NOTE: Although you enable this feature on VLANs, the MAC move limitation pertains to the number of movements for each individual MAC address rather than the total number of MAC address moves in the VLAN. For example, If the MAC move limit is set to 1, the switch allows an unlimited number of MAC address movements within the VLAN as long as the same MAC address does not change more than once.

You configure MAC move limiting per VLAN, not per interface (port). In the default configuration, the number of MAC moves permitted is unlimited.

You can choose to have one of the following actions performed when the MAC move limit is exceeded:

- **drop**—Drop the packet and generate a system log entry. This is the default.
- **log**—Do not drop the packet but generate a system log entry.
- **none**—Take no action.
- **shutdown**—Disable the interfaces in the VLAN and generate a system log entry. If you have configured the switch with the **port-error-disable** statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the **clear ethernet-switching port-error** command.

To configure a MAC move limit for MAC addresses within a specific VLAN or for MAC addresses within all VLANs, using the CLI:

- On a single VLAN: To limit the number of MAC address movements that can be made by an individual MAC address within the VLAN **employee-vlan**, set a MAC move limit of **5**:

  ```
  [edit ethernet-switching-options secure-access-port]
  user@switch# set vlan employee-vlan mac-move-limit 5
  ```

  The action is not specified, so the switch performs the default action **drop** if it tracks that an individual MAC address within the **employee-vlan** has moved more than 5 times within one second.

- On all VLANs: To limit the number of MAC movements that can be made by individual MAC addresses within all VLANs, set a MAC move limit of **5**:

  ```
  [edit ethernet-switching-options secure-access-port]
  user@switch# set vlan all mac-move-limit 5
  ```

  The action is not specified, so the switch performs the default action **drop** if it tracks that an individual MAC address within any of the VLANs has moved more than 5 times within 1 second.

Related Documentation

- *Configuring MAC Move Limiting (J-Web Procedure)*
- Example: Configuring Basic Port Security Features on page 79
- Verifying That MAC Move Limiting Is Working Correctly on page 243
- Monitoring Port Security on page 237
- *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*
- *Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches*
- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- *clear ethernet-switching port-error*
- clear ethernet-switching port-error on page 252
- port-error-disable on page 208
- port-error-disable on page 208
- *secure-access-port*
- secure-access-port on page 212

Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure)

An Ethernet access interface might shut down or be disabled as a result of one of the following configurations:

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

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

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

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

NOTE: You must specify the disable timeout value—there is no default disable timeout period. If you do not specify a timeout value, you must use the clear ethernet-switching port-error command to clear the errors and restore the interfaces to service.

Related Documentation

- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Configuring MAC Limiting on page 134
- Configuring MAC Move Limiting (CLI Procedure) on page 136
- Understanding Storm Control on page 69

Configuring the none Action to Override a MAC Limit Applied to All Interfaces (CLI Procedure)

If you set a MAC limit in your port security settings to apply to all interfaces, you can override that setting for a particular interface by specifying the action **none**.

To use the **none** action to override a MAC limit setting:

1. Set the MAC limit for all interfaces—for example, a limit of **5** with action **drop**:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface all mac-limit (Access Port Security) 5 action drop
   ```

2. Change the action for one interface with this command.

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set interface xe-0/0/2 mac-limit action none
   ```

Related Documentation

- Configuring MAC Limiting on page 134
- Example: Configuring Basic Port Security Features on page 79
- Verifying That MAC Limiting Is Working Correctly on page 240
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 91
- *Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks*

Configuring Static ARP Entries

You can create static ARP table entries, which are explicit mappings between IP addresses and MAC addresses.

- To configure a static ARP entry:

```
[edit interfaces interface-name unit logical-unit-number family inet address address]
user@switch# set arp ip-address (mac | multicast-mac) mac-address
```

The IP address that you specify must be part of the subnet defined in the enclosing **address** statement.

To associate a multicast MAC address with a unicast IP address, use the **multicast-mac** statement.

Specify the MAC address as 6 hexadecimal bytes in one of the following formats: *nnnn.nnnn.nnnn* or *nn:nn:nn:nn:nn:nn*; for example, **0011.2233.4455** or **00:11:22:33:44:55**.

Related Documentation

- Understanding Static ARP Entries on page 67
- *arp*

Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure)

You can add static (fixed) IP addresses and bind them to fixed MAC addresses in the DHCP snooping database. These bindings are labeled as “static” in the database, while those bindings that have been added through the process of DHCP snooping are labeled “dynamic.”

To configure a static IP address/MAC address binding in the DHCP snooping database (replace **ge-0/0/2**, **10.0.10.12**, **data-vlan**, and **00:05:85:3A:82:80** with values for your configuration):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/2 static-ip 10.0.10.12 vlan data-vlan mac 00:05:85:3A:82:80
```

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Related Documentation

- Verifying That DHCP Snooping Is Working Correctly on page 239
- Understanding DHCP Snooping for Port Security on page 52
- *secure-access-port*
- **secure-access-port on page 212**

Enabling DHCP Snooping (CLI Procedure)

DHCP snooping allows the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. It builds and maintains a database of valid IP-address/MAC-address (IP-MAC) bindings called the DHCP snooping database.

NOTE: If you configure DHCP snooping for all VLANs and you enable a different port security feature on a specific VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

This topic describes:

- Enabling DHCP Snooping on page 141
- Applying CoS Forwarding Classes to Prioritize Snooped Packets on page 141

Enabling DHCP Snooping

You configure DHCP snooping per VLAN, not per interface (port). By default, DHCP snooping is disabled for all VLANs. You can enable DHCP snooping on all VLANs or on specific VLANs.

To enable DHCP snooping on a VLAN or all VLANs:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan vlan-name examine-dhcp
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all examine-dhcp
```

TIP: By default, the IP-MAC bindings are lost when the switch is rebooted and DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the **dhcp-snooping-file** statement to store the database file either locally or remotely.

TIP: For private VLANs (PVLANs), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from PVLAN trunk ports are not snooped.

Applying CoS Forwarding Classes to Prioritize Snooped Packets

On EX Series switches you might need to use class of service (CoS) to protect packets from critical applications from being dropped during periods of network congestion and delay and you might also need the port security features of DHCP snooping on the same ports through which those critical packets are entering and leaving.

NOTE: This is not supported on the QFX Series switch.

To apply CoS forwarding classes and queues to snooped packets:

1. Create a user-defined forwarding class to be used for prioritizing snooped packets:

```
[edit class-of-service]
user@switch# set forwarding-classes class class-name queue queue-number
```

2. Enable DHCP snooping on a specific VLAN or on all VLANs and apply the desired forwarding class on the snooped packets:

   - On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan vlan-name examine-dhcp forwarding-class class-name
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all examine-dhcp forwarding-class class-name
```

Related Documentation

- *Enabling DHCP Snooping (J-Web Procedure)*
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 99
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 106
- *Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic*
- Verifying That DHCP Snooping Is Working Correctly on page 239
- Monitoring Port Security on page 237
- Understanding DHCP Snooping for Port Security on page 52
- *class-of-service*
- *secure-access-port*
- secure-access-port on page 212

Enabling Dynamic ARP Inspection (CLI Procedure)

Dynamic ARP inspection (DAI) protects switches against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP cache poisoning.

This topic describes:

- Enabling DAI on page 143
- Applying CoS Forwarding Classes to Prioritize Inspected Packets on page 143

Enabling DAI

You configure DAI for each VLAN, not for each interface (port). By default, DAI is disabled for all VLANs.

To enable DAI on a VLAN or all VLANs:

- On a single VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name arp-inspection
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all arp-inspection
```

Applying CoS Forwarding Classes to Prioritize Inspected Packets

You might need to use class of service (CoS) to protect packets from critical applications from being dropped during periods of network congestion and delay and you might also need the port security features of DHCP snooping on the same ports through which those critical packets are entering and leaving.

To apply CoS forwarding classes and queues to DAI packets:

1. Create a user-defined forwarding class to be used for prioritizing DAI packets:

```
[edit class-of-service]
user@switch# set forwarding-classes class class-name queue queue-number
```

2. Enable DAI on a specific VLAN or on all VLANs and apply the desired forwarding class on the DAI packets:

   - On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan vlan-name arp-inspection forwarding-class class-name
```

   - On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all arp-inspection forwarding-class class-name
```

Related Documentation

- *Enabling Dynamic ARP Inspection (J-Web Procedure)*
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 99
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 106
- *Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic*
- Verifying That DAI Is Working Correctly on page 239
- Monitoring Port Security on page 237

- Understanding DAI for Port Security on page 59
- Understanding DAI for Port Security on page 59
- *class-of-service*
- *secure-access-port*
- secure-access-port on page 212

Enabling a Trusted DHCP Server (CLI Procedure)

You can configure any interface on a switch that connects to a DHCP server as a trusted interface (port). Configuring a DHCP server on a trusted interface protects against rogue DHCP servers sending leases.

You configure a trusted DHCP server on an interface, not on a VLAN. By default, all access interfaces are untrusted, and all trunk interfaces are trusted.

To configure a trusted interface for a DHCP server by using the CLI (here, the interface is **ge-0/0/8**):

```
[edit ethernet-switching-options secure-access port]
user@switch# set interface ge-0/0/8 dhcp-trusted
```

Related Documentation

- *Enabling a Trusted DHCP Server (J-Web Procedure)*
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 95
- Verifying That a Trusted DHCP Server Is Working Correctly on page 245
- Monitoring Port Security on page 237
- Understanding Trusted DHCP Servers for Port Security on page 64
- *secure-access-port*
- secure-access-port on page 212

Enabling a Trusted Port for DHCP

By default, all access ports are untrusted and all trunk ports are trusted with regard to DHCP. Trusted ports allow DHCP servers to provide IP addresses and other information to requesting devices. Untrusted ports drop traffic from DHCP servers to prevent unauthorized servers from providing any configuration information to clients.

If you attach a DHCP server to an access port, you must configure it as trusted. You configure a trusted DHCP server on an interface, not on a VLAN.

NOTE: **Before you attach a DHCP server to a trusted access port, ensure that the server is physically secure—that is, that access to the server is monitored and controlled.**

- To configure a trusted interface for a DHCP server by using the CLI (here, the interface is **xe-0/0/8**):

```
[edit ethernet-switching-options secure-access port]
user@switch# set interface xe-0/0/8 dhcp-trusted
```

Related Documentation

- *Enabling a Trusted DHCP Server (J-Web Procedure)*
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 95
- Verifying That a Trusted DHCP Server Is Working Correctly on page 245
- Monitoring Port Security on page 237
- Understanding Trusted and Untrusted Ports on page 63

Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.

You can configure the DHCP option 82 feature in two topologies:

- The switch, DHCP clients, and DHCP server are all on the same VLAN. The switch forwards the clients' requests to the server and forwards the server's replies to the clients. This topic describes this configuration.
- The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as routed VLAN interfaces, or RVIs. The switch relays the clients' requests to the server and then forwards the server's replies to the clients. This configuration is described in "Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)" on page 149.

Before you configure DHCP option 82 on the switch, perform these tasks:

- Connect and configure the DHCP server.

  NOTE: Your DHCP server must be configured to accept DHCP option 82. If the server is not configured for DHCP option 82, the server does not use the DHCP option 82 information in the requests sent to it when it formulates its reply messages.

- Configure a VLAN on the switch and associate the interfaces on which the clients and the server connect to the switch with that VLAN.

To configure DHCP option 82:

NOTE: Replace values displayed in italics with values for your configuration.

1. Specify DHCP option 82 for all VLANs associated with the switch or for a specified VLAN. (You can also configure the feature for a VLAN range.)

   - On a specific VLAN:

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set vlan employee dhcp-option82
     ```

   - On all VLANs:

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set vlan all dhcp-option82
     ```

     The remaining steps are optional.

2. To configure a prefix for the circuit ID suboption (the prefix is always the hostname of the switch):

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee dhcp-option82 circuit-id prefix hostname
   ```

3. To specify that the circuit ID suboption value should contain the interface description rather than the interface name (the default):

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee dhcp-option82 circuit-id use-interface-description
   ```

4. To specify that the circuit ID suboption value should contain the VLAN ID rather than the VLAN name (the default):

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee dhcp-option82 circuit-id use-vlan-id
   ```

5. To specify that the remote ID suboption be included in the DHCP option 82 information:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee dhcp-option82 remote-id
   ```

6. To configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee dhcp-option82 remote-id prefix mac
   ```

7. To specify that the prefix for the remote ID suboption be the hostname of the switch rather than the MAC address of the switch (the default):

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee dhcp-option82 remote-id prefix hostname
   ```

8. To specify that the remote ID suboption value should contain the interface description:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee dhcp-option82 remote-id use-interface-description
   ```

9. To specify that the remote ID suboption value should contain a character string:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan employee dhcp-option82 remote-id use-string mystring
   ```

10. To configure a vendor ID suboption and use the default value (the default value is **Juniper**), do not type a character string after the **vendor-id** option keyword:

    ```
    [edit ethernet-switching-options secure-access-port]
    ```

```
user@switch# set vlan employee dhcp-option82 vendor-id
```

11. To specify that the vendor ID suboption value should contain a character string value that you specify rather than **Juniper** (the default):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 vendor-id mystring
```

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- *secure-access-port*
- secure-access-port on page 212
- *Understanding DHCP Option 82 for Port Security on EX Series Switches*
- Understanding DHCP Option 82 for Port Security on page 64
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)

You can use DHCP option 82, also known as the DHCP relay agent information option, to help switches against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.

You can configure the DHCP option 82 feature in two topologies:

- The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as routed VLAN interfaces, or RVIs. The switch relays the clients' requests to the server and then forwards the server's replies to the clients. This topic describes this configuration. The configuration for this topology is the same regardless of whether your switch is running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style or not.
- The switch, DHCP clients, and DHCP server are all on the same VLAN. The switch forwards the clients' requests to the server and forwards the server's replies to the clients. This configuration for this topology differs if your switch is running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style.
  - If your switch is running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. see *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*.
  - If your switch is running Junos OS for EX Series switches without support for ELS, see "Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)" on page 146.

Before you configure DHCP option 82 on the switch, perform these tasks:

- Connect and configure the DHCP server.

  NOTE: **Your DHCP server must be configured to accept DHCP option 82. If the server is not configured for DHCP option 82, the server does not use the DHCP option 82 information in the requests sent to it when it formulates its reply messages.**

- Configure the VLAN on the switch and associate the interfaces on which the clients connect to the switch with that VLAN.

- Configure the routed VLAN interface (RVI) to allow the switch to relay packets to the server and receive packets from the server. See *Configuring Routed VLAN Interfaces (CLI Procedure)* or *Configuring IRB Interfaces* for the QFX Series.
- Configure the switch as a BOOTP relay agent. See *DHCP/BOOTP Relay for Switches Overview*.

To configure DHCP option 82:

NOTE: Replace values displayed in italics with values for your configuration.

1. Specify DHCP option 82 for the BOOTP server:
   - On all interfaces that connect to the server:

     ```
     [edit forwarding-options helpers bootp]
     user@switch# set dhcp-option82
     ```
   - On a specific interface that connects to the server:

     ```
     [edit forwarding-options helpers bootp]
     user@switch# set interface ge-0/0/10 dhcp-option82
     ```

     The remaining steps are optional. They show configurations for all interfaces; include the specific interface designation to configure any of the following options on a specific interface:
2. To configure a prefix for the circuit ID suboption (the prefix is always the hostname of the switch):

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 circuit-id prefix hostname
   ```
3. To specify that the circuit ID suboption value should contain the interface description rather than the interface name (the default):

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 circuit-id use-interface-description
   ```
4. To specify that the circuit ID suboption value should contain the VLAN ID rather than the VLAN name (the default):

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 circuit-id use-vlan-id
   ```
5. To specify that the remote ID suboption be included in the DHCP option 82 information:

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 remote-id
   ```
6. To configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 remote-id prefix mac
   ```
7. To specify that the prefix for the remote ID suboption be the hostname of the switch rather than the MAC address of the switch (the default):

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 remote-id prefix hostname
   ```
8. To specify that the remote ID suboption value should contain the interface description:

   ```
   [edit forwarding-options helpers bootp]
   ```

```
user@switch# set dhcp-option82 remote-id use-interface-description
```

9. To specify that the remote ID suboption value should contain a character string:

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id use-string mystring
```

10. To configure a vendor ID suboption and use the default value (the default value is **Juniper**), do not type a character string after the **vendor-id** option keyword:

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 vendor-id
```

11. To specify that the vendor ID suboption value contains a character string value that you specify rather than **Juniper** (the default):

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 vendor-id mystring
```

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- *[edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches*
- *Understanding DHCP Option 82 for Port Security on EX Series Switches*
- Understanding DHCP Option 82 for Port Security on page 64
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

CHAPTER 9

Configuration Statements for Firewall Filters

family

Syntax

```
family family-name {
  filter filter-name {
    interface-specific;
    term term-name {
      from {
        match-conditions;
      }
      then {
        action;
        action-modifiers;
      }
    }
  }
}
```

Hierarchy Level [edit firewall]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the fields a firewall filter can match on.

Options *family-name*—Type of addressing protocol:

- **ethernet-switching**—Filter Layer 2 Ethernet packets and Layer 3 (IP) packets (allows some Layer 3 filtering).
- **inet**—Filter Layer 3 IPv4 packets (provides additional Layer 3 filter options).
- **inet6**—Filter Layer 3 IPv6 packets (provides additional Layer 3 filter options).
- **mpls**—Filter multiprotocol label switched packets.

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

- Firewall Filter Match Conditions and Actions on page 12
- Configuring Firewall Filters on page 121
- Overview of Firewall Filters on page 3

filter

Syntax

```
filter filter-name {
  interface-specific;
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
      action-modifiers;
    }
  }
}
```

Hierarchy Level [edit firewall family *family-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure firewall filters.

Options

filter-name—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.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Firewall Filter Match Conditions and Actions on page 12
- Configuring Firewall Filters on page 121
- Overview of Firewall Filters on page 3

filter (Layer 2 and Layer 3 Interfaces)

Syntax filter (input | output) *filter-name*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Apply a firewall filter to traffic transiting a port or Layer 3 interface.

Default All incoming traffic is accepted unmodified on the port or Layer 3 interface, and all outgoing traffic is sent unmodified from the port or Layer 3 interface.

Options ***filter-name***—Name of a firewall filter defined at the **[edit firewall family *family-name* filter]** hierarchy level.

input—Apply a firewall filter to traffic entering the port or Layer 3 interface.

output—Apply a firewall filter to traffic exiting the port or Layer 3 interface.

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

Related Documentation

- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Firewall Filters on page 121
- Overview of Firewall Filters on page 3

filter (VLANs)

Syntax filter (input | output) *filter-name*;

Hierarchy Level [edit vlans *vlan-name*]
[edit vlans *vlan-name* forwarding-options]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Apply a firewall filter to traffic ingressing or egressing a VLAN.

Default All incoming traffic is accepted unmodified to a VLAN, and all outgoing traffic is sent unmodified from a VLAN.

Options ***filter-name***—Name of a firewall filter defined at the **[edit firewall family *family-name* filter]** hierarchy level.

input—Apply a firewall filter to VLAN ingress traffic.

output—Apply a firewall filter to VLAN egress traffic.

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

Related Documentation

- Configuring Firewall Filters on page 121
- Overview of Firewall Filters on page 3

firewall

Syntax

```
firewall {
  family family-name {
    filter filter-name {
      interface-specific;
      term term-name {
        from {
          match-conditions;
        }
        then {
          action;
          action-modifiers;
        }
      }
    }
  }
  policer policer-name {
    filter-specific;
    if-exceeding {
      bandwidth-limit bps;
      burst-size-limit bytes;
    }
    then {
      policer-action;
    }
  }
  three-color-policer policer-name {
    action {
      loss-priority high then discard;
    }
    single-rate {
      (color-aware | color-blind);
      committed-information-rate bps;
      committed-burst-size bytes;
      excess-burst-size bytes;
    }
    two-rate {
      (color-aware | color-blind);
      committed-information-rate bps;
      committed-burst-size bytes;
      peak-information-rate bps;
      peak-burst-size bytes;
    }
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure firewall filters and policers.

The remaining statements are explained separately.

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

Related Documentation
- Firewall Filter Match Conditions and Actions on page 12
- Configuring Firewall Filters on page 121
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Firewall Filters on page 3

from

Syntax
```
from {
  match-conditions;
}
```

Hierarchy Level
[edit **firewall family** *family-name* **filter** *filter-name* **term** *term-name*]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Match packet fields to values specified in a match condition. If the **from** statement is not included in a firewall filter configuration, all packets are considered to match and the actions and action modifiers in the **then** statement are implemented.

Options
match-conditions—Conditions that define the values or fields that the incoming or outgoing packets must contain for a match. You can specify one or more match conditions. If you specify more than one, they all must match for a match to occur and for the action in the **then** statement to be implemented.

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

Related Documentation
- Firewall Filter Match Conditions and Actions on page 12
- Configuring Firewall Filters on page 121
- Understanding Firewall Filter Match Conditions on page 8

interface-specific

Syntax interface-specific;

Hierarchy Level [edit firewall family *family-name* filter *filter-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure separate counters for each interface to which a filter is applied.

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

Related Documentation

- Firewall Filter Match Conditions and Actions on page 12
- Configuring Firewall Filters on page 121
- Overview of Firewall Filters on page 3

term

Syntax

```
term term-name {
  from {
    match-conditions;
  }
  then {
    action;
    action-modifiers;
  }
}
```

Hierarchy Level [edit firewall family *family-name* filter *filter-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Define a firewall filter term.

Options *term-name*—Name that identifies the term. 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.

The remaining statements are explained separately.

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

Related Documentation

- Firewall Filter Match Conditions and Actions on page 12
- Configuring Firewall Filters on page 121
- Overview of Firewall Filters on page 3

then (Filters)

Syntax

```
then {
  action;
  action-modifiers;
}
```

Hierarchy Level [edit firewall family *family-name* filter *filter-name* term *term-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure a firewall filter action.

Options

action—Actions to accept, discard, or forward packets that match all conditions specified in a filter term.

action-modifiers—Additional actions to analyze, classify, count, or police packets that match all conditions specified in a filter term.

Required Privilege Level

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

Related Documentation

- Firewall Filter Match Conditions and Actions on page 12
- Configuring Firewall Filters on page 121
- Understanding Firewall Filter Match Conditions on page 8

CHAPTER 10

Configuration Statements for Policers

action

Syntax

```
action {
  loss-priority high then discard;
}
```

Hierarchy Level [edit firewall three-color-policer *name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Discard traffic on a logical interface using tricolor marking policing.

Options The statements are explained separately.

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

bandwidth-limit

Syntax bandwidth-limit *bps*;

Hierarchy Level [edit firewall policer *policer-name* if-exceeding]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify the traffic rate in bits per second.

Options ***bps***—Traffic rate in bits per second. Specify *bps* as a decimal value or as a decimal number followed by one of the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 32000 bps (32 Kbps) through 10,000,000,000 bps (10 Gbps)

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

burst-size-limit

Syntax burst-size-limit *bytes*;

Hierarchy Level [edit firewall policer *policer-name* if-exceeding]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify the maximum allowed burst size to control the amount of traffic bursting.

Options ***bytes***—Decimal value or a decimal number followed by k (thousand), m (million), or g (giga).

Range: 1 through 2,147,450,880 bytes (2147 MB)

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

color-aware

Syntax color-aware;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate],
[edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the way preclassified packets are metered. In color-aware mode, the switch can assign a higher packet-loss priority, but cannot assign a lower packet loss priority (PLP). For example, suppose an upstream device assigns medium-high PLP to a packet because the packet exceeded its committed information rate (CIR). The switch cannot change the PLP to low even if the packet conforms to the configured CIR of the appropriate interface. On the other hand, if an upstream device assigns low PLP to a packet but the packet exceeds the CIR and committed burst size (CBS) of the switch interface, the switch can increase the PLP to medium-high.

Default If you omit the **color-aware** statement, the default behavior is color-aware mode.

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

Related Documentation

- Overview of Policers on page 35
- Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 41
- Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 43
- color-blind on page 167

color-blind

Syntax color-blind;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate],
[edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the way preclassified packets are metered. In color-blind mode, the switch ignores any preclassification of packets and can assign a higher or lower packet loss priority (PLP). For example, suppose an upstream device assigns medium-high PLP to a packet because the packet exceeded the CIR on the upstream device. The switch can change the PLP to low if the packet conforms to the CIR of the appropriate interface.

Default If you omit the **color-blind** statement, the default behavior is color-aware mode.

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

Related Documentation

- Overview of Policers on page 35
- Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 41
- Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 43
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 127
- color-aware on page 166

committed-burst-size

Syntax committed-burst-size *bytes*;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate],
[edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum number of bytes allowed for incoming traffic to burst above the committed information rate and still be marked with low packet loss priority (green).

NOTE: When you include the **committed-burst-size** statement in the configuration, you must also include the **committed-information-rate** statement at the same hierarchy level.

Options ***bytes***—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 512 bytes through 268435456 bytes (268 MB)

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

committed-information-rate

Syntax committed-information-rate *bits-per-second*;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate],
[edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the guaranteed bandwidth under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green).

NOTE: When you include the **committed-information-rate** statement in the configuration, you must also include the **committed-burst-size** statement at the same hierarchy level.

Options ***bits-per-second***—Number of bits per second. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 32,000 bps through 10,000,000,000 bps (10 gbps)

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

excess-burst-size

Syntax excess-burst-size *bytes*;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum number of bytes allowed for incoming traffic to burst above the committed information rate and still be marked with medium-high packet loss priority (yellow). Packets that exceed the excess burst size (EBS) are marked with high packet loss priority (red).

NOTE: When you include the **excess-burst-size** statement in the configuration, you must also include the **committed-burst-size** and **committed-information-rate** statements at the same hierarchy level.

Options ***bytes***—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 512 bytes through 268435456 bytes (268 MB)

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

filter-specific

Syntax filter-specific;

Hierarchy Level [edit firewall policer *policer-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure a policer to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. If you use a filter-specific policer in multiple terms, both of the following are true:

- Traffic is policed at the aggregate rate. For example, if you create a policer that has a bandwidth limit of 100 Mbps and use the policer in two terms, the total allowed bandwidth for both terms is 100 Mbps—not 100 Mbps for each term.
- The implicit counter counts all the packets are that matched by any of the terms. For example, if you reference the same filter-specific policer in term1 and term2, and term1 matches 1000 packets and term2 matches 500 packets, the implicit counter shows 1500 matches for the policer.

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

firewall

Syntax

```
firewall {
  family family-name {
    filter filter-name {
      interface-specific;
      term term-name {
        from {
          match-conditions;
        }
        then {
          action;
          action-modifiers;
        }
      }
    }
  }
  policer policer-name {
    filter-specific;
    if-exceeding {
      bandwidth-limit bps;
      burst-size-limit bytes;
    }
    then {
      policer-action;
    }
  }
  three-color-policer policer-name {
    action {
      loss-priority high then discard;
    }
    single-rate {
      (color-aware | color-blind);
      committed-information-rate bps;
      committed-burst-size bytes;
      excess-burst-size bytes;
    }
    two-rate {
      (color-aware | color-blind);
      committed-information-rate bps;
      committed-burst-size bytes;
      peak-information-rate bps;
      peak-burst-size bytes;
    }
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure firewall filters and policers.

The remaining statements are explained separately.

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

Related Documentation
- Firewall Filter Match Conditions and Actions on page 12
- Configuring Firewall Filters on page 121
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Firewall Filters on page 3

if-exceeding

Syntax
```
if-exceeding {
    bandwidth-limit bps;
    burst-size-limit bytes;
}
```

Hierarchy Level
[edit firewall policer *policer-name*]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure policer rate limits.

The remaining statements are explained separately.

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

Related Documentation
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

loss-priority high then discard (Three-Color Policer)

Syntax loss-priority high then discard;

Hierarchy Level [edit firewall three-color-policer *policer-name* action]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description For packets with high loss priority, discard the packets. The loss priority setting is not configurable. Include this statement if you do not want the switch to forward packets that have high packet-loss priority.

For single-rate three-color policers, Junos OS assigns high loss priority to packets that exceed the committed information rate and the excess burst size.

For two-rate three-color policers, Junos OS assigns high loss priority to packets that exceed the peak information rate and the peak burst size.

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

peak-burst-size

Syntax peak-burst-size *bytes*;

Hierarchy Level [edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red).

NOTE: When you include the peak-burst-size statement in the configuration, you must also include the committed-burst-size and peak-information-rate statements at the same hierarchy level.

Options *bytes*—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 1500 bytes through 100,000,000,000 bytes (100 GB)

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

peak-information-rate

Syntax peak-information-rate *bits-per-second*;

Hierarchy Level [edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum achievable rate. Packets that exceed the committed information rate (CIR) but are below the peak information rate (PIR) are marked with medium-high packet loss priority (yellow). Packets that exceed the PIR are marked with high packet loss priority (red). You can configure a discard action for packets that exceed the PIR.

NOTE: When you include the peak-information-rate statement in the configuration, you must also include the committed-information-rate and peak-burst-size statements at the same hierarchy level.

Options ***bits-per-second***—Number of bits per second. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 32,000 bps through 10,000,000,000 bps (10 gbps)

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

policer

Syntax

```
policer policer-name {
  filter-specific;
  if-exceeding {
    bandwidth-limit bps;
    burst-size-limit bytes;
  }
  then {
    policer-action;
  }
}
```

Hierarchy Level [edit firewall]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure policer rate limits and actions. To activate a policer, you must include the **policer** action modifier in the **then** statement in a firewall filter term.

Each policer that you configure includes an implicit counter that counts the number of packets that exceed the rate limits that are specified for the policer. If you use the same policer in multiple terms—either within the same filter or across filters—the policer's implicit counter is used to count packets that are policed in all of these terms. If you want to obtain separate packet counts for each term, use these approaches:

- Configure a unique policer for each term.
- Configure only one policer, but use a unique, explicit counter in each term.

Options ***policer-name***—Name that identifies the policer. The name can contain letters, numbers, hyphens (-), and can be up to 64 characters long.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Configuring Firewall Filters on page 121
- Overview of Policers on page 35

single-rate

Syntax

```
single-rate {
  (color-aware | color-blind);
  committed-information-rate bps;
  committed-burst-size bytes;
  excess-burst-size bytes;
}
```

Hierarchy Level [edit firewall three-color-policer *policer-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure a single-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), and excess burst size (EBS).

Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but are within the EBS are assigned medium-high loss priority (yellow). Packets that exceed the EBS are assigned high loss priority (red).

Green and yellow packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.

The remaining statements are explained separately.

Options ***policer-name***—Name of the three-color policer. Use this name when you apply the policer to an interface.

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

then (Policers)

Syntax

```
then {
  policer-action;
}
```

Hierarchy Level [edit firewall policer *policer-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure a policer action.

Options ***policer-action***—Allowed policer actions are **discard**, **loss-priority high**, and **loss-priority low**. **discard** causes the system to drop traffic that exceeds the rate limits defined by the policer. Use **loss-priority high** to allow the system to forward matching traffic in some cases.

NOTE: If you specify a policer in an egress firewall filter, the only supported action is **discard**.

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Configuring Firewall Filters on page 121
- Overview of Policers on page 35

three-color-policer

Syntax

```
three-color-policer policer-name {
  action {
    loss-priority high then discard;
  }
  single-rate {
    (color-aware | color-blind);
    committed-information-rate bps;
    committed-burst-size bytes;
    excess-burst-size bytes;
  }
  two-rate {
    (color-aware | color-blind);
    committed-information-rate bps;
    committed-burst-size bytes;
    peak-information-rate bps;
    peak-burst-size bytes;
  }
}
```

Hierarchy Level

[edit firewall],
[edit logical-systems *logical-system-name* firewall]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure a three-color policer.

Options

policer-name—Name of the three-color policer. Use this name when you apply the policer to an interface.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Overview of Policers on page 35

two-rate

Syntax

```
two-rate {
  (color-aware | color-blind);
  committed-information-rate bps;
  committed-burst-size bytes;
  peak-information-rate bps;
  peak-burst-size bytes;
}
```

Hierarchy Level [edit firewall three-color-policer *policer-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure a two-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), peak information rate (PIR), and peak burst size (PBS).

Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but are within the PIR or the PBS are assigned medium-high loss priority (yellow). Packets that exceed the PIR and the PBS are assigned high loss priority (red).

Green and yellow packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.

The remaining statements are explained separately.

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

CHAPTER 11

Configuration Statements for Port Security

allowed-mac

Syntax allowed-mac *mac-address-list*

Hierarchy Level [edit ethernet-switching-options secure-access-port interface (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify particular MAC addresses to be added to the MAC address cache.

NOTE: Although this configuration restricts the addresses that can be added to the MAC address cache, it does not block the switch from receiving Layer 2 control packets—such as Link Layer Discovery Protocol (LLDP) packets—transmitted from MAC addresses that are not specified in the list of allowed MAC addresses. Control packets do not undergo the MAC address check, and they are therefore included in the statistics of packets received, though, they are not forwarded to another destination.

Default Allowed MAC addresses take precedence over dynamic MAC values. For example, if the **mac-limit** statement is set to four and three allowed MACs are configured, only one dynamic MAC can be learned on that interface.

Options ***mac-address-list***—One or more MAC addresses configured as allowed MAC addresses for a specified interface or all interfaces.

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

Related Documentation

- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Configuring MAC Limiting on page 134
- Configuring MAC Move Limiting (CLI Procedure) on page 136
- mac-limit on page 203
- no-allowed-mac-log on page 205

arp-inspection

Syntax

```
(arp-inspection | no-arp-inspection) {
    forwarding-class (for DHCP Snooping or DAI Packets) class-name;
}
```

Hierarchy Level [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*)]

Release Information Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description Perform dynamic ARP inspection on all VLANs or on the specified VLAN.

- **arp-inspection**—Enable ARP inspection.

  NOTE: When ARP inspection is enabled, the switch logs ARP request packets that it rejects.

- **no-arp-inspection**—Disable ARP inspection.

Default Disabled.

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

Related Documentation

- Enabling Dynamic ARP Inspection (CLI Procedure) on page 142
- Example: Configuring Basic Port Security Features on page 79Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 99
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 106

circuit-id

Syntax

```
circuit-id {
  prefix hostname;
  use-interface-description;
  use-vlan-id;
}
```

Hierarchy Level

- For platforms with ELS:

  [edit vlans *vlan-name* forwarding-options dhcp-security option-82]

- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82],
  [edit forwarding-options helpers bootp dhcp-option82] ,
  [edit forwarding-options helpers bootp interface *interface-name* dhcp-option82]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)

Description

Configure the **circuit-id** suboption (suboption 1) of DHCP option 82 (the DHCP relay agent information option) in DHCP packets destined for a DHCP server. This suboption identifies the circuit (the interface, the VLAN, or both) on which the DHCP request arrived.

The remaining statements are explained separately.

Default

If DCHP option 82 is enabled on the switch, the circuit ID is supplied by default in the format ***interface-name*:*vlan-name*** or, on a Layer 3 interface, just ***interface-name***.

Required Privilege Level

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

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

dhcp-trusted

Syntax (dhcp-trusted | no-dhcp-trusted);

Hierarchy Level [edit ethernet-switching-options secure-access-port interface (Access Port Security) (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Allow or deny DHCP responses from the specified interfaces (ports) or all interfaces.

- **dhcp-trusted**—Allow DHCP responses.
- **no-dhcp-trusted**—Deny DHCP responses.

Default Trusted for trunk ports, untrusted for access ports.

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

Related Documentation

- Overview of Access Port Protection on page 47
- Enabling a Trusted Port for DHCP on page 145

dhcp-option82

Syntax

```
dhcp-option82 {
  circuit-id {
    prefix hostname;
    use-interface-description;
    use-vlan-id;
  }
  remote-id {
    prefix hostname | mac | none;
    use-interface-description;
    use-string string;
  }
  vendor-id <string>;
}
```

Hierarchy Level

[edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*)]
[edit forwarding-options helpers bootp]
[edit forwarding-options helpers bootp interface *interface-name*]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

When the switch receives a DHCP request from a DHCP client connected on one of the switch's interfaces, have the switch insert DHCP option 82 (also known as the DHCP relay agent information option) information in the DHCP request packet header before it forwards or relays the request to a DHCP server. The server uses the option 82 information, which provides details about the circuit and host the request came from, in formulating the reply; the server does not, however, make any changes to the option 82 information in the packet header. The switch receives the reply and then removes the DHCP option 82 information before forwarding the reply to the client.

The remaining statements are explained separately.

Default

Insertion of DHCP option 82 information is not enabled.

Required Privilege Level

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

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149
- *[edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches*

- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

dhcp-snooping-file

Syntax

```
dhcp-snooping-file {
  location local_pathname | remote_URL;
  timeout seconds;
  write-interval seconds;
}
```

Hierarchy Level

For platforms without ELS:

[edit ethernet-switching-options secure-access-port]

For platforms with ELS:

[edit system processes] dhcp-service]

Release Information

Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Specify a local pathname or remote URL for the DHCP snooping database file to maintain persistence of IP-MAC bindings.

The remaining statements are explained separately.

Default

The IP-MAC bindings in the DHCP snooping database file are not persistent. If the switch is rebooted, the bindings are lost.

Required Privilege Level

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

Related Documentation

- Understanding DHCP Snooping for Port Security on page 52

dhcp-trusted

Syntax (dhcp-trusted | no-dhcp-trusted);

Hierarchy Level [edit ethernet-switching-options secure-access-port interface (Access Port Security) (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Allow or deny DHCP responses from the specified interfaces (ports) or all interfaces.

- **dhcp-trusted**—Allow DHCP responses.
- **no-dhcp-trusted**—Deny DHCP responses.

Default Trusted for trunk ports, untrusted for access ports.

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

Related Documentation

- Overview of Access Port Protection on page 47
- Enabling a Trusted Port for DHCP on page 145

disable-timeout (Port Error Disable)

Syntax disable-timeout *timeout*;

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

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

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

NOTE: If you modify an existing timeout value, the new timeout value does not affect currently disabled interfaces are configured for automatic recovery. The new timeout value applies only to subsequent port errors. Run the clear ethernet-switching port-error command to restore currently disabled interfaces.

Default The disable timeout statement is not enabled.

Options ***timeout***—Time, in seconds, that an interface remains disabled. The disabled interface automatically returns to service when the specified time expires.

Range: 10 through 3600 seconds

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

Related Documentation

- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Understanding Storm Control on page 69
- Example: Configuring Storm Control to Prevent Network Outages on page 87
- Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure) on page 138
- action-shutdown on page 224

ethernet-switching-options

Syntax

```
ethernet-switching-options {
  analyzer {
    name {
      input {
        egress {
          interface (all | interface-name);
        }
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      output {
        interface interface-name;
        ip-address ip-address;
        vlan (vlan-id | vlan-name);
      }
    }
  }
  bpdu-block {
    interface (all | [interface-name]);
    disable-timeout timeout;
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100)
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-table-aging-time seconds {
  }
  port-error-disable {
    disable-timeout timeout;
  }
  secure-access-port {
    dhcp-snooping-file {
      location local_pathname | remote_URL;
      timeout seconds;
      write-interval seconds;
    }
    interface (all | interface-name) {
      allowed-mac {
        mac-address-list;
      }
      (dhcp-trusted | no-dhcp-trusted);
      fcoe-trusted;
      mac-limit limit action action;
      no-allowed-mac-log;
    }
    vlan (all | vlan-name) {
      (arp-inspection | no-arp-inspection) [
        forwarding-class (for DHCP Snooping or DAI Packets) class-name;
      }
```

```
        dhcp-option82 {
          circuit-id {
            prefix (Circuit ID for Option 82) hostname;
            use-interface-description;
            use-vlan-id;
          }
          remote-id {
            prefix (Remote ID for Option 82) hostname | mac | none;
            use-interface-description;
            use-string string;
          }
          vendor-id <string>;
        }
        (examine-dhcp | no-examine-dhcp) {
          forwarding-class (for DHCP Snooping or DAI Packets) class-name;
        }
        examine-fip {
          examine-vn2vn {
            beacon-period milliseconds;
          }
          fc-map fc-map-value;
          no-fip-snooping-scaling;
        }
        mac-move-limit limit <fabric-limit limit action action;
      }
    }
    static {
      vlan vlan-id {
        mac mac-address next-hop interface-name;
      }
    }
    storm-control {
      interface (all | interface-name) {
        bandwidth bandwidth;
        no-broadcast;
        no-multicast;
        no-unknown-unicast;
      }
    }
    traceoptions {
      file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure Ethernet switching options.

The remaining statements are explained separately.

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

Related Documentation
- *Understanding Port Mirroring*
- Overview of Access Port Protection on page 47
- Understanding Storm Control on page 69

examine-dhcp

Syntax
(examine-dhcp | no-examine-dhcp);

Hierarchy Level
[edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*)]

Release Information
Statement introduced in Junos OS Release 12.1 for the QFX Series

Description
Enable DHCP snooping on all VLANs or on the specified VLAN.

- examine-dhcp—Enable DHCP snooping.

NOTE: When DHCP snooping is enabled, the switch logs DHCPDISCOVER packets that it rejects.

- no-examine-dhcp—Disable DHCP snooping.

Default
Disabled.

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

Related Documentation
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 99
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 106
- Enabling DHCP Snooping (CLI Procedure) on page 140

examine-fip

Syntax

```
examine-fip {
  examine-vn2vn {
    beacon-period milliseconds;
  }
  fc-map fc-map-value;
  no-fip-snooping-scaling;
}
```

Hierarchy Level [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*)]

Release Information

Statement introduced in Junos OS Release 10.4 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement **examine-vn2vn** introduced in Junos OS Release 12.2 for the QFX Series.
Statement **no-fip-snooping-scaling** introduced in Junos OS Release 13.2X52-D10 for the QFX Series.

Description

NOTE: This statement supports the original CLI. If your switch runs the Enhanced Layer 2 Software (ELS) CLI, see *examine-vn2vf* for VN_Port to VF_Port (VN2VF_Port) FIP snooping, and see *examine-vn2vn* for VN_Port to VN_Port (VN2VN_Port) FIP snooping. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

Enable FIP snooping on a specified VLAN. Ensure that the VLAN is a dedicated FCoE VLAN that transports only FCoE traffic.

(QFX Series only) Enable VN2VN_Port FIP snooping on the specified VLAN. The VLAN must be a dedicated FCoE VLAN that transports only VN2VN_Port traffic. One FCoE VLAN cannot support both VN2VF_Port FIP snooping and VN2VN_Port FIP snooping. Configure separate, dedicated FCoE VLANs for VN2VN_Port FIP snooping and VN2VN_Port FIP snooping.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *vlan*
- *Example: Configuring an FCoE Transit Switch*
- *Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

fc-map

Syntax fc-map *fc-map-value*;

Hierarchy Level Original CLI

[edit ethernet-switching options secure-access-port vlan (all | *vlan-name*) examine-fip]

ELS CLI for Platforms that Support FCoE

[edit vlans *vlan-name* forwarding-options fip-security]

NOTE: The fc-map configuration statement is in a different hierarchy on the original CLI than on the Enhanced Layer 2 Software (ELS) CLI.

QFX Series that Support FCoE-FC Gateway Configuration

[edit fc-fabrics *fc-fabric-name* protocols fip]

Release Information Statement introduced in Junos OS Release 10.4 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced for the ELS CLI in Junos OS Release 13.2 for the QFX Series.

Description Set the FCoE mapped address prefix (FC-MAP) value for the FCoE VLAN to match the FC switch (or FCoE forwarder) FC-MAP value for the FC fabric. The FC-MAP value is a unique MAC address prefix an FC switch uses to identify FCoE traffic for a given FC fabric (traffic on a particular FCoE VLAN).

You can configure the FC-MAP value or use the default value. The default FC-MAP value is different for VN_Port to VF_Port (VN2VF_Port) FIP snooping (0x0EFC00) than for VN_Port to VN_Port (VN2VN_Port) FIP snooping.

The FC switch provides the FC-MAP value to FCoE nodes (ENodes) in the FIP discovery advertisement message. If the EX Series switch or the QFX Series FCoE VLAN FC-MAP value does not match the FC switch FC-MAP value, neither device discovers the FC switch on that VLAN, and the ENodes on that VLAN cannot access the FC switch. The FC switch accepts only FCoE traffic that uses the correct FC-MAP value as part of the VN_Port MAC address.

When the QFX Series acts as an FCoE-FC gateway, the FC-MAP value for the gateway and the FCoE devices must match the FC switch FC-MAP value in order to communicate with the FC switch.

NOTE: Changing the FC-MAP value causes all logins to drop and forces the ENodes to log in again.

Options ***fc-map-value***—FC-MAP value, hexadecimal value preceded by “0x”.

Range: 0x0EFC00 through 0x0EFCFF

Default: 0x0EFC00 for VN2VF_Port FIP snooping0x0EFD00 for VN2VN_Port FIP snooping

Required Privilege Level

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

Related Documentation

- examine-fip on page 196
- *show fip snooping*
- *Example: Configuring an FCoE Transit Switch*
- *Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

fcoe-trusted

Syntax fcoe-trusted;

Hierarchy Level Original CLI

[edit ethernet-switching-options secure-access-port interface *interface-name*]

ELS CLI for Platforms that Support FCoE

[edit vlans *vlan-name* forwarding-options fip-security interface *interface-name*]

NOTE: The **fcoe-trusted** configuration statement is in a different hierarchy on the original CLI than on the Enhanced Layer 2 Software (ELS) CLI.

QFX Series that Support FCoE-FC Gateway Configuration

[edit fc-fabrics *fc-fabric-name* protocols fip]

Release Information Statement introduced in Junos OS Release 10.4 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced for the FC fabric in Junos OS Release 11.3 for the QFX Series.
Statement introduced for the ELS CLI in Junos OS Release 13.2 for the QFX Series.

Description Configure the specified 10-Gigabit Ethernet interface to trust Fibre Channel over Ethernet (FCoE) traffic. If an interface is connected to another switch such as an FCoE forwarder (FCF) or a transit switch, you can configure the interface as trusted so that the interface forwards FCoE traffic from the switch to the FCoE devices without installing FIP snooping filters.

(QFX Series FCoE-FC gateway) Configure the specified local Fibre Channel fabric to trust FCoE traffic on all ports in the fabric. Changing the fabric ports from untrusted to trusted removes any existing FIP snooping filters from the ports. Changing the fabric ports from trusted to untrusted by removing the **fcoe-trusted** configuration from the fabric forces all of the FCoE sessions on those ports to log out so that when the ENodes and VN_Ports log in again, the switch can build the appropriate FIP snooping filters.

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

Related Documentation

- *show fip snooping*
- *Example: Configuring an FCoE Transit Switch*
- *Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*
- *Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

forwarding-class (for DHCP Snooping or DAI Packets)

Syntax forwarding-class class *class-name*;

Hierarchy Level [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) (examine-dhcp | arp-inspection)]

Release Information Statement introduced in Junos OS Release 11.2 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description Assign a user-defined or a predefined forwarding class to the packets that have been checked for DHCP snooping or dynamic ARP inspection (DAI).

NOTE: To assign a user-defined class, you must first configure the user-defined class by using the *forwarding-classes* configuration statement at the [edit *class-of-service*] hierarchy level.

Default Disabled.

Options ***class-name***—Name of the forwarding class. The forwarding class can be one of the predefined forwarding classes (best-effort, assured-forwarding, expedited-forwarding, network-control) or it can be a user-defined forwarding class.

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

Related Documentation

- *Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic*
- *Understanding Junos OS CoS Components for EX Series Switches*
- Understanding DHCP Snooping for Port Security on page 52
- Understanding DAI for Port Security on page 59

interface (Secure Access Port)

Syntax

```
interface (all | interface-name) {
  allowed-mac mac-address-list;
  (dhcp-trusted | no-dhcp-trusted);
  mac-limit limit action action;
  no-allowed-mac-log;
  static-ip ip-address {
    vlan vlan-name;
    mac mac-address;
  }
}
```

Hierarchy Level [edit ethernet-switching-options secure-access-port]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Apply port security features to all interfaces or to the specified interface.

The remaining statements are explained separately.

Options **all**—Apply port security features to all interfaces. Does not apply to QFabric systems.

interface-name—Apply port security features to the specified interface.

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

Related Documentation

- Overview of Access Port Protection on page 47
- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Understanding Trusted and Untrusted Ports on page 63
- Configuring MAC Limiting on page 134
- Enabling a Trusted Port for DHCP on page 145

location

Syntax location *local_pathname* | *remote_URL*;

Hierarchy Level [edit ethernet-switching-options secure-access-port dhcp-snooping-file]

Release Information Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description Specify either a local pathname or a remote URL as the location in which to store the DHCP snooping database.

Options ***local_pathname* | *remote_URL*** —Location for storing the DHCP snooping database.

- ***local_pathname*** —Use ***/path*** to store the database on a local switch.
- ***remote_URL*** —Use **ftp://*ip-address*** or **ftp://** ***hostname/path*** to store the database at a remote location.

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

mac

Syntax mac *mac-address*;

Hierarchy Level [edit ethernet-switching-options secure-access-port interface (Access Port Security) (all | *interface-name*) static-ip *ip-address* vlan (DHCP Bindings on Access Ports) *vlan-name*]
[edit vlans *vlan-name* forwarding-options dhcp-security group *group-name* interface *interface-name* static-ip *ip-address*]

Release Information Statement introduced in Junos OS Release 11.1 on the QFX Series switches.

Description Specify a media access control (MAC) address (hardware address) for the specified static IP address.

Options ***mac-address***—Value in hexadecimal format.

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

mac-limit

Syntax

```
mac-limit limit {
  <action action>;
}
```

Hierarchy Level [edit ethernet-switching-options secure-access-port interface (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify the number of MAC addresses that can be dynamically added to the MAC address cache for this access interface (port) and the action to be taken if the limit is exceeded.

Default The default action is **drop**.

Options ***limit***—Maximum number of MAC addresses.

action *action*—(Optional) Action to take when the MAC address limit is exceeded:

- **drop**—Drop the packet and generate a system log entry. This is the default.
- **log**—Do not drop the packet but generate a system log entry.
- **none**—No action.
- **shutdown**—Disable the interface and generate an alarm. If you configure the switch with the port-error-disable statement, the disabled interface recovers automatically upon expiration of the specified timeout. If this statement is not configured, you can bring up the disabled interfaces by running the clear ethernet-switching port-error command.

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

Related Documentation

- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Configuring MAC Limiting on page 134
- allowed-mac on page 185

mac-move-limit

Syntax mac-move-limit *limit* <fabric-limit *limit*> action *action*;

Hierarchy Level For platforms without ELS:

[edit ethernet-switching-options secure-access-port (all | *vlan-name*)]

For platforms with ELS:

[edit vlans *vlan-name* switch-options],

Release Information Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description Specify the number of times a MAC address can move to a new interface (port) in 1 second and the action to be taken by the switch if the MAC address move limit is exceeded.

CAUTION: Mac move limiting does not work properly on a QFX5100 switch used as a Node device in a QFabric system. Do not use this feature on a QFX5100 switch in a QFabric system.

Default The default move limit is unlimited. The default action is **drop**.

Options **fabric-limit**—Specify the maximum number of moves in a QFabric system. If you do not specify a fabric limit, the value for **mac-move-limit** applies to the QFabric system.

limit—Maximum number of moves to a new interface per second.

action *action*—(Optional) Action to take when the MAC address move limit is reached:

- **drop**—Drop the packet and generate an alarm, an SNMP trap, or a system log entry. This is the default.
- **log**—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- **none**—No action.
- **shutdown**—Disable the interface and generate an alarm. If you have configured the switch with the **port-error-disable** statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the **clear-ethernet-switch-port** command.

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

Related Documentation

- mac-limit on page 203
- Example: Configuring Basic Port Security Features on page 79
- Configuring MAC Move Limiting (CLI Procedure) on page 136
- *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*

no-allowed-mac-log

Syntax no-allowed-mac-log;

Hierarchy Level

- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port interface (all | *interface-name*)]

- For platforms with ELS:

  [edit switch-options interface *interface-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify that the switch should not log messages when it receives packets from invalid MAC addresses on an interface that has been configured for allowed MAC addresses.

Default The switch logs messages when it receives packets from invalid MAC addresses on an interface that has been configured for particular allowed (specific) MAC addresses.

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

Related Documentation

- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Configuring MAC Limiting on page 134
- allowed-mac on page 185
- mac-limit on page 203

no-dhcp-trusted

Syntax (dhcp-trusted | no-dhcp-trusted);

Hierarchy Level [edit ethernet-switching-options secure-access-port interface (Access Port Security) (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Port security features, such as DHCP snooping and dynamic ARP inspection inspect packets only on untrusted interfaces.

Allow or deny DHCP responses from the specified interfaces (ports) or all interfaces.

- **dhcp-trusted**—Allow DHCP responses.
- **no-dhcp-trusted**—Deny DHCP responses.

Default Trusted for trunk ports, untrusted for access ports.

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

Related Documentation

- Overview of Access Port Protection on page 47
- Enabling a Trusted Port for DHCP on page 145

no-gratuitous-arp-request

Syntax no-gratuitous-arp-request;

Hierarchy Level [edit interfaces *interface-name*],
[edit interfaces interface-range *interface-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the switch not to respond to gratuitous ARP requests. You can disable responses to gratuitous ARP requests on both Layer 2 Ethernet switching interfaces and routed VLAN interfaces (RVIs).

Default Gratuitous ARP responses are enabled on all Ethernet switching interfaces and RVIs.

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

Related Documentation

- *Configuring IRB Interfaces*

persistent-learning

Syntax persistent-learning;

Hierarchy Level
- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port interface (all | *interface-name*)]
- For platforms with ELS:

  [edit switch-options interface *interface-name*]

Release Information Statement introduced in Junos OS Release 11.4 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.
Hierarchy level [edit switch-options interface interface-name] introduced in Junos OS Release 13.2X50-D10

Description Specify that learned MAC addresses persist on the specified interfaces across restarts of the switch and link-down conditions. This feature is also known as sticky MAC.

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

Related Documentation
- Example: Configuring Basic Port Security Features on page 79
- *Configuring Persistent MAC Learning (CLI Procedure)*
- *Configuring Persistent MAC Learning (CLI Procedure)*

port-error-disable

Syntax

```
port-error-disable {
  (disable-timeout seconds | recovery-timeout seconds);
}
```

Hierarchy Level

- For platforms without ELS:

  [edit ethernet-switching-options]

- For platforms with ELS:

  [edit switch-options]

Release Information Statement introduced in Junos OS Release 11.1 on the QFX Series.

Description Disable rather than block an interface when enforcing MAC limiting, MAC move limiting, and storm control, and allow the interface to recover automatically from the error condition after a specified period of time:

NOTE: The **port-error-disable** configuration does not apply to preexisting error conditions. It affects only error conditions that are detected after you enable and commit the **port-error-disable** statement. To clear a preexisting error condition and restore the interface to service, use the clear ethernet-switching port-error command.

- If you enable the mac-limit statement with the **shutdown** option and also enable the **port-error-disable** statement, the switch disables (rather than shuts down) the interface when the MAC address limit is reached.
- If you have enabled the mac-move-limit statement with the **shutdown** option and you enable the **port-error-disable** statement, the switch disables (rather than shuts down) the interface when the maximum number of moves to a new interface is reached.
- If you enable the storm-control statement with the **action-shutdown** option and you also enable **port-error-disable**, the switch disables (rather than shuts down) the interface when broadcast traffic and unknown unicast traffic exceed the specified levels.

Default Not enabled.

Required Privilege Level

routing—To view this statement in the configuration.
routing–control—To add this statement to the configuration.

Related Documentation

- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Understanding Storm Control on page 69
- Example: Configuring Storm Control to Prevent Network Outages on page 87

- Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure) on page 138
- action-shutdown on page 224
- disable-timeout on page 192
- clear ethernet-switching port-error on page 252

prefix (Remote ID for Option 82)

Syntax prefix hostname | mac | none;

Hierarchy Level [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82 remote-id]
[edit forwarding-options helpers bootp dhcp-option82 remote-id]
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82 remote-id]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description Configure an optional prefix for the remote ID suboption in the DHCP option 82 information that is inserted by the switch into the packet header of a DHCP request before it forwards or relays the request to a DHCP server.

Default If **prefix** is not explicitly specified, no prefix is appended to the remote ID.

Options

hostname—Name of the host system (the switch) that is forwarding or relaying the DHCP request from the DHCP client to the DHCP server.

mac—MAC address of the host system (the switch) that is forwarding or relaying the DHCP request from the DHCP client to the DHCP server.

none—No prefix is applied to the remote ID.

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

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149
- *[edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

remote-id

Syntax

```
remote-id {
  host-name host-name;
  mac;
  prefix hostname | mac | none; | host
  use-interface-description;
  use-string string;
}
```

Hierarchy Level

- For platforms with ELS:

  [edit vlans *vlan-name* forwarding-options dhcp-security option-82]

- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82],
  [edit forwarding-options helpers bootp dhcp-option82],
  [edit forwarding-options helpers bootp interface *interface-name* dhcp-option82]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security option-82]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)

Description

Insert the **remote-id** suboption of DHCP option 82 (also known as the DHCP relay agent information option) in DHCP request packet headers before forwarding or relaying requests to a DHCP server. This suboption provides a trusted identifier for the host system that has forwarded or relayed requests to the server.

The remaining statements are explained separately, and their availability depends on the hierarchy level at which **remote-id** is specified, as follows:

- The statement prefix is *not* supported at the **[edit vlans *vlan-name* forwarding-options dhcp-security option-82]** hierarchy level.
- The statement **host-name** is supported *only* at the **[edit vlans *vlan-name* forwarding-options dhcp-security option-82]** hierarchy level.

Default

If **remote-id** is not explicitly set, no remote ID value is inserted in the DHCP request packet header.

If **remote-id** is explicitly set, but is not qualified by a keyword:

- At the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level, the default keyword value is *interface-name*.
- At all other hierarchy levels, the default value of the **remote-id** keyword is the MAC address of the switch.

Required Privilege Level

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

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

secure-access-port

Syntax

```
secure-access-port {
  deactivate;
    dhcp-snooping-file {
    location (local_pathname | remote_URL);
    timeout seconds;
    write-interval seconds;
  }
  interface (all | interface-name) {
    allowed-mac mac-address-list;
    (dhcp-trusted | no-dhcp-trusted);
    fcoe-trusted;
    mac-limit limit {
      <action action>;
    }
    no-allowed-mac-log;
    persistent-learning;
    static-ip  ip-address {
      vlan vlan-name;
      mac mac-address;
    }
  }
  vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection) [
      forwarding-class (for DHCP Snooping or DAI Packets) class-name;
    }
    dhcp-option82 {
      circuit-id {
        prefix (Circuit ID for Option 82) hostname;
        use-interface-description;
        use-vlan-id;
      }
      remote-id {
        prefix (Remote ID for Option 82) hostname | mac | none;
        use-interface-description;
        use-string string;
      }
      vendor-id <string>;
    }
    (examine-dhcp | no-examine-dhcp) {
      forwarding-class (for DHCP Snooping or DAI Packets) class-name;
    }
    examine-fip {
      examine-vn2vn {
        beacon-period milliseconds;
      }
      fc-map fc-map-value;
      no-fip-snooping-scaling;
    }
    mac-move-limit limit action action;
  }
```

Hierarchy Level [edit ethernet-switching-options]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure port security features, including MAC limiting and whether interfaces can receive DHCP responses, and apply dynamic ARP inspection, DHCP snooping, DHCP option 82, and MAC move limiting on no VLANs, specific VLANs, or all VLANs.

The remaining statements are explained separately.

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

Related Documentation

- Overview of Access Port Protection on page 47
- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Understanding Trusted and Untrusted Ports on page 63
- Configuring MAC Limiting on page 134
- Enabling a Trusted Port for DHCP on page 145

static-ip

Syntax

```
static-ip ip-address;
  mac mac-address;
  vlan vlan-name;
}
```

Hierarchy Level [edit ethernet-switching-optionssecure-access-port interface (all | *interface-name*)]
[edit vlans *vlan-name* forwarding-options dhcp-security group *group-name* interface *interface-name*]

Release Information Statement introduced in Junos OS Release 12.1 on the QFX Series.

Description Bind a static IP address to a MAC address in the DHCP snooping database.

Options ***ip-address***—IP address assigned to the device connected on the specified interface.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 139

timeout (DHCP Snooping)

Syntax timeout *seconds*;

Hierarchy Level [edit ethernet-switching-options secure-access-port dhcp-snooping-file]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify a timeout value for remote read and write operations. This value determines the amount of time that the switch waits for a remote system to respond when the DHCP snooping database is stored on a remote FTP site.

Default None

Options ***seconds*** —Value in seconds.

Range: 10 through 3600

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

Related Documentation

- Understanding DHCP Snooping for Port Security on page 52

use-interface-description

Syntax use-interface-description;

Hierarchy Level

- For platforms with ELS:

  [edit vlans *vlan-name* forwarding-options dhcp-security option-82 circuit-id]

- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82 circuit-id],
  [edit forwarding-options helpers bootp dhcp-option82 circuit-id],
  [edit forwarding-options helpers bootp interface *interface-name* dhcp-option82 circuit-id],
  [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82 remote-id],
  [edit forwarding-options helpers bootp dhcp-option82 remote-id],
  [edit forwarding-options helpers bootp interface *interface-name* dhcp-option82 remote-id]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)

Description Use the interface description rather than the interface name (which is the default value) in the circuit ID or remote ID value in the DHCP option 82 information.

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

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

use-string

Syntax use-string *string*;

Hierarchy Level

- For platforms with ELS:

  [edit vlans *vlan-name* forwarding-options dhcp-security option-82 remote-id]

- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82 remote-id],
  [edit forwarding-options helpers bootp dhcp-option82 remote-id] ,
  [edit forwarding-options helpers bootp interface *interface-name* dhcp-option82 remote-id]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)

Description Use a string rather than the MAC address of the host system (the default) in the remote ID value in the DHCP option 82 information.

Options ***string***—Character string used as the remote ID value.

Range: 1–255 characters

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

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

use-vlan-id

Syntax use-vlan-id;

Hierarchy Level

- For platforms with ELS:

  [edit vlans *vlan-name* forwarding-options dhcp-security option-82 circuit-id]
  [edit forwarding-options dhcp-relay relay-option-82 circuit-id],
  [edit forwarding-options dhcp-relay group *group-name* relay-option-82 circuit-id],
  [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay relay-option-82 circuit-id],
  [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* relay-option-82 circuit-id]

- For platforms without ELS:

  [edit forwarding-options helpers bootp dhcp-option82-circuit-id],
  [edit forwarding-options helpers bootp interface *interface-name* dhcp-option82-circuit-id]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Different hierarchy levels (listed above) introduced in Junos OS Release 13.2X50-D10.
(See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)

Description Use the VLAN tag (VLAN ID) instead of the VLAN name (which is the default) in the circuit ID value in the DHCP option 82 information.

NOTE: The VLAN ID for a tagged VLAN is configured using the **vlan-id** statement at the **[edit vlana *vlan-name*]** hierarchy level.

Default The default value for **circuit-id** is the VLAN name.

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

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- *Using a VLAN Tag in Option 82*

- *Enabling and Disabling Insertion of Option 82 Information*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

vendor-id

Syntax vendor-id <*string*>;

Hierarchy Level
- For platforms with ELS:

  [edit vlans *vlan-name* forwarding-options dhcp-security option-82]
- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82],
  [edit forwarding-options helpers bootp dhcp-option82],
  [edit forwarding-options helpers bootp interface *interface-name* dhcp-option82]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)

Description Insert a vendor ID in the DHCP option 82 information in a DHCP request packet header before forwarding or relaying the request to a DHCP server.

Default If **vendor-id** is not explicitly configured for DHCP option 82, then no vendor ID is set.

Options ***string***—(Optional) A single string that designates the vendor ID.

Range: 1–255 characters

Default: If you specify **vendor-id** with no ***string*** value, then the default vendor ID **Juniper Networks** is configured.

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

Related Documentation
- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 114
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 118
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 146
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 149

vlan (Secure Access Port)

Syntax

```
vlan (all | vlan-name) {
  examine-fip {
    examine-vn2vn {
      beacon-period milliseconds;
    }
    fc-map fc-map-value;
    no-fip-snooping-scaling;
  }
  dhcp-option82
    circuit-id {
      prefix (Circuit ID for Option 82) hostname;
      use-interface-description;
      use-vlan-id;
    }
    remote-id {
      prefix (Remote ID for Option 82) hostname | mac | none;
      use-interface-description;
      use-string string;
    }
    vendor-id <string>;
  }
  (arp-inspection | no-arp-inspection);
    circuit-id {
      prefix (Circuit ID for Option 82) hostname;
      use-interface-description;
      use-vlan-id;
    }
    remote-id {
      prefix (Remote ID for Option 82) hostname | mac | none;
      use-interface-description;
      use-string string;
    }
  vendor-id <string>;
  }
  (examine-dhcp | no-examine-dhcp);
  mac-move-limitlimit action action;
}
```

Hierarchy Level [edit ethernet-switching-options secure-access-port]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Apply DHCP snooping, dynamic ARP inspection (DAI), DHCP option 82, and MAC move limiting.

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

The remaining statements are explained separately.

Options

all—Apply DHCP snooping, DAI, DHCP option 82, and MAC move limiting to all VLANs.

vlan-name —Apply DHCP snooping, DAI, DHCP option 82, and MAC move limiting to the specified VLAN.

Required Privilege Level

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

Related Documentation

- Overview of Access Port Protection on page 47
- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- Understanding Trusted and Untrusted Ports on page 63
- Configuring MAC Limiting on page 134
- Enabling a Trusted Port for DHCP on page 145

vlan (Static IP)

Syntax

vlan *vlan-name*;

Hierarchy Level

[edit ethernet-switching-options secure-access-port interface (all | *interface-name*) static-ip *ip-address*]

Release Information

Statement introduced in Junos OS Release 12.1 for the QFX Series switches.

Description

Associate a static IP address with the specified VLAN.

Options

vlan-name—Name of a VLAN associated with the specified interface.

Required Privilege Level

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

Related Documentation

- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 139

write-interval

Syntax write-interval *seconds*;

Hierarchy Level For platforms without ELS:

[edit ethernet-switching-options secure-access-port dhcp-snooping-file]

For platforms with ELS:

[edit system processes] dhcp-service dhcp-snooping-file]

Release Information Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description Specify how frequently the switch writes the database entries from memory into the specified DHCP snooping database file.

Default None

Options ***seconds***—Value in seconds.
Range: 60 through 86400

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

Related Documentation
- Understanding DHCP Snooping for Port Security on page 52

CHAPTER 12

Configuration Statements for Device Security

action-shutdown

Syntax action-shutdown;

Hierarchy Level For platforms without ELS:

[edit ethernet-switching-options storm-control]

For platforms with ELS:

[edit forwarding-options storm-control-profiles]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

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

- If you set both the **action-shutdown** and the **port-error-disable** statements, the affected interfaces are disabled temporarily and recover automatically when the disable timeout expires.
- If you set the **action-shutdown** statement and do not set the **port-error-disable** statement, the affected interfaces are shut down when the storm control level is exceeded, and they do not recover automatically. You must issue the **clear ethernet-switching port-error** command to clear the port error and restore the interfaces to service.

Default The **action-shutdown** feature is disabled. If the storm control level is exceeded, the switch drops broadcast and unknown unicast messages on the specified interfaces.

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

Related Documentation

- Understanding Storm Control on page 69
- Example: Configuring Storm Control to Prevent Network Outages on page 87
- port-error-disable on page 208
- disable-timeout on page 192
- clear ethernet-switching port-error on page 252

bandwidth

Syntax bandwidth *bandwidth*;

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

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description For interfaces configured for storm control, configure the storm control level as the bandwidth in kilobits per second (Kbps). If the combination of broadcast and unknown unicast traffic exceeds this level, the switch performs the appropriate action.

Default None.

Options **bandwith**—Broadcast and unknown unicast traffic rate in Kbps.
Range: 100 through 10000000 Kbps
Default: None

NOTE: When you configure storm control bandwidth, the value you configure is rounded off internally to the closest multiple of 64 Kbps, and the rounded-off value represents the bandwidth that is actually enforced. For example, if you configure a bandwidth limit of 150 Kbps, storm control enforces a bandwidth limit of 128 Kbps.

CAUTION: Junos OS allows you to configure a storm control value that exceeds the bandwidth of the interface. If you configure an interface with such a value, storm control does not drop broadcast or unknown unicast packets even if they consume all the available bandwidth.

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

Related Documentation

- Understanding Storm Control on page 69
- Example: Configuring Storm Control to Prevent Network Outages on page 87
- action-shutdown on page 224
- port-error-disable on page 208
- disable-timeout on page 192
- clear ethernet-switching port-error on page 252

ethernet-switching-options

Syntax

```
ethernet-switching-options {
  analyzer {
    name {
      input {
        egress {
          interface (all | interface-name);
        }
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      output {
        interface interface-name;
        ip-address ip-address;
        vlan (vlan-id | vlan-name);
      }
    }
  }
  bpdu-block {
    interface (all | [interface-name]);
    disable-timeout timeout;
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100)
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-table-aging-time seconds {
  }
  port-error-disable {
    disable-timeout timeout;
  }
  secure-access-port {
    dhcp-snooping-file {
      location local_pathname | remote_URL;
      timeout seconds;
      write-interval seconds;
    }
    interface (all | interface-name) {
      allowed-mac {
        mac-address-list;
      }
      (dhcp-trusted | no-dhcp-trusted);
      fcoe-trusted;
      mac-limit limit action action;
      no-allowed-mac-log;
    }
    vlan (all | vlan-name) {
      (arp-inspection | no-arp-inspection) [
        forwarding-class (for DHCP Snooping or DAI Packets) class-name;
      }
```

```
        dhcp-option82 {
          circuit-id {
            prefix (Circuit ID for Option 82) hostname;
            use-interface-description;
            use-vlan-id;
          }
          remote-id {
            prefix (Remote ID for Option 82) hostname | mac | none;
            use-interface-description;
            use-string string;
          }
          vendor-id <string>;
        }
        (examine-dhcp | no-examine-dhcp) {
          forwarding-class (for DHCP Snooping or DAI Packets) class-name;
        }
        examine-fip {
          examine-vn2vn {
            beacon-period milliseconds;
          }
          fc-map fc-map-value;
          no-fip-snooping-scaling;
        }
        mac-move-limit limit <fabric-limit limit action action;
      }
    }
    static {
      vlan vlan-id {
        mac mac-address next-hop interface-name;
      }
    }
    storm-control {
      interface (all | interface-name) {
        bandwidth bandwidth;
        no-broadcast;
        no-multicast;
        no-unknown-unicast;
      }
    }
    traceoptions {
      file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure Ethernet switching options.

The remaining statements are explained separately.

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

Related Documentation
- *Understanding Port Mirroring*
- Overview of Access Port Protection on page 47
- Understanding Storm Control on page 69

interface (Storm Control)

Syntax

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

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

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Apply storm control to all interfaces or to the specified interface.

The remaining statement is explained separately.

Default
Storm control is disabled.

Options
all—Apply storm control to all interfaces.

interface-name—Apply storm control to the specified interface.

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

Related Documentation
- Understanding Storm Control on page 69
- Example: Configuring Storm Control to Prevent Network Outages on page 87

no-broadcast

Syntax no-broadcast;

Hierarchy Level For platforms without ELS:

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

For platforms with ELS:

[edit forwarding-options storm-control-profiles]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description For interfaces configured for storm control, disable broadcast traffic storm control on the interface.

Default When storm control is enabled on an interface, it is enabled for both unknown unicast traffic and broadcast traffic.

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

Related Documentation

- Understanding Storm Control on page 69
- Example: Configuring Storm Control to Prevent Network Outages on page 87

no-multicast

Syntax no-multicast;

Hierarchy Level For platforms without ELS:

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

For platforms with ELS:

[edit forwarding-options storm-control-profiles]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

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

Default Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic.

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

Related Documentation

- Understanding Storm Control on page 69
- Example: Configuring Storm Control to Prevent Network Outages on page 87

no-unknown-unicast

Syntax no-unknown-unicast;

Hierarchy Level For platforms without ELS:

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

For platforms with ELS:

[edit forwarding-options storm-control-profiles]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description For interfaces configured for storm control, disable unknown unicast traffic storm control on the interface.

Default When storm control is enabled on an interface, it is enabled for both unknown unicast traffic and broadcast traffic.

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

Related Documentation

- Understanding Storm Control on page 69
- Example: Configuring Storm Control to Prevent Network Outages on page 87

storm-control

Syntax

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

Hierarchy Level [edit ethernet-switching-options]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Apply storm control to all interfaces or to the specified interfaces on switches running non-ELS software. (For the equivalent statement for switches running ELS software, see *storm-control*.

The statements are explained separately.

NOTE: The **no-multicast** option is not supported on QFabric systems.

Default On switches running non-ELS software, storm control is disabled by default on all switch interfaces. If you enable storm control and do not specify a storm control level, the default level is 80 percent of the available bandwidth for ingress traffic.You can change the storm control level by configuring it as a specific bandwidth value.

When you configure storm control bandwidth on an aggregated Ethernet interface, each member of the aggregated interface is assigned that bandwidth. For example, if you configure 7000000 Kbps on aggregated interface **ae1**, and **ae1** has two members, **xe-2:0/0/0** and **xe-2:0/0/1**, each member is allowed a bandwidth level of 7000000 Kbps. Thus, the storm control bandwidth on **ae1** could be as much as 14000000 Kbps of combined broadcast and unknown unicast traffic.

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

Related Documentation

- Understanding Storm Control on page 69
- Example: Configuring Storm Control to Prevent Network Outages on page 87
- port-error-disable on page 208
- disable-timeout on page 192
- clear ethernet-switching port-error on page 252

PART 3

Administration

CHAPTER 13

Routine Monitoring

Monitoring Firewall Filter Traffic

You can use operational mode commands to monitor firewall filter traffic.

Monitoring Traffic for All Firewall Filters and Policers That Are Configured

Purpose Monitor the number of packets and bytes that matched the firewall filters and monitor the number of packets that exceeded policer rate limits:

Action Use the **show firewall** operational mode command:

```
user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name                                                Bytes              Packets
counter-employee-web                                 3348                   27
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
```

```
Policers:
Name                                                Packets
icmp-connection-policer                                  10
tcp-connection-policer                                    0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

Meaning The **show firewall** command displays the names of all firewall filters, counters, and policers that are configured. For each counter that is specified in a filter configuration, the output field shows the byte count and packet count for the term in which the counter is specified. For each policer that is specified in a filter configuration, the output field shows the packet count for packets that exceed the specified rate limits.

Monitoring Traffic for a Specific Firewall Filter

Purpose Monitor the number of packets and bytes that matched a firewall filter and monitor the number of packets that exceeded policer rate limits.

Action Use the **show firewall filter *filter-name*** operational mode command:

```
user@switch> show firewall filter ingress-port-limit-tcp-icmp
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
```

Meaning The **show firewall filter *filter-name*** command limits the display information to the counters and policers that are defined for the specified filter.

Monitoring Traffic for a Specific Policer

Purpose Monitor the number of packets that exceeded the rate limits of a policer:

Action Use the **show firewall policer *policer-name*** operational mode command:

```
user@switch> show firewall policer icmp-connection-policer
Filter: ingress-port-limit-tcp-icmp
Policers:
Name                                                Packets
icmp-connection-policer                                  10
```

Meaning The **show firewall policer *policer-name*** command displays the number of packets that exceeded the rate limits for the specified policer.

Related Documentation

- Configuring Firewall Filters on page 121
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Verifying That Firewall Filters Are Operational on page 238

Monitoring Port Security

Purpose Use the monitoring functionality to view these port security details:

- DHCP snooping database for a VLAN or all VLANs
- ARP inspection details for all interfaces

Action To monitor port security in the J-Web interface, select **Monitor** > **Security** > **Port Security**.

To monitor and manipulate the DHCP snooping database and ARP inspection statistics in the CLI, enter the following commands:

- **show dhcp snooping binding**
- **clear dhcp snooping binding**—In addition to clearing the whole database, you can clear database entries for specified VLANs or MAC addresses.
- **show arp inspection statistics**
- **clear arp inspection statistics**

NOTE: On EX4300 switches, to monitor and manipulate the DHCP snooping database and ARP inspection statistics in the CLI, enter the following commands:

- **show dhcp-security binding**
- **clear dhcp-security binding**—In addition to clearing the whole database, you can clear database entries for specified VLANs or IP Address.
- **show dhcp-security arp inspection statistics**
- **clear arp inspection statistics**

Meaning The J-Web Port Security Monitoring page comprises two sections:

- DHCP Snooping Details—Displays the DHCP snooping database for all the VLANs for which DHCP snooping is enabled. To view the DHCP snooping database for a specific VLAN, select the specific VLAN from the list.
- ARP Inspection Details—Displays the ARP inspection details for all interfaces. The information includes details of the number of packets that passed ARP inspection and the number of packets that failed the inspection. The pie chart graphically represents these statistics when you select an interface. To view ARP inspection statistics for a specific interface, select the interface from the list.

You can use the following options on the page to clear DHCP snooping and ARP inspection details:

- Clear All—Clears the DHCP snooping database, either for all VLANs if the option **ALL** has been selected in the Select VLANs list or for the specific VLAN that has been selected in that list.
- Clear—Deletes a specific IP address from the DHCP snooping database.

To clear ARP inspection details on the page, click **Clear All** in the ARP inspection details section.

NOTE: Clear All button in the ARP inspection details section is not supported on EX4300 switches.

Use the CLI commands to show and clear DHCP snooping database and ARP inspection statistics details.

Related Documentation

- Configuring Port Security (CLI Procedure) on page 131
- *Configuring Port Security (J-Web Procedure)*
- Example: Configuring Basic Port Security Features on page 79

Verifying That Firewall Filters Are Operational

Purpose Verify that firewall filters are working properly after you apply them to ports, VLANs, or Layer 3 interfaces.

Action Use the **show firewall** operational mode command to verify that the firewall filters are working properly:

```
user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name                                                Bytes              Packets
counter-employee-web                                    0                    0
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
Policers:
Name                                              Packets
icmp-connection-policer                              10
tcp-connection-policer                                0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

Meaning The **show firewall** command displays the names of all firewall filters, counters, and policers that are configured. For each counter that is specified in a filter configuration, the output field shows the byte count and packet count for the term in which the counter is specified. In the above example, the **icmp-counter** in the filter **ingress-port-limit-tcp-icmp** shows that the filter matched 10 packets. For each policer that is specified in a filter configuration, the output field shows the packet count for packets that exceed the

specified rate limits. The policer **icmp-connection-policer** shows that 10 ICMP packets were policed.

Related Documentation

- Configuring Firewall Filters on page 121
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Monitoring Firewall Filter Traffic on page 235

Verifying That DAI Is Working Correctly

Purpose Verify that dynamic ARP inspection (DAI) is working on the switch.

Action Send some ARP requests from network devices connected to the switch.

Display the DAI information:

```
user@switch> show arp inspection statistics
ARP inspection statistics:
Interface        Packets received  ARP inspection pass   ARP inspection failed
---------------  ---------------   -------------------- ---------------------
ge-0/0/1.0                     7                     5                     2
ge-0/0/2.0                    10                    10                     0
ge-0/0/3.0                    12                    12                     0
```

Meaning The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

Related Documentation

- Enabling Dynamic ARP Inspection (CLI Procedure) on page 142
- *Enabling Dynamic ARP Inspection (J-Web Procedure)*
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 99
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 106
- Monitoring Port Security on page 237

Verifying That DHCP Snooping Is Working Correctly

Purpose Verify that DHCP snooping is working on the switch and that the DHCP snooping database is correctly populated with both dynamic and static bindings.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch>  show dhcp snooping binding
DHCP Snooping Information:
MAC address        IP address  Lease (seconds) Type     VLAN      Interface

00:05:85:3A:82:77  192.0.2.17  600             dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:79  192.0.2.18  653             dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:80  192.0.2.19  720             dynamic  employee  ge-0/0/2.0
00:05:85:3A:82:81  192.0.2.20  932             dynamic  employee  ge-0/0/2.0
00:05:85:3A:82:83  192.0.2.21  1230            dynamic  employee  ge-0/0/2.0
00:05:85:27:32:88  192.0.2.22  –               static   data      ge-0/0/4.0
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires. Static IP addresses have no assigned lease time. The statically configured entry never expires.

If the DHCP server had been configured as untrusted, no entries would be added to the DHCP snooping database and nothing would be shown in the output of the **show dhcp snooping binding** command.

Related Documentation

- Enabling DHCP Snooping (CLI Procedure) on page 140
- *Enabling DHCP Snooping (J-Web Procedure)*
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 139
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 99
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 106
- Monitoring Port Security on page 237
- *Troubleshooting Port Security*

Verifying That MAC Limiting Is Working Correctly

MAC limiting protects against flooding of the Ethernet switching table by setting a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface (port).

Junos OS provides two MAC limiting methods:

- Maximum number of MAC addresses—You configure the maximum number of dynamic MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses can be ignored, dropped, or logged. You can also specify that the interface be shut down or temporarily disabled.
- Allowed MAC addresses—You configure specific "allowed" MAC addresses for the access interface. Any MAC address that is not in the list of configured addresses is not learned, and the switch logs an appropriate message. The allowed MAC method binds MAC addresses to a VLAN so that the address is not registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.

This topic includes the following tasks:

1. Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly on page 241
2. Verifying That Allowed MAC Addresses Are Working Correctly on page 242
3. Verifying That Interfaces Are Shut Down on page 242
4. Customizing the Ethernet Switching Table Display to View Information for a Specific Interface on page 243

Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly

Purpose Verify that MAC limiting for dynamic MAC addresses is working.

Action Display the MAC addresses that have been learned. The following sample output shows the results of sending two packets from hosts connected to **xe-1:0/0/1** and five packets from hosts connected to **xe-1:0/0/2**, with both interfaces configured with a MAC limit of **4** and the action **drop**:

```
user@switch> show ethernet-switching table
Ethernet-switching table:  7 entries, 6 learned
  VLAN                MAC address         Type         Age    Interfaces

  employee-vlan       *                   Flood          -    xe-1:0/0/2.0
  employee-vlan       00:05:85:3A:82:77   Learn          0    xe-1:0/0/1.0
  employee-vlan       00:05:85:3A:82:79   Learn          0    xe-1:0/0/1.0
  employee-vlan       00:05:85:3A:82:80   Learn          0    xe-1:0/0/2.0
  employee-vlan       00:05:85:3A:82:81   Learn          0    xe-1:0/0/2.0
  employee-vlan       00:05:85:3A:82:83   Learn          0    xe-1:0/0/2.0
  employee-vlan       00:05:85:3A:82:85   Learn          0    xe-1:0/0/2.0
```

Meaning The output shows that the fifth packet received on the **xe-1:0/0/2** interface was dropped because it exceeded the MAC limit for that interface. The address was not learned, and thus an asterisk (*) rather than an address appears in the MAC address column in the first line of the sample output.

Verifying That Allowed MAC Addresses Are Working Correctly

Purpose Verify that allowed MAC addresses are working.

Action Display the MAC cache information after allowed MAC addresses have been configured on an interface. The following sample shows the MAC cache after four allowed MAC addresses had been configured on interface **xe-1:0/0/2** and a fifth MAC address appeared on the interface.

```
user@switch> show ethernet-switching table
Ethernet-switching table:  5 entries, 4 learned
  VLAN                MAC address         Type         Age    Interfaces

  employee-vlan       00:05:85:3A:82:80   Learn          0    xe-1:0/0/2.0
  employee-vlan       00:05:85:3A:82:81   Learn          0    xe-1:0/0/2.0
  employee-vlan       00:05:85:3A:82:83   Learn          0    xe-1:0/0/2.0
  employee-vlan       00:05:85:3A:82:85   Learn          0    xe-1:0/0/2.0
  employee-vlan       *                   Flood          -    xe-1:0/0/2.0
```

Meaning Because the fifth address was not allowed it was not learned, and an asterisk (*) rather than an address appears in the MAC address column in the last line of the sample output.

Verifying That Interfaces Are Shut Down

Purpose Verify that an interface is shut down when the MAC limit is exceeded.

Action For more information about interfaces that have been shut down because the MAC limit was exceeded, use the **show ethernet-switching interfaces** command.

```
user@switch> show ethernet-switching interfaces
Interface    State  VLAN members        Tag   Tagging  Blocking


bme0.32770     down   mgmt     untagged unblocked

xe-0/0/0.0     down   v1       untagged MAC limit exceeded

xe- 0/0/1.0      up     v1       untagged unblocked

xe-0/0/2.0      up     v1       untagged unblocked

me0.0          up     mgmt     untagged unblocked
```

NOTE: You can configure interfaces to recover automatically when the MAC limit has been exceeded by specifying the **port-error-disable** statement with a **disable timeout** value. The switch automatically restores the disabled interface to service when the disable timeout expires. The **port-error-disable** configuration does not apply to preexisting error conditions—it affects only error conditions that are detected after the **port-error-disable** statement has been enabled and the configuration has been committed. To clear a preexisting error condition and restore the interface to service, use the clear ethernet-switching port-error command.

Customizing the Ethernet Switching Table Display to View Information for a Specific Interface

Purpose You can use the **show ethernet-switching table** command to view information for a specific interface.

Action For example, to display the MAC addresses that have been learned on the **xe-0/0/2** interface, enter:

```
user@switch> show ethernet-switching table interface xe-0/0/2.0
Ethernet-switching table: 1 unicast entries

  VLAN              MAC address       Type         Age Interfaces

  v1                *                 Flood          - All-members

  v1                00:00:06:00:00:00 Learn          0 xe-0/0/2.0
```

Meaning The MAC limit value for the **xe-0/0/2** interface had been set to **1**, and the output shows that only one MAC address was learned and added to the MAC cache.

Related Documentation

- Configuring MAC Limiting on page 134
- Monitoring Port Security on page 237
- *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 111
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 88

Verifying That MAC Move Limiting Is Working Correctly

Purpose Verify that MAC move limiting is working on the switch.

Action Display the MAC addresses in the Ethernet switching table when MAC move limiting has been configured for a VLAN. The following sample shows the results after two of the hosts on **ge-0/0/2** sent packets after the MAC addresses for those hosts had moved to other interfaces more than five times in 1 second. The VLAN, **employee-vlan**, was set to a MAC move limit of **5** with the action **drop**:

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

Ethernet-switching table:  7 entries, 4 learned
  VLAN                MAC address         Type         Age    Interfaces

  employee-vlan       00:05:85:3A:82:77   Learn          0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:79   Learn          0    ge-0/0/1.0
  employee-vlan       00:05:85:3A:82:80   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:81   Learn          0    ge-0/0/2.0
  employee-vlan       *                   Flood          -    ge-0/0/2.0
  employee-vlan       *                   Flood          -    ge-0/0/2.0
```

Meaning The last two lines of the sample output show that MAC addresses for two hosts on **ge-0/0/2** were not learned, because the hosts had been moved back and forth from the original interfaces more than five times in 1 second.

Related Documentation

- Configuring MAC Move Limiting (CLI Procedure) on page 136
- *Configuring MAC Move Limiting (J-Web Procedure)*
- *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*
- Example: Configuring Basic Port Security Features on page 79
- Monitoring Port Security on page 237

Verifying That the Port Error Disable Setting Is Working Correctly

Purpose Verify that the port error disable setting is working as expected for MAC limited and storm control interfaces.

Action Display information about interfaces:

```
user@switch> show ethernet-switching interfaces
Interface        State    VLAN members          Blocking
xe-2:0/0/0.0  up       T1122                 unblocked
xe-2:0/0/1.0  down     default               MAC limit exceeded
xe-2:0/0/2.0  down     default               Storm control in effect
xe-2:0/0/3.0  down     default               unblocked
xe-2:0/0/4.0  down     default               unblocked
xe-2:0/0/5.0  down     default               unblocked
xe-2:0/0/6.0  down     default               unblocked
```

Meaning For interfaces disabled by port security features, the sample output from the **show ethernet-switching interfaces** command specifies the reasons that the interfaces are disabled:

- **MAC limit exceeded**—The interface is temporarily disabled because of a mac-limit error. The disabled interface is automatically restored to service when the disable-timeout (Port Error Disable) expires.
- **MAC move limit exceeded**—The interface is temporarily disabled because of a *mac-move-limit* error. The disabled interface is automatically restored to service when the *disable-timeout* expires.
- **Storm control in effect**—The interface is temporarily disabled because of a storm-control error. The disabled interface is automatically restored to service when the disable-timeout (Port Error Disable) expires.

Related Documentation

- Understanding MAC Limiting and MAC Move Limiting for Port Security on page 61
- port-error-disable on page 208
- Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure) on page 138

Verifying That a Trusted DHCP Server Is Working Correctly

Purpose Verify that a DHCP trusted server is working on the switch. See what happens when the DHCP server is trusted and then untrusted.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch>  show dhcp snooping binding
DHCP Snooping Information:
MAC Address         IP Address    Lease    Type     VLAN          Interface
-----------------   ----------    -----    ----     ----          ---------
00:05:85:3A:82:77    192.0.2.17    600    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:79    192.0.2.18    653    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:80    192.0.2.19    720    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:3A:82:81    192.0.2.20    932    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:3A:82:83    192.0.2.21   1230    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:27:32:88    192.0.2.22   3200    dynamic  employee-vlan   ge-0/0/2.0
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

If the DHCP server had been configured as untrusted, no entries would be added to the DHCP snooping database and nothing would be shown in the output of the **show dhcp snooping binding** command.

Related Documentation

- Enabling a Trusted DHCP Server (CLI Procedure) on page 144
- Enabling a Trusted Port for DHCP on page 145
- *Enabling a Trusted DHCP Server (J-Web Procedure)*
- Example: Configuring Basic Port Security Features on page 79
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 95
- Monitoring Port Security on page 237
- *Troubleshooting Port Security*

Verifying That Three-Color Policers Are Operational

Purpose Verify that three-color policers in firewall filter configurations are working properly.

Action Use the following operational mode commands to verify that a three-color policer is working properly:

- **show class-of-service forwarding-table classifiers**
- **show interfaces *interface-name* extensive**
- **show interfaces queue *interface-name***

Related Documentation

- Overview of Policers on page 35
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128

Verifying That Two-Color Policers Are Operational

Purpose Verify that two-color policers in firewall filter configurations are working properly.

Action Use the **show firewall policer** operational mode command to verify that the policers are working properly:

```
user@switch> show firewall policer
Filter: egress-vlan-watch-employee
Filter: ingress-port-filter
Filter: ingress-port-limit-tcp-icmp
Policers:
Name                                                Packets
icmp-connection-policer                                  10
tcp-connection-policer                                  539
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

Meaning The **show firewall policer** command displays the names of all firewall filters and policers that are configured. For each policer that is specified in a filter configuration, the output field shows the current packet count for all packets that exceed the specified rate limits.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 128
- Configuring Firewall Filters on page 121
- Monitoring Firewall Filter Traffic on page 235

CHAPTER 14

Monitoring Commands

clear arp inspection statistics

Syntax clear arp inspection statistics
<interface *interface*>

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description Clear ARP inspection statistics.

Options **none**—Clears ARP statistics on all interfaces.

interface *interface-names*—(Optional) Clear ARP statistics on one or more interfaces.

Required Privilege Level clear

Related Documentation
- show arp inspection statistics on page 254
- Example: Configuring Basic Port Security Features on page 79
- Verifying That DAI Is Working Correctly on page 239

List of Sample Output clear arp inspection statistics on page 250

Output Fields This command produces no output.

Sample Output

clear arp inspection statistics

```
user@switch> clear arp inspection statistics
```

clear dhcp snooping binding

Syntax
clear dhcp snooping binding
<mac (all | *mac-address*)>
<vlan (all | *vlan-name*)>
<vlan (all | *vlan-name*) mac (all | *mac-address*)>

Release Information
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description
Clear the DHCP snooping database information.

Options
mac (all | *mac-address*)—(Optional) Clear DHCP snooping information for the specified MAC address or all MAC addresses.

vlan (all | *vlan-name*)—(Optional) Clear DHCP snooping information for the specified VLAN or all VLANs.

Required Privilege Level
clear

Related Documentation
- Example: Configuring Basic Port Security Features on page 79
- show dhcp snooping binding on page 255

List of Sample Output
clear dhcp snooping binding on page 251

Output Fields
This command produces no output.

Sample Output

clear dhcp snooping binding

```
user@switch> clear dhcp snooping binding
```

clear ethernet-switching port-error

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

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.

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

Options

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

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

Required Privilege Level clear

Related Documentation

- Configuring MAC Limiting on page 134
- Example: Configuring Storm Control to Prevent Network Outages on page 87
- Configuring Port Security (CLI Procedure) on page 131
- **port-error-disable on page 208**
- Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure) on page 138

Output Fields This command produces no output.

clear firewall

Syntax clear firewall (all | counter *counter-name* | filter *filter-name*)

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Clear statistics provided by firewall filters.

When you clear the counters of a filter, this not only impacts the counters shown by the CLI, but also the ones tracked by SNMP 2.

Options

all—Clear the packet and byte counts for all firewall filter counters and clear the packet counts for all policer counters.

counter *counter-name*—Clear the packet and byte counts for the specified firewall filter counter.

filter *filter-name*—Clear the packet and byte counts for the specified firewall filter.

Required Privilege Level clear

Related Documentation

- Verifying That Firewall Filters Are Operational on page 238
- Verifying That Two-Color Policers Are Operational on page 246
- Overview of Firewall Filters on page 3
- Overview of Policers on page 35

Sample Output

clear firewall all

```
user@switch> clear firewall all
```

clear firewall counter

```
user@switch> clear firewall counter port-filter-counter
```

clear firewall filter

```
user@switch> clear firewall filter ingress-port-filter
```

show arp inspection statistics

Syntax show arp inspection statistics

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description Display ARP inspection statistics.

Required Privilege Level view

Related Documentation

- clear arp inspection statistics on page 250
- Example: Configuring Basic Port Security Features on page 79
- Verifying That DAI Is Working Correctly on page 239

List of Sample Output show arp inspection statistics on page 254

Output Fields Table 22 on page 254 lists the output fields for the **show arp inspection statistics** command. Output fields are listed in the approximate order in which they appear.

Table 22: show arp inspection statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which ARP inspection has been applied.	All levels
Packets received	Total number of packets total that underwent ARP inspection.	All levels
ARP inspection pass	Total number of packets that passed ARP inspection.	All levels
ARP inspection failed	Total number of packets that failed ARP inspection.	All levels

Sample Output

show arp inspection statistics

```
user@switch> show arp inspection statistics

Interface     Packets received     ARP inspection pass  ARP inspection failed
---------     ----------------     -------------------  ---------------------
  ge-0/0/0                   0                       0                     0
  ge-0/0/1                   0                       0                     0
  ge-0/0/2                   0                       0                     0
  ge-0/0/3                   0                       0                     0
  ge-0/0/4                   0                       0                     0
  ge-0/0/5                   0                       0                     0
  ge-0/0/6                   0                       0                     0
  ge-0/0/7                 703                     701                     2
```

show dhcp snooping binding

Syntax **show dhcp snooping binding**
<interface *interface-name*>
<vlan *vlan-name*>

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description Display the DHCP snooping database information.

Options **interface *interface-name***—(Optional) Display the DHCP snooping database information for an interface.

vlan *vlan-name*—(Optional) Display the DHCP snooping database information for a VLAN.

Required Privilege Level view

Related Documentation
- *clear dhcp snooping binding*
- Example: Configuring Basic Port Security Features on page 79
- Verifying That DHCP Snooping Is Working Correctly on page 239

List of Sample Output show dhcp snooping binding on page 255

Output Fields Table 23 on page 255 lists the output fields for the **show dhcp snooping binding** command. Output fields are listed in the approximate order in which they appear.

Table 23: show dhcp snooping binding Output Fields

Field Name	Field Description	Level of Output
MAC Address	MAC address of the network device; bound to the IP address.	All levels
IP Address	IP address of the network device; bound to the MAC address.	All levels
Lease	Lease granted to the IP address.	All levels
Type	How the MAC address was acquired.	All levels
VLAN	VLAN name of the network device whose MAC address is shown.	All levels
Interface	Interface address (port).	All levels

Sample Output

show dhcp snooping binding

```
user@switch> show dhcp snooping binding
```

```
DHCP Snooping Information:
MAC Address             IP Address Lease   Type     VLAN    Interface
-----------------       ---------- -----   -------  ----    ---------
00:00:01:00:00:03       192.0.2.0  640     dynamic  guest    ge-0/0/12.0
00:00:01:00:00:04       192.0.2.1  720     dynamic  guest    ge-0/0/12.0
00:00:01:00:00:05       192.0.2.5  800     dynamic  guest    ge-0/0/13.0
```

show firewall

Syntax

show firewall
<counter *counter-name*>
<filter *filter-name*>
<log <detail | interface *interface-name*>>
<terse>

Release Information

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

Description

Display statistics about configured firewall filters.

Options

counter *counter-name*—(Optional) Display statistics about a particular firewall filter counter.

filter *filter-name*—(Optional) Display statistics about a particular firewall filter.

log—(Optional) Display log entries for all firewall filter activity.

terse—(Optional) Display firewall filter names only.

Required Privilege Level

view

Related Documentation

- Verifying That Firewall Filters Are Operational on page 238
- Verifying That Two-Color Policers Are Operational on page 246
- Overview of Firewall Filters on page 3
- Overview of Policers on page 35

List of Sample Output

show firewall on page 258
show firewall filter filter-name on page 259
show firewall counter counter-name on page 259
show firewall log on page 259
show firewall log detail on page 259

Output Fields

Table 24 on page 257 lists the output fields for the **show firewall** command. Output fields are listed in the approximate order in which they appear.

Table 24: show firewall Output Fields

Field Name	Field Description	Level of Output
Filter	Name of the filter that is configured at the **[edit firewall family *family-name* filter]** hierarchy level.	All levels

Table 24: show firewall Output Fields *(continued)*

Field Name	Field Description	Level of Output
Counters	Display filter counter information: • Name—Name of a filter counter that has been configured with the **count** firewall filter action modifier. • Bytes—Number of bytes that match the filter term where the **count** action modifier was specified. • Packets—Number of packets that matched the filter term where the **count** action modifier was specified.	All levels
Policers	Display policer information: • Name—Name of the policer that is configured at the **[edit firewall policer]** hierarchy level. • Packets—Number of packets that matched the filter term where the **policer** action modifier was specified. This is the number of packets that exceeded the rate limits that the policer specifies.	All levels
Action	Filter action: • **A**—Accept • **D**—Discard	All levels
Interface	Interface on which the firewall filter is applied.	All levels
Protocol	Name of the packet protocol.	All levels
Packet Length	Length of the packet.	All levels
Src Addr	Source address of the packet.	All levels
Dest Addr	Destination address of the packet.	All levels

Sample Output

show firewall

```
user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name                                                Bytes              Packets
counter-employee-web                                    0                    0
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
Policers:
Name                                               Packets
icmp-connection-policer                                10
tcp-connection-policer                                  0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

show firewall filter filter-name

```
user@switch> show firewall filter ingress-port-limit-tcp-icmp
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
Policers:
Name                                               Packets
icmp-connection-policer                                 10
tcp-connection-policer                                   0
```

show firewall counter counter-name

```
user@switch> show firewall counter icmp-counter
Filter: ingress-port-voip-class-filter
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
```

show firewall log

```
user@switch> show firewall log
Log :

Time      Filter    Action Interface     Protocol        Src Addr
          Dest Addr
08:00:53  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:52  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:51  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:50  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:49  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:48  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:47  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
```

show firewall log detail

```
user@switch> show firewall log detail
Log :

Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0Name of protocol: TCP, Packet Length: 50824, Source address:
172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 1020, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
```

```
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
```

show firewall policer

Syntax show firewall policer
<policer-name>

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Display statistics about configured policers.

Options **none**—Display the count of policed packets for all configured policers.

policer-name—(Optional) Display the count of policed packets for the specified policer.

Required Privilege Level view

Related Documentation
- Verifying That Firewall Filters Are Operational on page 238
- Verifying That Two-Color Policers Are Operational on page 246
- Overview of Firewall Filters on page 3
- Overview of Policers on page 35

List of Sample Output
show firewall policer on page 261
show firewall policer policer-name on page 262

Output Fields Table 25 on page 261 lists the output fields for the **show firewall policer** command. Output fields are listed in the approximate order in which they appear.

Table 25: show firewall policer Output Fields

Field Name	Field Description	Level of Output
Filter	Name of the filter that is configured at the **[edit firewall family *family-name* filter]** hierarchy level.	All levels
Policers	Display policer information: • Filter—Name of filter that specifies the **policer** action modifier. • Name—Name of policer. • Packets—Number of packets that matched the filter term in which the **policer** action modifier is specified. This is the number of packets that exceed the rate limits that the policer specifies.	All levels

Sample Output

show firewall policer

```
user@switch> show firewall policer
Filter: egress-vlan-filter
Filter: ingress-port-filter
Policers:
Name                                                Packets
```

```
icmp-connection-policer                                0
tcp-connection-policer                                 0
Filter: ingress-vlan-rogue-block
```

show firewall policer policer-name

```
user@switch> show firewall policer tcp-connection-policer
Filter: ingress-port-filter
Policers:
Name                                                Packets
tcp-connection-policer                                    0
```

show interfaces filters

Syntax show interfaces filters
<*interface-name*>

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Display firewall filters that are configured on each interface in a switch.

Options **none**—Display firewall filter information about all interfaces.

interface-name—(Optional) Display firewall filter information about a particular interface.

Required Privilege Level view

Related Documentation
- show firewall on page 257

List of Sample Output
show interfaces filters on page 263
show interfaces filters interface-name on page 264

Output Fields Table 26 on page 263 lists the output fields for the **show interfaces filters** command. Output fields are listed in the approximate order in which they appear.

Table 26: show interfaces filters Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the physical interface.	All levels
Admin	Interface state: **up** or **down**.	All levels
Link	Link state: **up** or **down**.	All levels
Proto	Protocol that is configured on the interface.	All levels
Input Filter	Name of the firewall filter to be evaluated when packets are received on the interface.	All levels
Output Filter	Name of the firewall filter to be evaluated when packets are transmitted on the interface.	All levels

Sample Output

show interfaces filters

```
user@switch> show interfaces filters
Interface       Admin Link Proto Input Filter         Output Filter
ge-0/0/6        up    up
ge-0/0/6.0      up    up   eth-switch ingress-port-limit-tcp-icmp
ge-0/0/7        up    down
ge-0/0/8        up    down
```

```
ge-0/0/9        up    down
ge-0/0/10       up    down
ge-0/0/10.0     up    down
```

show interfaces filters interface-name

```
user@switch> show interfaces filters ge-0/0/6
Interface       Admin Link Proto Input Filter         Output Filter
ge-0/0/6        up    up
ge-0/0/6.0      up    up eth-switch ingress-port-limit-tcp-icmp
```

PART 4

Troubleshooting

CHAPTER 15

Troubleshooting Procedures

Troubleshooting Firewall Filter Configuration

Use the following information to troubleshoot your firewall filter configuration.

Firewall Filter Configuration Returns a No Space Available in TCAM Message

Problem **Description:** When a firewall filter configuration exceeds the amount of available Ternary Content Addressable Memory (TCAM) space, the system returns the following **syslogd** message:

```
No space available in tcam.
Rules for filter filter-name will not be installed.
```

A switch returns this message during the commit operation if the firewall filter that has been applied to a port, VLAN, or Layer 3 interface exceeds the amount of space available in the TCAM table. The filter is not applied, but the commit operation for the firewall filter configuration is completed in the CLI module.

Solution When a firewall filter configuration exceeds the amount of available TCAM table space, you must configure a new firewall filter with fewer filter terms so that the space requirements for the filter do not exceed the available space in the TCAM table.

You can perform either of the following procedures to correct the problem:

To delete the filter and its binding and apply the new smaller firewall filter to the same binding:

1. Delete the filter and its binding to ports, VLANs, or Layer 3 interfaces. For example:

   ```
   [edit]
   user@switch# delete firewall family ethernet-switching filter ingress-vlan-rogue-block
   user@switch# delete vlans employee-vlan description "filter to block rogue devices on
   employee-vlan"
   user@switch# delete vlans employee-vlan filter input ingress-vlan-rogue-block
   ```
2. Commit the changes:

   ```
   [edit]
   user@switch# commit
   ```
3. Configure a smaller filter with fewer terms that does not exceed the amount of available TCAM space. For example:

   ```
   [edit]
   user@switch# set firewall family ethernet-switching filter new-ingress-vlan-rogue-block ...
   ```
4. Apply (bind) the new firewall filter to a port, VLAN , or Layer 3 interface. For example:

   ```
   [edit]
   user@switch# set vlans employee-vlan description "filter to block rogue devices on
   employee-vlan"
   user@switch# set vlans employee-vlan filter input new-ingress-vlan-rogue-block
   ```
5. Commit the changes:

   ```
   [edit]
   user@switch# commit
   ```

To apply a new firewall filter and overwrite the existing binding but not delete the original filter:

1. Configure a firewall filter with fewer terms than the original filter:

   ```
   [edit]
   user@switch# set firewall family ethernet-switching filter new-ingress-vlan-rogue-block...
   ```
2. Apply the firewall filter to the port, VLAN, or Layer 3 interfaces to overwrite the binding of the original filter—for example:

   ```
   [edit]
   user@switch# set vlans employee-vlan description "smaller filter to block rogue devices on
   employee-vlan"
   user@switch# set vlans employee-vlan filter input new-ingress-vlan-rogue-block
   ```

   Because you can apply no more than one firewall filter per VLAN per direction, the binding of the original firewall filter to the VLAN is overwritten with the new firewall filter **new-ingress-vlan-rogue-block**.
3. Commit the changes:

   ```
   [edit]
   user@switch# commit
   ```

NOTE: The original filter is not deleted and is still available in the configuration.

Filter Counts Previously Dropped Packet

Problem **Description:** If you configure two or more filters in the same direction for a physical interface and one of the filters includes a counter, the counter will be incorrect if the following circumstances apply:

- You configure the filter that is applied to packets first to discard certain packets. For example, imagine that you have a VLAN filter that accepts packets sent to 10.10.1.0/24 addresses and implicitly discards packets sent to any other addresses. You apply the filter to the **admin** VLAN in the output direction, and interface xe-0/0/1 is a member of that VLAN.
- You configure a subsequent filter to accept and count packets that are dropped by the first filter. In this example, you have a port filter that accepts and counts packets sent to 192.168.1.0/24 addresses that is also applied to xe-0/0/1 in the output direction.

The egress VLAN filter is applied first and correctly discards packets sent to 192.168.1.0/24 addresses. The egress port filter is applied next and counts the discarded packets as matched packets. The packets are not forwarded, but the counter displayed by the egress port filter is incorrect.

Remember that the order in which filters are applied depends on the direction in which they are applied, as indicated here:

Ingress filters:

1. Port (Layer 2) filter
2. VLAN filter
3. Router (Layer 3) filter

Egress filters:

1. Router (Layer 3) filter
2. VLAN filter
3. Port (Layer 2) filter

Solution This is expected behavior.

Matching Packets Not Counted

Problem **Description:** If you configure two egress filters with counters for a physical interface and a packet matches both of the filters, only one of the counters includes that packet.

For example:

- You configure an egress port filter with a counter for interface xe-0/0/1.
- You configure an egress VLAN filter with a counter for the **admin**VLAN, and interface xe-0/0/1 is a member of that VLAN.
- A packet matches both filters.

In this case, the packet is counted by only one of the counters even though it matched both filters.

Solution This is expected behavior.

Counter Reset When Editing Filter

Problem **Description:** If you edit a firewall filter term, the value of any counter associated with any term in the same filter is set to 0, including the implicit counter for any policer referenced by the filter. Consider the following examples:

- Assume that your filter has **term1**, **term2**, and **term3**, and each term has a counter that has already counted matching packets. If you edit any of the terms in any way, the counters for all the terms are reset to 0.
- Assume that your filter has **term1** and **term2**. Also assume that **term2** has a **policer** action modifier and the implicit counter of the policer has already counted 1000 matching packets. If you edit **term1** or **term2** in any way, the counter for the policer referenced by **term2** is reset to 0.

Solution This is expected behavior.

Cannot Include loss-priority and policer Actions in Same Term

Problem **Description:** You cannot include both of the following actions in the same firewall filter term in a QFX Series switch:

- **loss-priority**
- **policer**

If you do so, you see the following error message when you attempt to commit the configuration: “cannot support policer action if loss-priority is configured.”

Solution This is expected behavior.

Cannot Egress Filter Certain Traffic Originating on QFX Switch

Problem **Description:** On a QFX Series switch, you cannot filter certain traffic with a firewall filter applied in the output direction if the traffic originates on the QFX switch. This limitation applies to control traffic for protocols such as ICMP (ping), STP, LACP, and so on.

Solution This is expected behavior.

Firewall Filter Match Condition Not Working with Q-in-Q Tunneling

Problem **Description:** If you create a firewall filter that includes a match condition of **dot1q-tag** or **dot1q-user-priority** and apply the filter on input to a trunk port that participates in a service VLAN, the match condition does not work if the Q-in-Q EtherType is not 0x8100. (When Q-in-Q tunneling is enabled, trunk interfaces are assumed to be part of the service provider or data center network and therefore participate in service VLANs.)

Solution This is expected behavior. To set the Q-in-Q EtherType to 0x8100, enter the **set dot1q-tunneling ethertype 0x8100** statemen at the **[edit ethernet-switching-options]** hierarchy level. You must also configure the other end of the link to use the same Ethertype.

Egress Firewall Filters with Private VLANs

Problem **Description:** If you apply a firewall filter in the output direction to a primary VLAN, the filter also applies to the secondary VLANs that are members of the primary VLAN when the traffic egresses with the primary VLAN tag or isolated VLAN tag, as listed below:

- Traffic forwarded from a secondary VLAN trunk port to a promiscuous port (trunk or access)
- Traffic forwarded from a secondary VLAN trunk port that carries an isolated VLAN to a PVLAN trunk port.
- Traffic forwarded from a promiscuous port (trunk or access) to a secondary VLAN trunk port
- Traffic forwarded from a PVLAN trunk port. to a secondary VLAN trunk port
- Traffic forwarded from a community port to a promiscuous port (trunk or access)

If you apply a firewall filter in the output direction to a primary VLAN, the filter does *not* apply to traffic that egresses with a community VLAN tag, as listed below:

- Traffic forwarded from a community trunk port to a PVLAN trunk port
- Traffic forwarded from a secondary VLAN trunk port that carries a community VLAN to a PVLAN trunk port
- Traffic forwarded from a promiscuous port (trunk or access) to a community trunk port
- Traffic forwarded from a PVLAN trunk port. to a community trunk port

If you apply a firewall filter in the output direction to a community VLAN, the following behaviors apply:

- The filter is applied to traffic forwarded from a promiscuous port (trunk or access) to a community trunk port (because the traffic egresses with the community VLAN tag).
- The filter is applied to traffic forwarded from a community port to a PVLAN trunk port (because the traffic egresses with the community VLAN tag).

- The filter is *not* applied to traffic forwarded from a community port to a promiscuous port (because the traffic egresses with the primary VLAN tag or untagged).

Solution These are expected behaviors. They occur only if you apply a firewall filter to a private VLAN in the output direction and do not occur if you apply a firewall filter to a private VLAN in the input direction.

Egress Filtering of L2PT Traffic Not Supported

Problem **Description:** Egress filtering of L2PT traffic is not supported on the QFX3500 switch. That is, if you configure L2PT to tunnel a protocol on an interface, you cannot also use a firewall filter to filter traffic for that protocol on that interface in the output direction. If you commit a configuration for this purpose, the firewall filter is not applied to the L2PT-tunneled traffic.

Solution This is expected behavior.

Cannot Drop BGP Packets in Certain Circumstances

Problem **Description:** BGP packets with a time-to-live (TTL) value greater than 1 cannot be discarded using a firewall filter applied to a loopback interface or applied on input to a Layer 3 interface. BGP packets with TTL value of 1 or 0 can be discarded using a firewall filter applied to a loopback interface or applied on input to a Layer 3 interface.

Solution This is expected behavior.

Invalid Statistics for Policer

Problem **Description:** If you apply a single-rate two-color policer in more than 128 terms in a firewall filter, the output of the **show firewall** command displays incorrect data for the policer.

Solution This is expected behavior.

Policers can Limit Egress Filters

Problem **Description:** The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional

egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters. Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms, 1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.
- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
  - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
  - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

Solution You can prevent this problem by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.
- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.

Related Documentation

- *Understanding FIP Snooping, FBF, and MVR Filter Scalability*
- Configuring Firewall Filters on page 121
- Verifying That Firewall Filters Are Operational on page 238

Troubleshooting Policer Configuration

- Incomplete Count of Packet Drops on page 274
- Counter Reset When Editing Filter on page 274
- Invalid Statistics for Policer on page 274
- Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured on page 274

- Filter-Specific Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured on page 275
- Policers Can Limit Egress Filters on page 276

Incomplete Count of Packet Drops

Problem **Description:** Under certain circumstances, Junos OS might display a misleading number of packets dropped by an ingress policer.

If packets are dropped because of ingress admission control, policer statistics might not show the number of packet drops you would expect by calculating the difference between ingress and egress packet counts. This might happen if you apply an ingress policer to multiple interfaces, and the aggregate ingress rate of those interfaces exceeds the line rate of a common egress interface. In this case, packets might be dropped from the ingress buffer. These drops are not included in the count of packets dropped by the policer, which causes policer statistics to underreport the total number of drops.

Solution This is expected behavior.

Counter Reset When Editing Filter

Problem **Description:** If you edit a firewall filter term, the value of any counter associated with any term in the same filter is set to 0, including the implicit counter for any policer referenced by the filter. Consider the following examples:

- Assume that your filter has **term1**, **term2**, and **term3**, and each term has a counter that has already counted matching packets. If you edit any of the terms in any way, the counters for all the terms are reset to 0.
- Assume that your filter has **term1** and **term2**. Also assume that **term2** has a **policer** action modifier and the implicit counter of the policer has already counted 1000 matching packets. If you edit **term1** or **term2** in any way, the counter for the policer referenced by **term2** is reset to 0.

Solution This is expected behavior.

Invalid Statistics for Policer

Problem **Description:** If you apply a single-rate two-color policer in more than 128 terms in a firewall filter, the output of the **show firewall** command displays incorrect data for the policer.

Solution This is expected behavior.

Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured

Problem **Description:** If you configure a policer to rate-limit throughput and apply it on egress to multiple interfaces on a QFX3500 switch or Node, the measured aggregate policed rate might be twice the configured rate, depending on which interfaces you apply the policer

to. The doubling of the policed rate occurs if you apply a policer to multiple interfaces and *both* of the following are true:

- There is at least one policed interface in the range xe-0/0/0 to xe-0/0/23 or the range xe-0/1/1 to xe-0/1/7.
- There is at least one policed interface in the range xe-0/0/24 to xe-0/0/47 or the range xe-0/1/8 to xe-0/1/15.

For example, if you configure a policer to rate-limit traffic at 1 Gbps and apply the policer (by using a firewall filter) to xe-0/0/0 and xe-0/0/24 in the output direction, each interface is rate-limited at 1 Gbps, for a total allowed throughput of 2 Gbps. The same behavior occurs if you apply the policer to xe-0/1/1 and xe-0/0/24—each interface is rate-limited at 1 Gbps.

If you apply the same policer on egress to multiple interfaces in these groups, each *group* is rate-limited at 1 Gbps. For example, if you apply the policer to xe-0/0/0 through xe-0/0/4 (five interfaces) and xe-0/0/24 through xe-0/0/33 (ten interfaces), each group is rate-limited at 1 Gbps, for a total allowed throughput of 2 Gbps.

Here is another example: If you apply the policer to xe-0/0/0 through xe-0/0/4 and xe-0/1/1 through xe-0/1/5 (a total of ten interfaces), that group is rate-limited at 1 Gbps in aggregate. If you also apply the policer to xe-0/0/24, that one interface is rate-limited at 1 Gbps while the other ten are still rate-limited at 1 Gbps in aggregate.

Interfaces xe-0/1/1 through xe-0/1/15 are physically located on the QSFP+ uplink ports, according to the following scheme:

- xe-0/1/1 through xe-0/1/3 are on Q0.
- xe-0/1/4 through xe-0/1/7 are on Q1.
- xe-0/1/8 through xe-0/1/11 are on Q2.
- xe-0/1/2 through xe-0/1/15 are on Q3.

The doubling of the policed rate occurs only if the policer is applied in the output direction. If you configure a policer as described above but apply it in the input direction, the total allowed throughput for all interfaces is 1 Gbps.

Solution This is expected behavior.

Filter-Specific Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured

Problem **Description:** You can configure policers to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps. However, the behavior of a filter-specific policer is affected by how the firewall filter terms that reference the policer are stored in ternary content addressable memory (TCAM). If you create a filter-specific policer and reference it in multiple firewall filter terms, the policer allows more traffic than expected

if the terms are stored in different TCAM slices. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms that are stored in three separate memory slices, the total bandwidth allowed by the filter is 3 Gbps, not 1 Gbps.

Solution To prevent this unexpected behavior, use the information about TCAM slices presented in "Planning the Number of Firewall Filters to Create" on page 29 to organize your configuration file so that all the firewall filter terms that reference a given filter-specific policer are stored in the same TCAM slice.

Policers Can Limit Egress Filters

Problem **Description:** The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters.

Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms, 1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.
- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
  - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
  - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

Solution You can prevent this problem by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.

- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.