Junos® OS

Layer 2 Security Feature Guide

Modified: 2017-12-17

Copyright © 2017, Juniper Networks, Inc.

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

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

Junos® OS Layer 2 Security Feature Guide

Copyright © 2017 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation xi
Documentation and Release Notes xi
Supported Platforms xi
Using the Examples in This Manual xi
Merging a Full Example xii
Merging a Snippet xii
Documentation Conventions xiii
Documentation Feedback xv
Requesting Technical Support xv
Self-Help Online Tools and Resources xv
Opening a Case with JTAC xvi

Chapter 1 **Configuring Layer 2 Port Security 17**

Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity 18
Configuring Port Security to Protect Access Ports on the Device Against Loss of Information and Productivity (CLI Procedure) 20
Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing (CLI Procedure) 23
Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) 23
Understanding Dynamic ARP Inspection for Protecting Switching Devices Against ARP Spoofing 24
Address Resolution Protocol 24
ARP Spoofing 25
Dynamic ARP Inspection 25
Prioritizing Inspected Packets 26
Configuring Dynamic ARP Inspection to Protect Switching Devices Against ARP Spoofing (CLI Procedure) 27
Understanding Trusted DHCP Servers for Port Security 27
Configuring a DHCP Server on a Trusted Interface to Protect it Against Rogue DHCP Servers Sending Leases (CLI Procedure) 28
Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices 28
DHCP Snooping Basics 29
DHCP Snooping Process 30
DHCPv6 Snooping 31
Rapid Commit for DHCPv6 31

Copyright © 2017, Juniper Networks, Inc.

DHCP Server Access . . . 32
Switching Device, DHCP Clients, and DHCP Server Are All on the Same VLAN . . . 32
Switching Device Acts as DHCP Server . . . 33
Switching Device Acts as Relay Agent . . . 34
Static IP Address Additions to the DHCP Snooping Database . . . 35
Snooping DHCP Packets That Have Invalid IP Addresses . . . 35
Prioritizing Snooped Packets . . . 36
Configuring Persistent Bindings in the DHCP or DHCPv6 Snooping Database to Improve Network Performance (CLI Procedure) . . . 36
Understanding DHCP Option 82 for Protecting Switching Devices Against Attacks . . . 39
DHCP Option 82 Overview . . . 39
Suboption Components of Option 82 . . . 40
Switching Device Configurations That Support Option 82 . . . 41
Switching Device, DHCP Clients, and the DHCP Server Are on the Same VLAN or Bridge Domain . . . 41
Switching Device Acts as a Relay Agent . . . 41
DHCPv6 Options . . . 42
Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) . . . 43
Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks . . . 45

Chapter 2 Configuring Layer 2 Device Security . . . 51

Understanding Storm Control for Managing Traffic Levels on Switching Devices . . . 51
Configuring or Disabling Storm Control (CLI Procedure) . . . 53
Configuring Storm Control . . . 55
Disabling Storm Control on Broadcast Traffic . . . 55
Disabling Storm Control on All Multicast Traffic . . . 56
Disabling Storm Control on Registered Multicast Traffic . . . 56
Disabling Storm Control on Unregistered Multicast Traffic . . . 57
Disabling Storm Control on Unknown Unicast Traffic . . . 57
Disabling Storm Control on Multiple Types of Traffic . . . 58
Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) . . . 59
Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers . . . 60

Chapter 3 Configuration Statements for Layer 2 Port Security . . . 65

arp-inspection (MX Series) . . . 66
bridge-domains . . . 67
circuit-id . . . 69
dhcp-security (MX Series) . . . 71
dhcp-service . . . 73
dhcp-snooping-file . . . 74
forwarding-options . . . 75
group (DHCP Security for MX Series) . . . 77
host-name . . . 78

Copyright © 2017, Juniper Networks, Inc.

interface (DHCP Security for MX Series) . . . 79
ip-source-guard (MX Series) . . . 80
mac . . . 81
no-dhcp-snooping . . . 82
no-option82 . . . 83
option-82 . . . 84
overrides (DHCP Security for MX Series) . . . 85
prefix (Circuit ID for Option 82) . . . 86
remote-id (MX Series) . . . 88
routing-instance-name . . . 89
static-ip (MX Series) . . . 90
trusted . . . 90
untrusted . . . 91
use-interface-description . . . 92
use-string . . . 94
use-vlan-id . . . 96
vendor-id . . . 98
write-interval . . . 99

Chapter 4 Configuration Statements for Layer 2 Device Security . . . 101

action-shutdown . . . 102
bandwidth-level . . . 104
bandwidth-percentage . . . 105
icmpv4-rate-limit . . . 106
no-broadcast . . . 107
no-multicast . . . 109
no-registered-multicast . . . 111
no-unknown-unicast . . . 112
no-unregistered-multicast . . . 114
recovery-timeout . . . 115
storm-control . . . 117
storm-control-profiles . . . 118

Chapter 5 Operational Commands for Layer 2 Port Security . . . 119

clear arp . . . 120
clear dhcp-security binding . . . 122
show dhcp-security arp inspection statistics . . . 123
show dhcp-security binding . . . 125
show dhcp-security binding ip-source-guard . . . 128

Chapter 6 Operational Commands for Layer 2 Device Security . . . 131

clear bridge recovery-timeout . . . 132

Copyright © 2017, Juniper Networks, Inc.

Copyright © 2017, Juniper Networks, Inc.

List of Figures

Chapter 1 **Configuring Layer 2 Port Security 17**

Figure 1: DHCP Server Connected Directly to a Switching Device 32
Figure 2: DHCP Server Connected Directly to Switching Device 2, with Switching Device 2 Connected to Switching Device 1 Through a Trusted Trunk Port . . . 33
Figure 3: Switching Device Is the DHCP Server 34
Figure 4: Switching Device Acting as Relay Agent Through Router to DHCP Server 35
Figure 5: DHCP Clients, Switching Device, and the DHCP Server Are All on the Same VLAN or Bridge Domain 41
Figure 6: Switching Device Acting as an Extended Relay Server 42
Figure 7: Switching Device Network Topology for Basic Port Security 46

Chapter 2 **Configuring Layer 2 Device Security 51**

Figure 8: Example Storm Control to Prevent Network Outages 61

Copyright © 2017, Juniper Networks, Inc.

Copyright © 2017, Juniper Networks, Inc.

List of Tables

About the Documentation xi

Table 1: Notice Icons xiii
Table 2: Text and Syntax Conventions xiv

Chapter 1 Configuring Layer 2 Port Security 17

Table 3: DHCPv6 Messages and Equivalent DHCPv4 Messages 31
Table 4: Components of the Port Security Topology 47

Chapter 5 Operational Commands for Layer 2 Port Security 119

Table 5: show dhcp-security arp inspection statistics Output Fields 123
Table 6: show dhcp-security binding Output Fields 126
Table 7: show dhcp-security binding ip-source-guard Output Fields 128

Copyright © 2017, Juniper Networks, Inc.

Copyright © 2017, Juniper Networks, Inc.

About the Documentation

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

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:

- MX Series

Using the Examples in This Manual

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

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

Copyright © 2017, Juniper Networks, Inc.

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; }
   ```


Copyright © 2017, Juniper Networks, Inc.

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 CLI Explorer.

Documentation Conventions

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

Copyright © 2017, Juniper Networks, Inc.

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**
`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

Copyright © 2017, Juniper Networks, Inc.

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

Convention	Description	Examples
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**.
> (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 of the Juniper Networks TechLibrary 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 http://www.juniper.net/techpubs/feedback/.
- 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 Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

Copyright © 2017, Juniper Networks, Inc.

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: http://www.juniper.net/documentation/
- 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://entitlementsearch.juniper.net/entitlementsearch/

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.

Copyright © 2017, Juniper Networks, Inc.

CHAPTER 1

Configuring Layer 2 Port Security

- Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity on page 18
- Configuring Port Security to Protect Access Ports on the Device Against Loss of Information and Productivity (CLI Procedure) on page 20
- Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing (CLI Procedure) on page 23
- Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) on page 23
- Understanding Dynamic ARP Inspection for Protecting Switching Devices Against ARP Spoofing on page 24
- Configuring Dynamic ARP Inspection to Protect Switching Devices Against ARP Spoofing (CLI Procedure) on page 27
- Understanding Trusted DHCP Servers for Port Security on page 27
- Configuring a DHCP Server on a Trusted Interface to Protect it Against Rogue DHCP Servers Sending Leases (CLI Procedure) on page 28
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28
- Configuring Persistent Bindings in the DHCP or DHCPv6 Snooping Database to Improve Network Performance (CLI Procedure) on page 36
- Understanding DHCP Option 82 for Protecting Switching Devices Against Attacks on page 39
- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 45

Copyright © 2017, Juniper Networks, Inc.

Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity

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 device against the loss of information and productivity that such attacks can cause.

The Juniper Networks Junos operating system (Junos OS) provides features to help secure ports on a device. 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 device'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 bridge domain interfaces.

Port security features supported on switching devices are:

- DHCP snooping—Filters and blocks ingress Dynamic Host Configuration Protocol (DHCP) server messages on untrusted ports, and builds and maintains a database of DHCP lease information, which is called the DHCP snooping database.

  NOTE: **DHCP snooping is not enabled in the default configuration of the switching device. DHCP snooping is enabled on a VLAN or bridge domain. The details of enabling DHCP snooping depend on the particular device.**

- DHCPv6 snooping—DHCP snooping for IPv6.
- DHCP option 82—Also known as the DHCP Relay Agent Information option. This DHCPv4 feature helps protect the switching device against attacks such as spoofing 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.
- DHCPv6 option 37—Option 37 is the remote ID option for DHCPv6 and is used to insert information about the network location of the remote host into DHCPv6 packets. You enable option 37 on a VLAN.

  NOTE: **DHCPv6 snooping with option 37 is not supported on the MX Series.**

- DHCPv6 option 18—Option 18 is the circuit ID option for DHCPv6 and is used to insert information about the client port into DHCPv6 packets. This option includes other details that can be optionally configured, such as the prefix and the interface description.
- DHCPv6 option 16—Option 16 is the vendor ID option for DHCPv6 and is used to insert information about the vendor of the client hardware into DHCPv6 packets.

Copyright © 2017, Juniper Networks, Inc.

- 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 DHCP snooping database. If the packet cannot be validated, it is discarded. You enable IP source guard on a VLAN or bridge domain.
- IPv6 source guard—IP source guard for IPv6.
- 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—Tracks MAC movement and detects MAC spoofing on access ports. You enable this feature on a VLAN or bridge domain.
- 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.
- 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 Monitoring DHCP Messages Received from Untrusted Devices on page 28
- *Understanding DHCP Snooping for Port Security*
- *Understanding IPv6 Neighbor Discovery Inspection*
- Understanding Dynamic ARP Inspection for Protecting Switching Devices Against ARP Spoofing on page 24
- *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 Protecting Switching Devices Against Attacks on page 39

Copyright © 2017, Juniper Networks, Inc.

Configuring Port Security to Protect Access Ports on the Device Against Loss of Information and Productivity (CLI Procedure)

Copyright © 2017, Juniper Networks, Inc.

Ethernet LANs are vulnerable to attacks such as address spoofing and Layer 2 denial of service (DoS) on network devices. The Dynamic Host Configuration Protocol (DHCP) port security features help protect the access ports on the device against the loss of information and productivity that can result from such attacks.

The following port security features are supported for DHCPv4 and MX Series routers:

- DHCP snooping
- DAI (dynamic ARP inspection)
- IP source guard
- DHCP option 82

DHCP snooping is disabled in the default configuration. There is no explicit configuration for enabling DHCP snooping. However, if you configure any other port security features for a bridge domain at the **[edit vlans *vlan-name* forwarding-options dhcp-security]**or the **[edit bridge-domain *bridge-domain-name* forwarding-options dhcp-security]** hierarchy level, then DHCP snooping is automatically enabled on that bridge domain.

DAI, neighbor discovery inspection, IP source guard, and DHCP option 82 are configured per bridge domain. You must configure a bridge domain prior to configuring these DHCP port security features. See *Configuring a Bridge Domain*.

The DHCP port security features that you specify for the bridge domain apply to all included interfaces. However, you can create a specific group of access interfaces within the bridge domain to have different attributes, such as:

- Specifying a specific interface to have a static IP-MAC address (static-ip)
- Specifying an access interface to act as a trusted interface to a DHCP server (trusted)
- Specifying a specific interface not to transmit DHCP (no-option82)

NOTE:

- If you configure any of these DHCP port security features—including configuring a group of access interfaces—for a specific bridge domain, the software automatically enables DHCP snooping for that bridge domain.
- If you explicitly disable DHCP snooping by setting no-dhcp-snooping for a specific bridge domain, the software automatically disables any other DHCP port security features for that bridge domain.

NOTE: Trunk interfaces are trusted by default. However, on an MX Series router, you can override this default behavior and set a trunk interface as untrusted.

Copyright © 2017, Juniper Networks, Inc.

For additional details, see:

- Configuring Dynamic ARP Inspection to Protect Switching Devices Against ARP Spoofing (CLI Procedure) on page 27
- Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing (CLI Procedure) on page 23
- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43

You can override the general port security settings for the bridge domain by configuring a group of access interfaces within it. For details, see:

- Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) on page 23
- Configuring a DHCP Server on a Trusted Interface to Protect it Against Rogue DHCP Servers Sending Leases (CLI Procedure) on page 28

Related Documentation

- Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity on page 18
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28

Copyright © 2017, Juniper Networks, Inc.

Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing (CLI Procedure)

You can use the IP source guard access port security feature on MX Series routers to mitigate the effects of source IP address spoofing and source MAC address spoofing. If IP source guard determines that a host connected to an access interface has sent a packet with an invalid source IP address or source MAC address in the packet header, then IP source guard ensures that the switching device does not forward the packet—that is, the packet is discarded.

To configure IP source guard on a specific bridge domain by using the CLI:

- Configure the IP source guard on a bridge domain:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security]
user@device# set ip-source-guard (MX Series)
```

To configure IP source guard at the routing instance level by using the CLI:

- Configure the IP source guard at the routing instance level:

```
[edit routing-instances ri-name bridge-domains bridge-domain-name
forwarding-options dhcp-security]
user@device# set ip-source-guard (MX Series)
```

Related Documentation

- ip-source-guard (MX Series) on page 80

Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (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, you must first create a group of access interfaces under **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]**. Creating this group automatically enables DHCP snooping, which is a prerequisite for creating the DHCP snooping database. The following procedure shows the configuration in two steps, but it can be done in one. You can then configure a specific interface within the group to have a static IP address that is bound to a fixed MAC address. If you want to have multiple static IP addresses, configure additional interfaces within the same group.

To configure a static IP address and MAC address binding in the DHCP snooping database:

1. Create a group by including an access interface:

   [edit bridge-domains *bd-name* forwarding-options dhcp-security]

Copyright © 2017, Juniper Networks, Inc.

```
user@device# set group group-name interface interface-name
```

2. Configure a static IP address:

```
[edit bridge-domains bd-name forwarding-options dhcp-security]
user@device# set group group-name interface interface-name static-ip ip-address
  mac mac-address
```

Related Documentation

- show dhcp-security binding on page 125
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28

Understanding Dynamic ARP Inspection for Protecting Switching Devices Against ARP Spoofing

Dynamic ARP inspection (DAI) protects switching devices 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 switching device from CPU overload.

- Address Resolution Protocol on page 24
- ARP Spoofing on page 25
- Dynamic ARP Inspection on page 25
- Prioritizing Inspected Packets on page 26

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 switching device 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.

Copyright © 2017, Juniper Networks, Inc.

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 switching device sending traffic to the proper network device, it 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 switching device 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.

Copyright © 2017, Juniper Networks, Inc.

NOTE:

- If your switching device is an EX Series switch and uses Junos OS 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.

For packets directed to the switching device 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 Packet Forwarding Engine. 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

- Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity on page 18
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28
- *Example: Configuring Basic Port Security Features*
- *Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch*
- *Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks*
- *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)*
- *Enabling Dynamic ARP Inspection (CLI Procedure)*
- *Enabling Dynamic ARP Inspection (J-Web Procedure)*

Copyright © 2017, Juniper Networks, Inc.

Configuring Dynamic ARP Inspection to Protect Switching Devices Against ARP Spoofing (CLI Procedure)

Dynamic ARP inspection (DAI) protects switching devices against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping database on the switching devices to validate ARP packets and to protect against ARP cache poisoning.

Before you can enable DAI on a bridge domain, you must configure a bridge domain. See *Configuring a Bridge Domain*.

- To enable DAI on a VLAN by using the CLI:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security]
user@device# set arp-inspection
```

Related Documentation

- Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 45
- Understanding Dynamic ARP Inspection for Protecting Switching Devices Against ARP Spoofing on page 24

Understanding Trusted DHCP Servers for Port Security

Any interface on the switching device 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 Monitoring DHCP Messages Received from Untrusted Devices on page 28
- *Example: Configuring Basic Port Security Features*
- *Enabling a Trusted DHCP Server (CLI Procedure)*
- *Enabling a Trusted DHCP Server (J-Web Procedure)*

Copyright © 2017, Juniper Networks, Inc.

Configuring a DHCP Server on a Trusted Interface to Protect it Against Rogue DHCP Servers Sending Leases (CLI Procedure)

You can configure any interface on a switching device 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.

By default, all access interfaces are untrusted, and all trunk interfaces are trusted. However, you can override the default setting for access interfaces by configuring a group of access interfaces within a bridge domain, specifying an interface to belong to that group, and then configuring the group as trusted.

Before you can configure a trusted DHCP server, you must configure a bridge domain.

To configure an untrusted access interface as a trusted interface for a DHCP server by using the CLI :

1. Configure a group within a bridge domain with a specific access interface:

   ```
   [edit bridge-domains bridge-domain-name forwarding-options dhcp-security]
   user@device# set group group-name interface interface-name
   ```

2. Configure that group as **trusted** to make the specified interface contained within the group a trusted interface:

   ```
   [edit bridge-domains bridge-domain-name forwarding-options dhcp-security group
   group-name]
   user@device# set overrides trusted
   ```

Related Documentation

- Understanding Trusted DHCP Servers for Port Security on page 27

Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices

DHCP snooping enables the switching device, which can be either a switch or a router, to monitor DHCP messages received from untrusted devices connected to the switching device. When DHCP snooping is enabled on a VLAN, the system examines DHCP messages sent from untrusted hosts associated with the VLAN and extracts their IP addresses and lease information. This information is used to build and maintain the DHCP snooping database. Only hosts that can be verified using this database are allowed access to the network.

- DHCP Snooping Basics on page 29
- DHCP Snooping Process on page 30
- DHCPv6 Snooping on page 31
- Rapid Commit for DHCPv6 on page 31

Copyright © 2017, Juniper Networks, Inc.

- DHCP Server Access on page 32
- Static IP Address Additions to the DHCP Snooping Database on page 35
- Snooping DHCP Packets That Have Invalid IP Addresses on page 35
- Prioritizing Snooped Packets on page 36

DHCP Snooping Basics

The 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 switching device is used to create the DHCP snooping table, also known as the binding table. The table shows the IP-MAC binding, as well as the lease time for the IP address, type of binding, VLAN name, and interface for each host.

NOTE: **DHCP snooping is disabled in the default configuration of the switching device. 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 snooping database are updated in these events:

- When a DHCP client releases an IP address (sends a DHCPRELEASE message). In this event, the associated mapping entry is deleted from the database.
- If you move a network device from one VLAN to another. In this event, typically the device needs to acquire a new IP address. Therefore, its entry in the database, including its VLAN ID, is updated.
- When the lease time (timeout value) assigned by the DHCP server expires. In this event, the associated entry is deleted from the database.

TIP: **By default, the IP-MAC bindings are lost when the switching device 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 switching device to snoop DHCP server responses from particular VLANs only. This prevents spoofing of DHCP server messages.

Copyright © 2017, Juniper Networks, Inc.

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

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 the 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 a DHCPDISCOVER packet to request an IP address.
2. The switching device 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 switching device forwards the packet to the DHCP client.
4. The network device sends a DHCPREQUEST packet to accept the IP address. The switching device 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 switching device updates the DHCP snooping database according to the type of packet received:
   - If the switching device receives a DHCPACK packet, it updates lease information for the IP-MAC bindings in its database.
   - If the switching device receives a DHCPNACK packet, it deletes the placeholder.

NOTE: The DHCP snooping 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 Administration Library*.

Copyright © 2017, Juniper Networks, Inc.

DHCPv6 Snooping

DHCPv6 snooping is the equivalent of DHCP snooping for IPv6. The process for DHCPv6 snooping is similar to that for DHCP snooping, but uses different names for the messages exchanged between the client and server to assign IPv6 addresses. Table 3 on page 31 shows DHCPv6 messages and their DHCP equivalents.

Table 3: DHCPv6 Messages and Equivalent DHCPv4 Messages

Sent by	DHCPv6 Messages	Equivalent DHCP Messages
Client	SOLICIT	DHCPDISCOVER
Server	ADVERTISE	DHCPOFFER
Client	REQUEST, RENEW, REBIND	DHCPREQUEST
Server	REPLY	DHCPACK/DHCPNAK
Client	RELEASE	DHCPRELEASE
Client	INFORMATION-REQUEST	DHCPINFORM
Client	DECLINE	DHCPDECLINE
Client	CONFIRM	none
Server	RECONFIGURE	DHCPFORCERENEW
Client	RELAY-FORW, RELAY-REPLY	none

Rapid Commit for DHCPv6

DHCPv6 provides for a Rapid Commit option (DHCPv6 option 14), which, when supported by the server and set by the client, shortens the exchange from a four-way relay to a two-message handshake. For more information about enabling the Rapid Commit option, see *Enabling DHCPv6 Rapid Commit Support*.

In the rapid commit process:

1. The DHCPv6 client sends out a SOLICIT message that contains a request that rapid assignment of address, prefix, and other configuration parameters be preferred.

2. If the DHCPv6 server supports rapid assignment, it responds with a REPLY message, which contains the assigned IPv6 address and prefix and other configuration parameters.

Copyright © 2017, Juniper Networks, Inc.

DHCP Server Access

You can configure a switching device's access to the DHCP server in three ways:

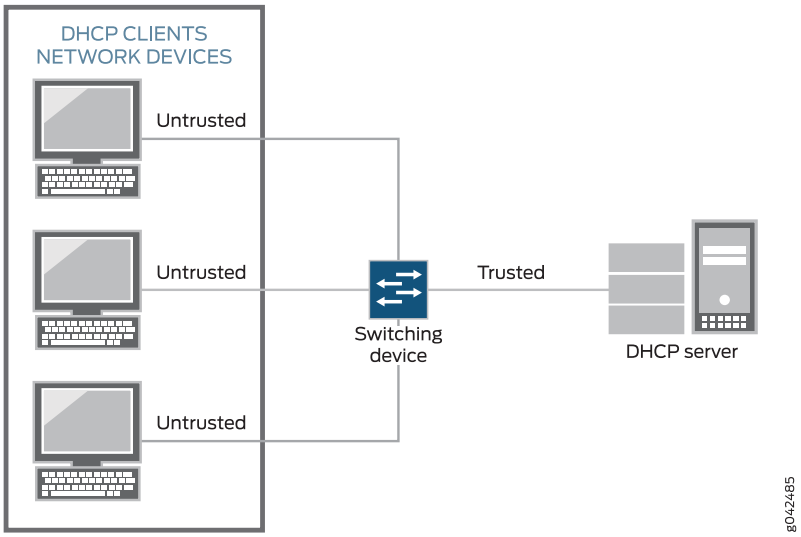
- Switching Device, DHCP Clients, and DHCP Server Are All on the Same VLAN on page 32
- Switching Device Acts as DHCP Server on page 33
- Switching Device Acts as Relay Agent on page 34

Switching Device, DHCP Clients, and DHCP Server Are All on the Same VLAN

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

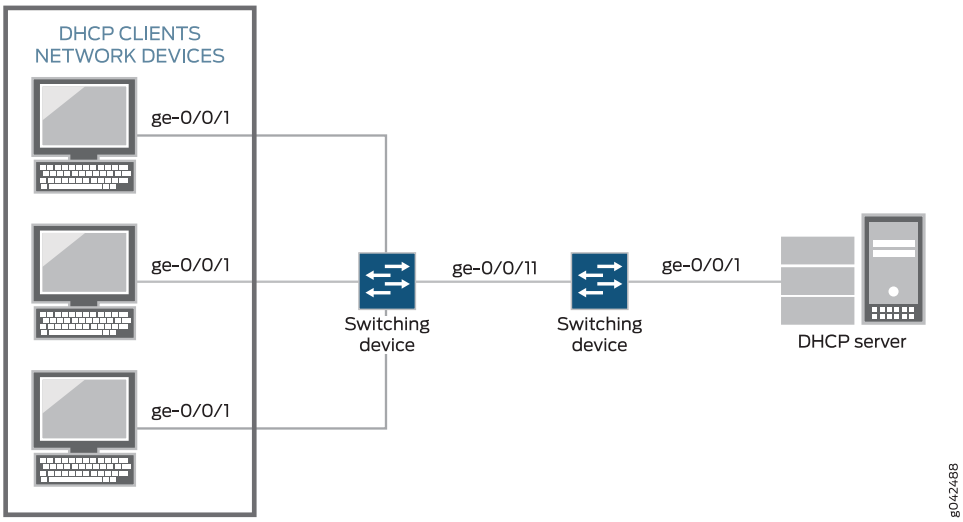
- The server is directly connected to the same switching device as the one connected to the DHCP clients (the hosts, or network devices, that are requesting IP addresses from the server). The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. See Figure 1 on page 32.
- The server is connected to an intermediary switching device (Switching Device 2). The DHCP clients are connected to Switching Device 1, which is connected through a trunk port to Switching Device 2. Switching Device 2 is being used as a transit device. The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. As shown in Figure 2 on page 33, ge-0/0/11 is a trusted trunk port.

Figure 1: DHCP Server Connected Directly to a Switching Device



Copyright © 2017, Juniper Networks, Inc.

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



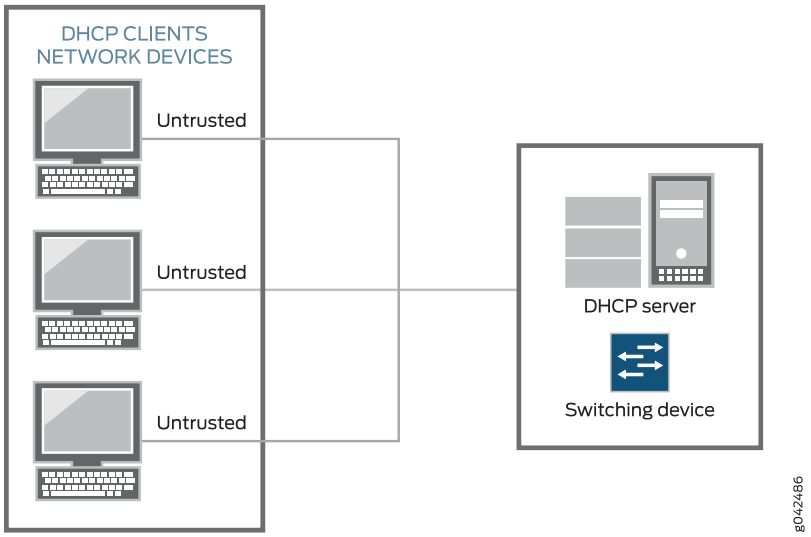
Switching Device Acts as DHCP Server

NOTE: The switching device acting as a DHCP server is not supported on the QFX Series.

The switching device itself is configured as a DHCP server; this is known as a *local configuration*. See Figure 3 on page 34.

Copyright © 2017, Juniper Networks, Inc.

Figure 3: Switching Device Is the DHCP Server



Switching Device Acts as Relay Agent

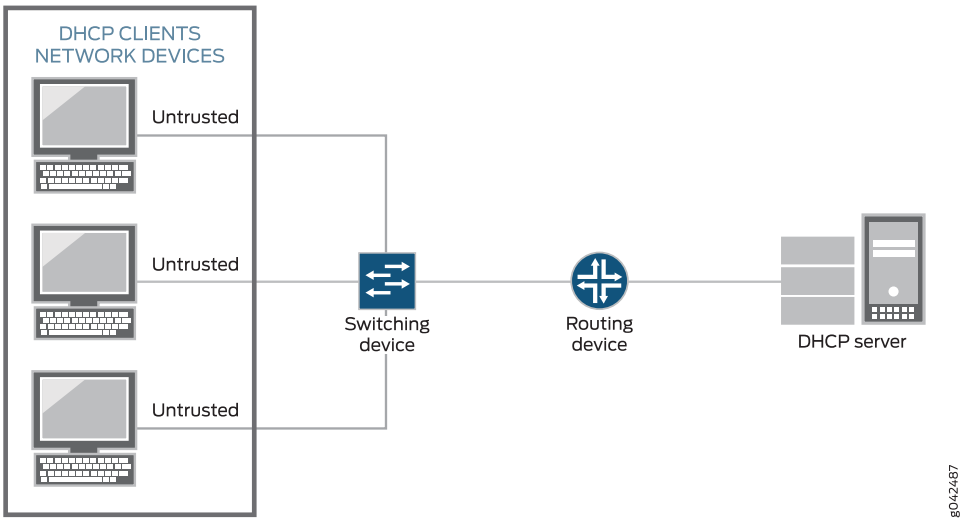
The switching device functions as a relay agent when the DHCP clients or the DHCP server is connected to the device through a Layer 3 interface. The Layer 3 interfaces on the switching device are configured as routed VLAN interfaces (RVIs), which are also known as integrated routing and bridging (IRB)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

These two scenarios illustrate the switching device acting as a relay agent:

- The DHCP server and clients are in different VLANs.
- The switching device is connected to a router that is in turn connected to the DHCP server. See Figure 4 on page 35.

Copyright © 2017, Juniper Networks, Inc.

Figure 4: Switching Device Acting as Relay Agent Through Router to DHCP Server



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 are 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 switching device 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

Copyright © 2017, Juniper Networks, Inc.

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 a specified egress queue, so that the security procedure does not interfere with the transmission of high-priority traffic.

Related Documentation

- Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity on page 18
- Understanding Trusted DHCP Servers for Port Security on page 27
- Configuring a DHCP Server on a Trusted Interface to Protect it Against Rogue DHCP Servers Sending Leases (CLI Procedure) on page 28
- Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) on page 23

Configuring Persistent Bindings in the DHCP or DHCPv6 Snooping Database to Improve Network Performance (CLI Procedure)

NOTE: This task uses Junos OS for MX Series routers and EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

By default, IP-MAC address bindings in the DHCP snooping database do not persist through device reboots. You can improve network performance by configuring the IP-MAC address bindings in the DHCP snooping database to persist through reboots so that the table does not need to be rebuilt after rebooting. Do this by configuring a storage location for the DHCP snooping database file, where you must specify how frequently the device writes the database entries into the DHCP snooping database file.

NOTE: You can also configure persistent bindings for IPv6 addresses and MAC addresses on devices that support DHCPv6 snooping.

DHCPv6 is not supported on the MX Series routers.

The DHCP snooping database of IP-MAC bindings is created when you enable any of the port security features for a specific VLAN or bridge domain in either of the following hierarchy levels:

- **[edit vlans *vlan-name* forwarding-options dhcp-security]**

Copyright © 2017, Juniper Networks, Inc.

- **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]**

On devices that support DHCPv6, enabling any port security features will automatically enable DHCPv6 snooping. DHCP snooping and DHCPv6 snooping are not enabled by default.

Copyright © 2017, Juniper Networks, Inc.

To configure a *local* storage location for the DHCP snooping database file:

- For DHCP snooping:

  ```
  [edit system processes]
  user@device# set dhcp-service dhcp-snooping-file local-pathname write-interval seconds
  ```

  For example:

  ```
  [edit system processes]
  user@device# set dhcp-service dhcp-snooping-file /var/tmp/test.log write-interval 60
  ```

- For DHCPv6 snooping:

  ```
  [edit system processes]
  user@device# set dhcp-service dhcpv6-snooping-file local-pathname write-interval seconds
  ```

  For example:

  ```
  [edit system processes]
  user@device# set dhcp-service dhcpv6-snooping-file /var/tmp/test.log write-interval 60
  ```

To configure a *remote* storage location for IP-MAC bindings, use **tftp://*ip-address*** or **ftp://*hostname/path*** as the remote URL, or the local pathname for the storage location of the DHCP or DHCPv6 snooping database file:

- For DHCP snooping:

  ```
  [edit system processes]
  user@device# set dhcp-service dhcp-snooping-file remote_url write-interval seconds
  ```

  For example:

  ```
  [edit system processes]
  user@device# set dhcp-service dhcp-snooping-file tftp://@14.1.2.1 write-interval 60
  ```

- For DHCPv6 snooping:

  ```
  [edit system processes]
  user@device# set dhcp-service dhcpv6-snooping-file remote_url write-interval seconds
  ```

  For example:

  ```
  [edit system processes]
  user@device# set dhcp-service dhcpv6-snooping-file tftp://@14.1.2.1 write-interval 60
  ```

Related Documentation

- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28

Copyright © 2017, Juniper Networks, Inc.

Understanding DHCP Option 82 for Protecting Switching Devices Against Attacks

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect Juniper Networks EX Series Ethernet Switches and MX Series 3D Universal Edge Routers against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Hosts on untrusted access interfaces on an Ethernet LAN switching device send requests for IP addresses to access the Internet. The switching device 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 penetrate the network by address spoofing.

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 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 Overview on page 39
- Suboption Components of Option 82 on page 40
- Switching Device Configurations That Support Option 82 on page 41
- DHCPv6 Options on page 42

DHCP Option 82 Overview

If DHCP option 82 is enabled on a VLAN or bridge domain, then when a network device—a DHCP client—that is connected to the VLAN or bridge domain on an untrusted interface sends a DHCP request, the switching device inserts information about the client's network location into the packet header of that request. The switching device 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 40 for more information about option 82.

NOTE: On EX4300 switches, DHCP option 82 information is added to DHCP packets received on trusted interfaces as well as untrusted interfaces.

If option 82 is enabled on a VLAN or bridge domain, the following sequence of events occurs when a DHCP client sends a DHCP request:

1. The switching device receives the request and inserts the option 82 information in the packet header.
2. The switching device 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 to the switching device. It does not alter the option 82 information.

Copyright © 2017, Juniper Networks, Inc.

4. The switching device strips the option 82 information from the response packet.

5. The switching device forwards the response packet to the client.

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

NOTE: If your switching device is an EX Series switch and uses Junos OS with Enhanced Layer 2 Software (ELS) configuration style, you can enable DHCP option 82 only for a specific VLAN. See *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*.

If your switching device is an EX Series switch and does *not* use Junos OS with Enhanced Layer 2 Software (ELS) configuration style, you can enable DHCP option 82 either for a specific VLAN or for all VLANs. See *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*.

Suboption Components of Option 82

Option 82 as implemented on a switching device comprises the suboptions circuit ID, remote ID, and vendor ID. These suboptions are fields in the packet header:

- circuit ID—Identifies the circuit (interface or VLAN) on the switching device on which the request was received. The circuit ID contains the interface name and VLAN name, with the two elements separated by a colon—for example, ge-0/0/10:vlan1, where ge-0/0/10 is the interface name and vlan1 is the VLAN name. If the request packet is received on a Layer 3 interface, the circuit ID is just the interface name—for example, ge-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 switching device is used as the prefix; for example, device1:ge-0/0/10:vlan1, where device1 is the hostname.

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

- remote ID—Identifies the remote host. See *remote-id* for details.

- 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.

Copyright © 2017, Juniper Networks, Inc.

Switching Device Configurations That Support Option 82

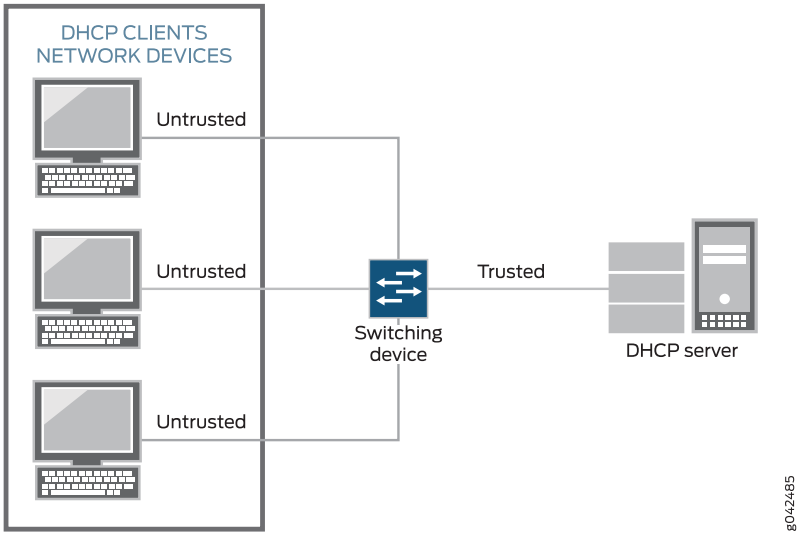
Switching device configurations that support option 82 are:

- Switching Device, DHCP Clients, and the DHCP Server Are on the Same VLAN or Bridge Domain on page 41
- Switching Device Acts as a Relay Agent on page 41

Switching Device, DHCP Clients, and the DHCP Server Are on the Same VLAN or Bridge Domain

If the switching device, the DHCP clients, and the DHCP server are all on the same VLAN or bridge domain, the switching device forwards the requests from the clients on untrusted access interfaces to the server on a trusted interface. See Figure 5 on page 41.

Figure 5: DHCP Clients, Switching Device, and the DHCP Server Are All on the Same VLAN or Bridge Domain

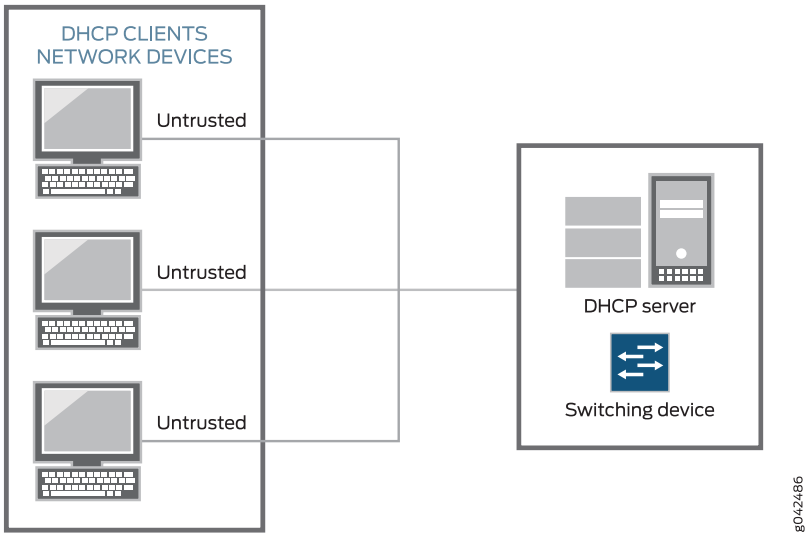


Switching Device Acts as a Relay Agent

The switching device functions as a relay agent (extended relay server) when the DHCP clients or the DHCP server is connected to the switching device through a Layer 3 interface. On the switching device, these interfaces are configured as routed VLAN interfaces (RVIs). Figure 6 on page 42 illustrates a scenario for the switching device acting as an extended relay server; in this instance, the switching device relays requests to the server. This figure shows the relay agent and server on the same network, but they can also be on different networks—that is, the relay agent can be external.

Copyright © 2017, Juniper Networks, Inc.

Figure 6: Switching Device Acting as an Extended Relay Server



DHCPv6 Options

NOTE: MX Series routers do not support DHCPv6.

DHCPv6 provides several options that can be used to insert information into the DHCPv6 request packets that are relayed to a server from a client. These options are equivalent to the sub-options of DHCP option 82.

- Option 37—Identifies the remote host. Option 37 is equivalent to the **remote-id** sub-option of DHCP option 82.
- Option 18—Identifies the interface on which the DHCP request packet was received from the client. Option 18 is equivalent to the **circuit-id** sub-option of DHCP option 82.
- Option 16—Identifies the vendor of the hardware on which the client is hosted. Option 16 is equivalent to the **vendor-id** sub-option of DHCP option 82.

DHCPv6 options are not enabled automatically when DHCPv6 snooping is enabled on a VLAN. They must be configured using the **dhcpv6-options** statement.

Related Documentation

- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*

Copyright © 2017, Juniper Networks, Inc.

Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure)

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switching device 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 switching device, DHCP clients, and DHCP server are all on the same bridge domain. The switching device forwards the clients' requests to the server and forwards the server's responses to the clients. This topic describes this configuration.
- The switching device functions as a relay agent when the DHCP clients or the DHCP server are connected to the switching device through a Layer 3 interface. On the switching device, these interfaces are configured as integrated routing and bridging (IRB) interfaces. The switching device relays the clients' requests to the server and then forwards the server's responses to the clients.

Before you configure DHCP option 82 on the switching device, 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 bridge domain on the switching device and associate the interfaces on which the clients and the server connect, to the switch with that bridge domain.

To configure DHCP option 82:

1. Specify DHCP option 82 for the bridge domain that you configured:

   [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]
   `user@device#` **set** option-82

   NOTE: If you want to enable DHCP option 82 on all bridge domains, you must configure it separately for each specific bridge domain.

   The remaining steps are optional.

2. Configure the prefix for the circuit ID suboption to include the hostname or the routing instance name for the bridge domain:

Copyright © 2017, Juniper Networks, Inc.

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set circuit-id prefix (host-name | routing-instance-name)
```

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

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set circuit-id use-interface-description
```

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

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set circuit-id use-vlan-id
```

5. Specify that the remote ID suboption is included in the DHCP option 82 information:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set remote-id
```

NOTE: If you do not specify a keyword after **remote-id**, the default value for the **remote-id** suboption is the interface name.

6. Specify that the remote ID suboption is the hostname of the switch:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set remote-id host-name
```

7. Specify that the remote ID suboption value contains the interface description:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set remote-id use-interface-description
```

8. Specify that the remote ID suboption value contains a character string:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set remote-id use-string mystring
```

9. Configure a vendor ID suboption:

   - To use the default value (the default value is **Juniper**), do not type a character string after the **vendor-id** option keyword:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set vendor-id
```


Copyright © 2017, Juniper Networks, Inc.

- To configure it so that the vendor ID suboption value contains a character string value that you specify rather than **Juniper** (the default):

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set vendor-id use-string mystring
```

Related Documentation

- Understanding DHCP Option 82 for Protecting Switching Devices Against Attacks on page 39
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28

Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks

This example describes how to enable IP source guard and ynamic ARP inspection (DAI) on a specified bridge domain to protect the device against spoofed IP/MAC addresses and ARP spoofing attacks. When you enable either IP source guard or DAI, the configuration automatically enables DHCP snooping for the same bridge domain.

- Requirements on page 45
- Overview and Topology on page 45
- Configuration on page 47
- Verification on page 48

Requirements

This example uses the following hardware and software components:

- One MX Series router
- Junos OS Release 14.1
- A DHCP server to provide IP addresses to network devices on the device

Before you configure IP source guard to prevent IP/MAC spoofing or DAI to mitigate ARP spoofing attacks, be sure you have:

- Connected the DHCP server to the device.
- Configured the bridge domain to which you are adding DHCP security features. See *Configuring the Bridge Domain for MX Series Router Cloud CPE Services*.

Overview and Topology

Ethernet LAN devices are vulnerable to attacks on security that involve spoofing (forging) of source MAC addresses or source IP addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the device. IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the device against entries stored in the DHCP snooping

Copyright © 2017, Juniper Networks, Inc.

database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the device does not forward the packet—that is, the packet is discarded.

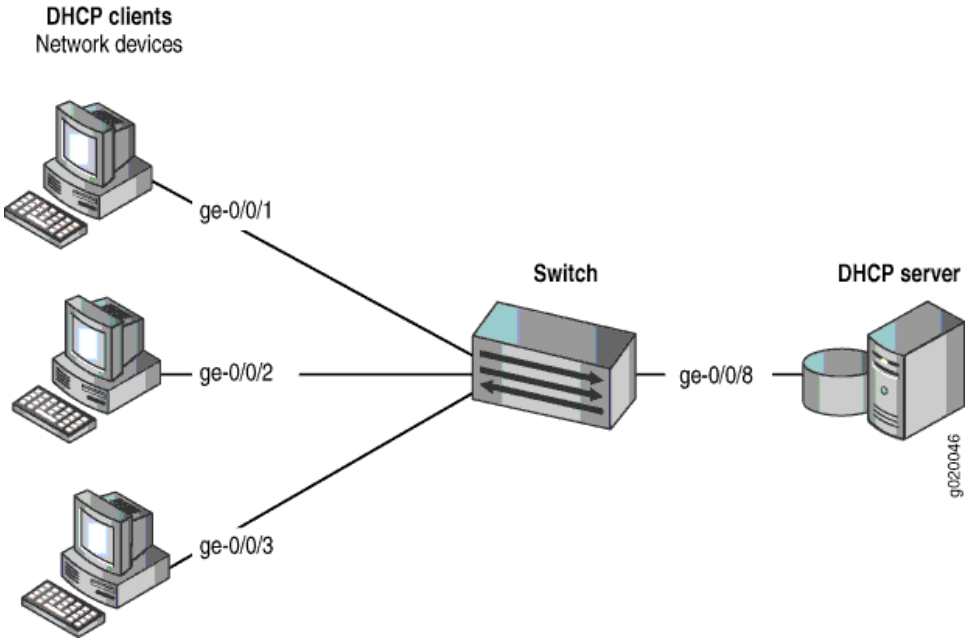
Another type of security attack is ARP spoofing (also known as ARP poisoning or ARP cache poisoning). ARP spoofing is a way to initiate man-in-the-middle attacks. The attacker sends an ARP packet that spoofs the MAC address of another device on the bridge domain. Instead of the device sending traffic to the proper network device, it sends it 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 device that should have gone to another device. The result is that traffic from the device is misdirected and cannot reach its proper destination.

NOTE: When DAI is enabled, the device 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.

This example shows how to configure these important port security features on a device that is connected to a DHCP server. The setup for this example includes the bridge domain **employee-bdomain** on the switching device. Figure 7 on page 46 illustrates the topology for this example.

NOTE: The trunk interface connecting to the DHCP server interface is a trusted port by default.

Figure 7: Switching Device Network Topology for Basic Port Security



Copyright © 2017, Juniper Networks, Inc.

The components of the topology for this example are shown in Table 4 on page 47.

Table 4: Components of the Port Security Topology

Properties	Settings
Device hardware	One MX Series router
Bridge domain name and ID	**employee-bdomain**, tag **20**
Bridge domain 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-bdomain**	**ge-0/0/1**, **ge-0/0/2**, **ge-0/0/3**, **ge-0/0/8**
Interface connecting to DHCP server	**ge-0/0/8**

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

- All access ports are untrusted, which is the default setting.
- The trunk port (ge-0/0/8) is trusted, which is the default setting.
- The bridge-domain (**employee-bdomain**) has been configured to include the specified interfaces.

Configuration

CLI Quick Configuration

To quickly configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping to protect the device against IP spoofing and ARP attacks), copy the following commands and paste them into the device terminal window:

```
[edit]
set bridge-domains employee-bdomain forwarding-options dhcp-security ip-source-guard
set bridge-domains employee-bdomain forwarding-options dhcp-security arp-inspection
```

Step-by-Step Procedure

To configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping) on the bridge domain:

1. Configure IP source guard on the bridge domain:

```
[edit bridge-domains employee-bdomain forwarding-options dhcp-security]
user@device# set ip-source-guard
```

2. Enable DAI on the bridge domain:

```
[edit bridge-domains employee-bdomain forwarding-options dhcp-security]
user@device# set arp-inspection
```

Results

Check the results of the configuration:

Copyright © 2017, Juniper Networks, Inc.

```
user@device> show bridge-domains employee-bdomain forwarding-options
employee-bdomain {
  forwarding-options {
    dhcp-security {
      arp-inspection;
      ip-source-guard;
    }
  }
}
```

Verification

Confirm that the configuration is working properly.

- Verifying That DHCP Snooping Is Working Correctly on the Device on page 48
- Verifying That IP Source Guard Is Working on the Bridge Domain on page 48
- Verifying That DAI Is Working Correctly on the Device on page 49

Verifying That DHCP Snooping Is Working Correctly on the Device

Purpose Verify that DHCP snooping is working on the device.

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

Display the DHCP snooping information when the port on which the DHCP server connects to the device 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@device> show dhcp-security binding

IP Address    MAC Address      Vlan      Expires   State      Interface
192.0.2.17    00:05:85:3A:82:77    employee-vlan   86265  BOUND     ge-0/0/1.0
192.0.2.18    00:05:85:3A:82:79    employee-vlan   86265  BOUND     ge-0/0/1.0
192.0.2.19    00:05:85:3A:82:80    employee-vlan   86287  BOUND     ge-0/0/2.0
192.0.2.20    00:05:85:3A:82:81    employee-vlan   86287  BOUND     ge-0/0/2.0
192.0.2.21    00:05:85:3A:82:83    employee-vlan   86287  BOUND     ge-0/0/2.0
192.0.2.22    00:05:85:27:32:88    employee-vlan   86254  BOUND     ge-0/0/3.0
```

Meaning When the interface on which the DHCP server connects to the device has been set to trusted, the output (see the preceding sample) shows, for the assigned IP address, the device's MAC address, the VLAN name, and the time, in seconds, remaining before the lease expires.

Verifying That IP Source Guard Is Working on the Bridge Domain

Purpose Verify that IP source guard is enabled and working on the bridge domain.

Copyright © 2017, Juniper Networks, Inc.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the device. View the IP source guard information for the data bridge domain.

```
user@device> show dhcp-security binding ip-source-guard

IP Address    MAC Address      Vlan      Expires   State      Interface
192.0.2.17    00:05:85:3A:82:77    employee-vlan   86265  BOUND     ge-0/0/1.0
192.0.2.18    00:05:85:3A:82:79    employee-vlan   86265  BOUND     ge-0/0/1.0
192.0.2.19    00:05:85:3A:82:80    employee-vlan   86287  BOUND     ge-0/0/2.0
192.0.2.20    00:05:85:3A:82:81    employee-vlan   86287  BOUND     ge-0/0/2.0
192.0.2.21    00:05:85:3A:82:83    employee-vlan   86287  BOUND     ge-0/0/2.0
192.0.2.22    00:05:85:27:32:88    employee-vlan   86254  BOUND     ge-0/0/3.0
```

Meaning The IP source guard database table contains the VLANS and bridge domains enabled for IP source guard.

Verifying That DAI Is Working Correctly on the Device

Purpose Verify that DAI is working on the device.

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

Display the DAI information:

```
user@device> show dhcp-security 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 device 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

- *Configuring IP Source Guard (CLI Procedure)*
- *Enabling Dynamic ARP Inspection (CLI Procedure)*

Copyright © 2017, Juniper Networks, Inc.

Copyright © 2017, Juniper Networks, Inc.

CHAPTER 2

Configuring Layer 2 Device Security

- Understanding Storm Control for Managing Traffic Levels on Switching Devices on page 51
- Configuring or Disabling Storm Control (CLI Procedure) on page 53
- Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 59
- Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers on page 60

Understanding Storm Control for Managing Traffic Levels on Switching Devices

NOTE: This topic uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switching device is an EX Series switch and runs software that does support ELS, see *Getting Started with Enhanced Layer 2 Software*.

A traffic storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect. The LAN is suddenly flooded with packets, creating unnecessary traffic that leads to poor network performance or even a complete loss of network service.

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

Copyright © 2017, Juniper Networks, Inc.

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

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

Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems. Storm control is not enabled by default on Juniper Networks MX Series routers.

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

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

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

You can disable the storm control selectively for broadcast, multicast, or unknown unicast traffic, or any combination of traffic types. When disabling storm control for multicast traffic, you can specify the traffic to be either registered multicast or unregistered multicast. Registered multicast MAC addresses are multicast MAC addresses that are within the range 01-00-5E-00-00-00 through 01-00-5E-7F-FF-FF. This range has been reserved by the Internet Assigned Numbers Association (IANA) for multicast Ethernet addresses. Multicast MAC addresses that are outside this range are called unregistered multicast addresses.

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

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

Copyright © 2017, Juniper Networks, Inc.

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

Release History Table

Release	Description
17.4R1	Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.

Related Documentation

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers on page 60
- Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 59
- Configuring or Disabling Storm Control (CLI Procedure) on page 53

Configuring or Disabling Storm Control (CLI Procedure)

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

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

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

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

Copyright © 2017, Juniper Networks, Inc.

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

In the tasks described in this topic, you use the **[edit interfaces *interface-name* unit 0 family ethernet-switching]** hierarchy level to bind the storm control profile for EX Series switches and the **[edit interfaces *interface-name* unit 0 family bridge]** hierarchy level to bind the storm control profile for MX Series routers. Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.

- Configuring Storm Control on page 55
- Disabling Storm Control on Broadcast Traffic on page 55
- Disabling Storm Control on All Multicast Traffic on page 56
- Disabling Storm Control on Registered Multicast Traffic on page 56
- Disabling Storm Control on Unregistered Multicast Traffic on page 57
- Disabling Storm Control on Unknown Unicast Traffic on page 57
- Disabling Storm Control on Multiple Types of Traffic on page 58

Copyright © 2017, Juniper Networks, Inc.

Configuring Storm Control

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

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

To configure storm control:

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

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

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

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

   For EX Series switches:

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

   For MX Series routers:

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

Disabling Storm Control on Broadcast Traffic

To disable storm control on broadcast traffic:

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

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

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

   For EX Series switches:

   ```
   [edit]
   ```

Copyright © 2017, Juniper Networks, Inc.

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

For MX Series routers:

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

Disabling Storm Control on All Multicast Traffic

To disable storm control on all multicast traffic:

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

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

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

   For EX Series switches:

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

   For MX Series routers:

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

Disabling Storm Control on Registered Multicast Traffic

To disable storm control on only registered multicast traffic:

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

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

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

   For EX Series switches:

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

   For MX Series routers:

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


Copyright © 2017, Juniper Networks, Inc.

Disabling Storm Control on Unregistered Multicast Traffic

To disable storm control on only unregistered multicast traffic:

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

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

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

   For EX Series switches:

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

   For MX Series routers:

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

Disabling Storm Control on Unknown Unicast Traffic

To disable storm control on only unknown unicast traffic:

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

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

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

   For EX Series switches:

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

   For MX Series routers:

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

Copyright © 2017, Juniper Networks, Inc.

Disabling Storm Control on Multiple Types of Traffic

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

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

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

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

   For EX Series switches:

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

   For MX Series routers:

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

Release History Table

Release	Description
17.4R1	Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.

Related Documentation

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers on page 60
- Understanding Storm Control for Managing Traffic Levels on Switching Devices on page 51

Copyright © 2017, Juniper Networks, Inc.

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

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

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

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

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

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

To specify the recovery timeout period for the interface:

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

  For EX Series switches:

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

  For MX Series routers:

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

Copyright © 2017, Juniper Networks, Inc.

Related Documentation

- *Configuring MAC Limiting (CLI Procedure)*
- *Configuring MAC Move Limiting (CLI Procedure)*
- Configuring or Disabling Storm Control (CLI Procedure) on page 53

Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers

Storm control enables you to prevent network outages caused by broadcast storms on the LAN. You can configure storm control on an MX Series router to rate-limit broadcast traffic, multicast traffic, and unknown unicast traffic at a specified level and to have packets dropped when the specified traffic level is exceeded, thereby preventing packets from proliferating and degrading the LAN.

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

This example shows how to configure storm control on an pair of MX Series routers running Junos OS with Enhanced Layer 2 Software (ELS).

- Requirements on page 60
- Overview and Topology on page 60
- Configuration on page 61
- Verification on page 63

Requirements

This example uses the following hardware and software components:

- Two MX Series routers
- Junos OS Release 14.1 or later with ELS
- A traffic generator that can send broadcast and unknown unicast traffic at a rate that exceeds 100 Kbps
- A second host

Overview and Topology

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

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

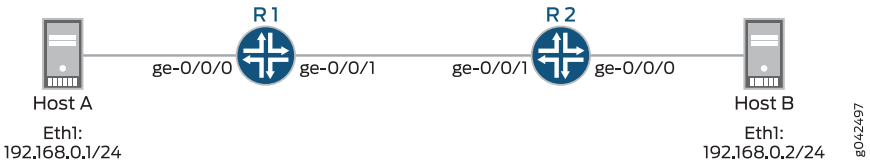
Storm control monitors the level of applicable incoming traffic and compares it with the level that you specify. If the combined level of the applicable traffic exceeds the specified

Copyright © 2017, Juniper Networks, Inc.

level, the router drops packets for the controlled traffic types. As an alternative to having the router drop packets, you can configure storm control to shut down interfaces or temporarily disable interfaces (see the action-shutdown statement or the recovery-timeout statement) when the storm control level is exceeded.

This example shows how to configure the storm control level on interface ge-0/0/1 by setting the level to a traffic rate of 100 Kbps. The topology used consists of two routers that could be connected to various network devices. If the combined traffic exceeds this level, the router drops packets for the controlled traffic types to prevent a network outage. (Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.)

Figure 8: Example Storm Control to Prevent Network Outages



Configuration

This example excludes multicast traffic from the storm traffic. Many protocols use multicast for control traffic, and for that reason network administrators and operators may want to keep multicast working to avoid obstructing protocol operation.

CLI Quick Configuration

To quickly configure storm control based on the traffic rate in Kbps of the combined traffic streams, copy the following commands and paste them into the terminal window. The configurations of routers R1 and R2 are exactly the same:

```
set interfaces ge-0/0/0 unit 0 family bridge interface-mode access
set interfaces ge-0/0/0 unit 0 family bridge vlan-id 15
set interfaces ge-0/0/1 vlan-tagging
set interfaces ge-0/0/1 unit 0 family bridge interface-mode trunk
set interfaces ge-0/0/1 unit 0 family bridge vlan-id-list 15
set interfaces ge-0/0/1 unit 0 family bridge storm-control sc
set interfaces ge-0/0/1 unit 0 family bridge recovery-timeout 120
set bridge-domains bd1 domain-type bridge vlan-id 15
set forwarding-options storm-control-profiles sc all bandwidth-level 100 no multicast
set forwarding-options storm-control-profiles sc action-shutdown
```

Step-by-Step Procedure

To configure storm control:

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

```
[edit]
user@host# set forwarding-options storm-control-profiles sc all bandwidth-level
  100 no-multicast
user@host# set forwarding-options storm-control-profiles sc action-shutdown
```

Copyright © 2017, Juniper Networks, Inc.

2. Bind the storm control profile **sc** to a logical interface. Remember to do this for both interfaces between the routers.

```
[edit]
user@host#set interfaces ge-0/0/1 unit 0 family bridge storm-control sc
```

3. Configure interface ge-0/0/1 (the interface between routers). Do this for both interfaces between the routers.

```
[edit]
user@host# set interfaces ge-0/0/1 vlan-tagging
user@host#set interfaces ge-0/0/1 unit 0 family bridge interface-mode trunk
user@host#set interfaces ge-0/0/1 unit 0 family bridge vlan-id-list 15
user@host#set interfaces ge-0/0/1 unit 0 family bridge recovery-timeout 120
```

4. Configure interface ge-0/0/0 (the interface from host to router). Remember to do this for both interfaces between the routers.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family bridge interface-mode access
user@host# set interfaces ge-0/0/0 unit 0 family bridge vlan-id 15
```

5. Set the bridge domain domain type and VLAN ID.

```
[edit]
user@host# set bridge-domains bd1 domain-type bridge vlan-id 15
```

Results Display the results of the configuration:

```
[edit forwarding-options]
user@router> show storm-control-profiles sc
all {
   bandwidth-level 100;
   no-multicast;
}
action-shutdown;
```

```
[edit]
user@router> show interfaces ge-0/0/0
unit 0 {
   family bridge {
      interface-mode access;
      vlan-id 15;
   }
}
```

```
[edit]
user@router> show interfaces ge-0/0/1
vlan-tagging;
unit 0 {
   family bridge {
      interface-mode trunk;
      vlan-id-list 15;
      storm-control sc;
```


Copyright © 2017, Juniper Networks, Inc.

```
    recovery-timeout 120;
  }
}
```

```
[edit]
user@router> show bridge-domains bd1
domain-type bridge;
vlan-id 15;
```

Verification

Verifying That the Storm Control Configuration Is in Effect

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

Action

1. From Host A to Host B, use a traffic generator to send broadcast and unknown unicast traffic at a rate that exceeds 100 Kbps.

2. Verify on device R1's ge-0/0/0 interface that traffic is entering at a rate that exceeds 100 Kbps.

```
user@R1# run show interfaces detail ge-0/0/0
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 137, SNMP ifIndex: 513, Generation: 140
  Link-level type: Ethernet-Bridge, MTU: 1514, MRU: 1522, Speed: 1000mbps,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Pad to minimum frame size: Disabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x20004000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:05:86:71:6a:00, Hardware address: 00:05:86:71:6a:00
  Last flapped   : 2014-05-20 14:43:25 PDT (1w1d 01:20 ago)
  Statistics last cleared: 2014-05-28 15:59:39 PDT (00:04:02 ago)
  Traffic statistics:
   Input  bytes  :               830088               180432 bps
   Output bytes  :               0                    0 bps
   Input  packets:               8472                 230 pps
   Output packets:               0                    0 pps
   IPv6 transit statistics:
    Input  bytes  :                    0
    Output bytes  :                    0
    Input  packets:                    0
    Output packets:                    0
  Active alarms  : None
  Active defects : None
  Interface transmit statistics: Disabled
```

   The Input bytes field shows the ingress traffic rate in bytes per second (bps). The input rate is within the storm control limit of 100 Kbps.

3. Verify that interface ge-0/0/1 on R1 is down (Admin down).

Copyright © 2017, Juniper Networks, Inc.

```
user@R1# run show interfaces ge-0/0/1.0 terse
Interface               Admin Link   Proto    Local                 Remote
ge-0/0/1.0              down    up   bridge
```

Because the link remains up, control traffic continues to flow.

4. After the timeout period of 120 seconds (2 minutes), verify that the interface comes back up.

```
user@R1# run show interfaces ge-0/0/1.0 terse
Interface               Admin Link Proto    Local                 Remote
ge-0/0/1.0              up    up   bridge
```

Release History Table

Release	Description
17.4R1	(Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.)

Related Documentation

- Configuring or Disabling Storm Control (CLI Procedure) on page 53
- Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 59

Copyright © 2017, Juniper Networks, Inc.

CHAPTER 3

Configuration Statements for Layer 2 Port Security

- arp-inspection (MX Series) on page 66
- bridge-domains on page 67
- circuit-id on page 69
- dhcp-security (MX Series) on page 71
- dhcp-service on page 73
- dhcp-snooping-file on page 74
- forwarding-options on page 75
- group (DHCP Security for MX Series) on page 77
- host-name on page 78
- interface (DHCP Security for MX Series) on page 79
- ip-source-guard (MX Series) on page 80
- mac on page 81
- no-dhcp-snooping on page 82
- no-option82 on page 83
- option-82 on page 84
- overrides (DHCP Security for MX Series) on page 85
- prefix (Circuit ID for Option 82) on page 86
- remote-id (MX Series) on page 88
- routing-instance-name on page 89
- static-ip (MX Series) on page 90
- trusted on page 90
- untrusted on page 91
- use-interface-description on page 92
- use-string on page 94
- use-vlan-id on page 96

Copyright © 2017, Juniper Networks, Inc.

- vendor-id on page 98
- write-interval on page 99

arp-inspection (MX Series)

Syntax arp-inspection;

Hierarchy Level [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]

Release Information Statement introduced in Junos OS Release 14.1 for the MX Series.

Description Perform dynamic ARP inspection (DAI).

DAI can only be configured for a specific bridge domain, not for a list or a range of bridge domain names.

DHCP snooping is automatically enabled on the specified VLAN or bridge domain.

Default Disabled.

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

Related Documentation

- Configuring Dynamic ARP Inspection to Protect Switching Devices Against ARP Spoofing (CLI Procedure) on page 27
- Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 45

Copyright © 2017, Juniper Networks, Inc.

bridge-domains

Syntax

```
bridge-domains {
  bridge-domain-name {
    bridge-options {
      ...bridge-options-configuration...
    }
    domain-type bridge;
    interface interface-name;
    no-irb-layer-2-copy;
    no-local-switching;
    routing-interface routing-interface-name;
    vlan-id (all | none | number);
    vlan-id-list [ vlan-id-numbers ];
    vlan-tags outer number inner number;
    bridge-options {
      interface interface-name {
        mac-pinning
        static-mac mac-address;
      }
      interface-mac-limit limit;
      mac-statistics;
      mac-table-size limit;
      no-mac-learning;
    }
  }
}
```

Hierarchy Level

[edit],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*],
[edit routing-instances *routing-instance-name*]

Release Information

Statement introduced in Junos OS Release 8.4.
Support for logical systems added in Junos OS Release 9.6.
Support for the **no-irb-layer-2-copy** statement added in Junos OS Release 10.2.

Description

(MX Series routers only) Configure a domain that includes a set of logical ports that share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

Options

bridge-domain-name—Name of the bridge domain.

NOTE: You cannot use the slash (/) character as part of the bridge domain name. If you do, the configuration will not commit.

The remaining statements are explained separately. See CLI Explorer.

Copyright © 2017, Juniper Networks, Inc.

Required Privilege Level

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

Related Documentation

- *Configuring a Bridge Domain*
- *Configuring a Layer 2 Virtual Switch*

Copyright © 2017, Juniper Networks, Inc.

circuit-id

Syntax

```
circuit-id {
  prefix {
    host-name;
    logical-system-name;
    routing-instance-name;
  }
  use-interface-description (device | logical);
  use-vlan-id;
}
```

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS):

  [edit vlans *vlan-name* forwarding-options dhcp-security option-82]

- For MX Series platforms:

  [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82]

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.)
Statement introduced in Junos OS Release 14.1 for the MX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

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. See CLI Explorer.

Default

If DHCP 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***.

NOTE: When you configure **circuit-id**, **remote-id** is also enabled, even if you do not explicitly configure **remote-id** .

Required Privilege Level

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

Related Documentation

- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43

Copyright © 2017, Juniper Networks, Inc.

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

Copyright © 2017, Juniper Networks, Inc.

dhcp-security (MX Series)

Syntax

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

Hierarchy Level [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]

Release Information Statement introduced in Junos OS Release 14.1 for the MX Series.

Description Configure port security features on the switching device. DHCP snooping is enabled automatically if you configure any of the following port security features within this hierarchy:

- Dynamic ARP inspection (DAI)
- IP source guard
- DHCP option 82
- Static IP

Copyright © 2017, Juniper Networks, Inc.

The remaining statements are explained separately. See CLI Explorer.

Options *mac-address*—Value (in hexadecimal format) of the address assigned to this device.

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

Related Documentation

- Configuring Dynamic ARP Inspection to Protect Switching Devices Against ARP Spoofing (CLI Procedure) on page 27
- Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing (CLI Procedure) on page 23
- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) on page 23

Copyright © 2017, Juniper Networks, Inc.

dhcp-service

Syntax

```
dhcp-service {
  accept-max-tcp-connections max-tcp-connections;
  dhcp-snooping-file(local_pathname | remote_URL ) {
    write-interval interval;
  }
  interface-traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    level  (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
  ltv-syslog-interval seconds;
  request-max-tcp-connections max-tcp-connections;
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    level  (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
```

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description Enable DHCP services on the device. DHCP services automate network-parameter assignment to network devices. The DHCP service process is enabled by default. However, by default, IP-MAC bindings in the DHCP snooping database do not persist through device reboots. You can inprove performance after rebooting by configuring the IP-MAC bindings to persist, by configuring a storage location for the DHCP database file. When specifying the location for the DHCP database, you must also specify how frequently the switch writes the database entries into the DHCP snooping database file.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation

- Configuring Persistent Bindings in the DHCP or DHCPv6 Snooping Database to Improve Network Performance (CLI Procedure) on page 36

Copyright © 2017, Juniper Networks, Inc.

dhcp-snooping-file

Syntax

```
dhcp-snooping-file (local_pathname | remote_URL);
  write-interval seconds;
}
```

Hierarchy Level [edit system processes dhcp-service]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description Ensure that IP-MAC bindings persist through the device reboots by specifying a local pathname or a remote URL for the storage location of the DHCP snooping database file. You *must* specify how frequently the device writes the database entries into the DHCP snooping database file.

The remaining statement is explained separately. See CLI Explorer.

Default The IP-MAC bindings in the DHCP snooping database file are not persistent by default. If the device is rebooted, the bindings are lost, and the table must be rebuilt on reboot.

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

Related Documentation

- Configuring Persistent Bindings in the DHCP or DHCPv6 Snooping Database to Improve Network Performance (CLI Procedure) on page 36
- Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) on page 23
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28

Copyright © 2017, Juniper Networks, Inc.

forwarding-options

Syntax

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

Hierarchy Level

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

Release Information

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

Copyright © 2017, Juniper Networks, Inc.

Hierarchy level **[edit vlans *vlan-name*]** introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Hierarchy level **[edit** bridge-domains ***bridge-domain-name*]** introduced in Junos OS Release 14.1 for MX Series routers.

Description Configure traffic forwarding.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- *Configuring Traffic Forwarding and Monitoring*

Copyright © 2017, Juniper Networks, Inc.

group (DHCP Security for MX Series)

Syntax

```
group group-name {
  interface interface-name {
    static-ip ip-address {
      mac mac-address;
    }
  }
  overrides {
    no-option82;
    trusted;
    untrusted;
  }
}
```

Hierarchy Level [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX series.
Support for the **static-ipv6** and **no-option37** statements introduced in Junos OS Release 13.2X51-D20 for EX Series switches.
Statement introduced in Junos OS Release 14.1 for the MX Series.

Description

Specify the name of a group of access interfaces that you want to configure for DHCP security attributes that are different from the attributes set for other interfaces in the VLAN or bridge domain. A group must contain at least one interface.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) on page 23
- Configuring a DHCP Server on a Trusted Interface to Protect it Against Rogue DHCP Servers Sending Leases (CLI Procedure) on page 28
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28

Copyright © 2017, Juniper Networks, Inc.

host-name

Syntax host-name *host-name;*

Hierarchy Level (EX Series) [edit vlans *vlan-name* forwarding-options dhcp-security option-82 remote-id]

Hierarchy Level (MX Series) [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security remote-id option-82]

Release Information Statement introduced in Junos OS Release 13.2X50-D10.
Statement introduced in Junos OS Release 14.1 for the MX Series.

Description Use the hostname of the switching device as 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.

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

Related Documentation

- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046

Copyright © 2017, Juniper Networks, Inc.

interface (DHCP Security for MX Series)

Syntax

```
interface interface-name {
  static-ip ip-address {
    mac mac-address;
  }
}
```

Hierarchy Level [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security group *group-name*]

Release Information Statement introduced in Junos OS Relese 14.1 for the MX Series.

Description Configure an interface for a static IPaddress to MAC address binding (IP-MAC binding) or configure an interface to belong to a group within the bridge domain that has DHCP security attributes that are different from the attributes of other interfaces in the bridge domain.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation

- Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) on page 23

Copyright © 2017, Juniper Networks, Inc.

ip-source-guard (MX Series)

Syntax ip-source-guard;

Hierarchy Level [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]

Release Information Hierarchy level **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]** introduced in Junos OS Release 14.1 for the MX Series.

Description Perform IP source guard checking on packets sent from access interfaces. Validate source IP addresses and source MAC addresses on all bridge domains or on the specified bridge domain or bridge domain range. Forward packets with valid addresses and drop those with invalid addresses.

- **ip-source-guard**—Enable IP source guard checking.

If you configure IP source guard at the **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]** hierarchy level:

- IP source guard can be configured only for a specific bridge domain, not for a list or range of bridge domains.
- DHCP snooping is automatically enabled.

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

Related Documentation

- Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing (CLI Procedure) on page 23
- Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 45

Copyright © 2017, Juniper Networks, Inc.

mac

Syntax mac *mac-address*;

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS):

  [edit vlans *vlan-name* forwarding-options dhcp-security group *group-name* interface *interface-name* static-ip *ip-address*]

- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port interface (all | *interface-name*) static-ip *ip-address* vlan *vlan-name*]

- For MX Series platforms:

  [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security group *group-name* interface *interface-name* static-ip *ip-address*]

Release Information Statement introduced in Junos OS Release 9.2 for EX Series switches.
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.)
Hierarchy level **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]** introduced in Junos OS Release 14.1 for the MX Series.

Description Configure the media access control (MAC) address or hardware address of the device connected to the specified interface.

Options *mac-address*—Value (in hexadecimal format) of the address assigned to this device.

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

Related Documentation

- *Configuring Static IP Addresses in the DHCP Snooping Database for Access Ports (CLI Procedure)*
- *Configuring Static IP Addresses in the DHCP Snooping Database for Access Ports (CLI Procedure)*
- Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) on page 23

Copyright © 2017, Juniper Networks, Inc.

no-dhcp-snooping

Syntax no-dhcp-snooping;

Hierarchy Level (EX Series, QFX Series) [edit vlans *vlan-name* forwarding-options dhcp-security]

Hierarchy Level (MX Series) [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX series.
Hierarchy level **[edit bridge-domains *bridge-domain-name* forwarding-options** dhcp-security**]** introduced in Junos OS Release 14.1 for the MX Series.

Description Disable DHCP snooping for the specified VLAN or bridge domain.

NOTE: Explicitly disabling DHCP snooping also disables any other port security features that you have enabled under **[edit vlans *vlan-name* forwarding-options dhcp-security]**, including dynamic ARP inspection (DAI) and IP source guard for the specified VLAN or bridge domain.

There is no configuration statement that explicitly enables DHCP snooping.

Default DHCP snooping is not enabled.

NOTE: Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style and MX Series routers do not have a configuration statement that explicitly enables DHCP snooping.

DHCP snooping is enabled automatically by Junos OS if any of the following is configured at the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level for EX Series and QFX Series switches or at the **[edit bridge-domains *bridge-domain-name* forwarding-options** dhcp-security**]** for MX Series routers:

- DAI
- IP source guard
- Static IP
- DHCP option 82

Copyright © 2017, Juniper Networks, Inc.

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

Related Documentation
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28

no-option82

Syntax
no-option82;

Hierarchy Level (EX Series, QFX Series)
[edit vlans *vlan-name* forwarding-options dhcp-security group *group-name* overrides]

Hierarchy Level (MX Series)
[edit bridge-domains *bridge-domain-name* forwarding-options group group *group-name* overrides]

Release Information
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX series.
Statement introduced in Junos OS Release 14.1 for the MX Series.

Description
Configure a specific group of one or more access interfaces within the VLAN or bridge domain *not* to transmit DHCP option 82 information, even if the VLAN or bridge domain is configured to use option 82.

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

Related Documentation
- option-82 on page 84
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- Understanding DHCP Option 82 for Protecting Switching Devices Against Attacks on page 39
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28

Copyright © 2017, Juniper Networks, Inc.

option-82

Syntax

```
option-82 {
  circuit-id {
    prefix (host-name | routing-instance-name);
    use-interface-description;
    use-vlan-id;
  }
  remote-id {
    host-name;
    mac (Option 82);
    use-interface-description;
    use-string string;
  }
  vendor-id {
    use-string string;
  }
}
```

Hierarchy Level (EX Series, QFX Series)

[edit vlans *vlan-name* forwarding-options dhcp-security]

Hierarchy Level (MX Series)

[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for the MX Series.

Description

Have the device insert DHCP option 82 (also known as the DHCP relay agent information option) information in the DHCP request packet header of a DHCP request that it receives from a DHCP client connected to one of its interfaces before it forwards or relays that DHCP request to a DHCP server. The server uses the option 82 information, which provides details about the circuit and host the request came from. However, in formulating the reply, the server does not make any changes to the option 82 information in the packet header. The device receives the reply and then removes the DHCP option 82 information before forwarding the reply to the client.

The remaining statements are explained separately. See CLI Explorer.

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

- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- no-option82 on page 83

Copyright © 2017, Juniper Networks, Inc.

- Understanding DHCP Option 82 for Protecting Switching Devices Against Attacks on page 39
- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046

overrides (DHCP Security for MX Series)

Syntax overrides (trusted | untrusted | no-option82);

Hierarchy Level [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security group *group-name*]

Release Information Statement introduced in Junos OS Release 14.1 for the MX Series.

Description Modify selected attributes of a specific interface within a group of interfaces configured within a specified bridge domain.

Options

no-option 82 —The interface specified in this group does not support DHCP option 82.

trusted—The interface specified in this group is trusted. DHCP snooping does not apply to the trusted interface. Likewise, DAI and IP source guard—even if they are enabled for the VLAN or bridge domain—do not apply to the interface that is configured with the **overrides** and the **trusted** options. Trunk interfaces are trusted by default. Access interfaces are untrusted by default.

untrusted— The interface specified in this group is untrusted. Trunk interfaces are trusted by default. Access interfaces are untrusted by default.

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

Related Documentation

- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- Understanding DHCP Option 82 for Protecting Switching Devices Against Attacks on page 39

Copyright © 2017, Juniper Networks, Inc.

prefix (Circuit ID for Option 82)

Syntax

```
prefix {
  host-name;
  logical-system-name;
  routing-instance-name;
}
```

Hierarchy Level

- For platforms with enhanced Layer 2 software (ELS):

  [edit vlans 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]

- For MX Series platforms:

  [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82circuit-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 option-82 circuit-id]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 14.1 for the MX Series.

Description

Configure an optional prefix for the circuit ID suboption in the DHCP option 82 information that is inserted by the switch or router into the packet header of a DHCP request before it forwards or relays the request to a DHCP server.

Default

If the **prefix** statement is not explicitly specified, no prefix is prepended to the circuit ID.

Options

host-name—Add router host name to DHCP option 82 circuit ID.

logical-system-name—Add logical system name to DHCP option-82 circuit ID.

This option is not used for the **prefix** statement at any of the above hierarchy levels.

routing-instance-name—Add routing instance name to DHCP option-82 circuit ID.

This option is not used for the **prefix** statement occurring at the following hierarchy levels:

- **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82circuit-id]**

Copyright © 2017, Juniper Networks, Inc.

- Any of the hierarchy levels for the platforms without ELS

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*
- *Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server*
- *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)*
- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

Copyright © 2017, Juniper Networks, Inc.

remote-id (MX Series)

Syntax

```
remote-id {
  host-name;
  use-interface-description (logical | device);
  use-string string;
}
```

Hierarchy Level [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82]

Release Information Statement introduced in Junos OS Release 14.1 for the MX Series.

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. See CLI Explorer.

Default If the **remote-id** statement is not explicitly set, no remote ID value is inserted in the DHCP request packet header.

If the **remote-id** statement is explicitly set, but is not qualified by a keyword, the default value is the device MAC address.

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

Related Documentation

- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046

Copyright © 2017, Juniper Networks, Inc.

routing-instance-name

Syntax routing-instance-name;

Hierarchy Level (EX Series) [edit vlans forwarding-options dhcp-security option-82 circuit-id prefix]

Hierarchy Level (MX Series) [edit bridge-domains *bridge domain name* forwarding-options dhcp-security option-82 circuit-id prefix]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 14.1 for the MX Series.

Description Specify that the routing instance name be included within the optional prefix for the circuit 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.

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

Related Documentation

- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43

Copyright © 2017, Juniper Networks, Inc.

static-ip (MX Series)

Syntax static-ip *ip-address* mac *mac-address*;

Hierarchy Level [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security group *group-name* interface *interface-name*]

Release Information Statement introduced in Juos OS Release 14.1 for the MX Series.

Description Configure a static IP address to MAC address (IP-MAC) binding record to be added to the DHCP snooping database.

Options ***ip-address***—Static IP address assigned to a device connected on the specified interface.

mac-address—Static MAC address assigned to a device connected on the specified interface.

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

Related Documentation

- Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure) on page 23

trusted

Syntax trusted;

Hierarchy Level [edit bridge domains *bridge-domain-name* forwarding-options dhcp-security group *group-name* overrides]

Release Information Statement introduced in Junos OS Release 14.1 for the MX Series.

Description Allow DHCP responses from the specified interface.

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

Related Documentation

- Configuring a DHCP Server on a Trusted Interface to Protect it Against Rogue DHCP Servers Sending Leases (CLI Procedure) on page 28
- Understanding Trusted DHCP Servers for Port Security on page 27

Copyright © 2017, Juniper Networks, Inc.

untrusted

Syntax untrusted;

Hierarchy Level [edit bridge domains *bridge-domain-name* forwarding-options dhcp-security group *group-name* overrides]

Release Information Statement introduced in Junos OS Release 14.1 for the MX Series.

Description Allow DHCP responses from the specified interface.

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

Related Documentation

- Configuring a DHCP Server on a Trusted Interface to Protect it Against Rogue DHCP Servers Sending Leases (CLI Procedure) on page 28
- Understanding Trusted DHCP Servers for Port Security on page 27

Copyright © 2017, Juniper Networks, Inc.

use-interface-description

Syntax use-interface-description (device | logical);

For Platforms with Enhanced Layer 2 Software (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]

For MX Series Platforms [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82circuit-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.)
Hierarchy level **[edit bridge-domains *bridge domain name* forwarding-options dhcp-security]** introduced in Junos OS Release 14.1 for the MX Series.

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.

The textual description is configured using the **description** statement at the **[edit interfaces *interface-name*]** hierarchy level. If you specify that the textual description be used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name. When you use the interface description rather than the interface name, the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.

Options
device—Use the device interface description. Only available for MX Series platform configuration.

logical—Use the logical interface description. Only available for MX Series platform configuration.

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

Copyright © 2017, Juniper Networks, Inc.

Related Documentation

- *Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server*
- *Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server*
- *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)*
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046

Copyright © 2017, Juniper Networks, Inc.

use-string

Syntax use-string *string*;

For Platforms with Enhanced Layer 2 Software (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]

For MX Series Platforms [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82 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.
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.)
Hierarchy level **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]** introduced in Junos OS Release 14.1 for the MX Series.

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

- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- Understanding DHCP Option 82 for Protecting Switching Devices Against Attacks on page 39
- *Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server*
- *Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server*
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*

Copyright © 2017, Juniper Networks, Inc.

- *Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- *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

Copyright © 2017, Juniper Networks, Inc.

use-vlan-id

Syntax use-vlan-id;

For Platforms with Enhanced Layer 2 Software (ELS)
[edit forwarding-options helpers bootp dhcp-option82-circuit-id]
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82-circuit-id]

For MX Series Platforms
[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82 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.
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.)
Hierarchy level **[edit bridge-domains *bridge-domain-name* forwarding-options** dhcp-security**]** introduced in Junos OS Release 14.1 for the MX Series.

NOTE: The EX Series switches that support the **use-vlan-id** statement are the EX4300, EX4600, and EX9200 switches.

Description Use the VLAN ID rather than the VLAN name (the default) in the circuit ID or remote ID value in the DHCP option 82 information.

NOTE: The **use-vlan-id** statement is mutually exclusive with the **use-interface-description** and **no-vlan-interface-name** statements.

The **use-vlan-id** statement only applies to interfaces in a bridge domain. The format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces is as follows:

(fe | ge)-*fpc/pic/port.subunit*:*svlan_id-vlan_id*

NOTE: The *subunit* is required and used to differentiate the interface for remote systems, and *svlan_id-vlan_id* represents the VLANs associated with the bridge domain.

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

Copyright © 2017, Juniper Networks, Inc.

Related Documentation

- *Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server*
- *Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server*
- *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)*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

Copyright © 2017, Juniper Networks, Inc.

vendor-id

Syntax vendor-id <*string*>;

For Platforms with Enhanced Layer 2 Software (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]

For MX Series Platforms [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82]

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.)
Hierarchy level **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]** introduced in Junos OS Release 14.1 for the MX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

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

- Configuring DHCP Option 82 to Help Protect the Switching Devices Against Attacks (CLI Procedure) on page 43
- *Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server*
- *Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server*

Copyright © 2017, Juniper Networks, Inc.

- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*

write-interval

Syntax write-interval *seconds*;

For Platforms with Enhanced Layer 2 Software (ELS) [edit system processes dhcp-service dhcp-snooping-file],
[edit system processes dhcp-service dhcpv6-snooping-file]

For Platforms Without ELS [edit ethernet-switching-options secure-access-port dhcp-snooping-file],
[edit ethernet-switching-options secure-access-port dhcpv6-snooping-file]

For MX Series Platforms [edit system processes dhcp-service dhcp-snooping-file]

Release Information Statement introduced in Junos OS Release 9.4 for EX Series switches.
Support at the **[edit system processes dhcp-service dhcp-snooping-file]** hierarchy level introduced in Junos OS Release 13.2X50-D10.
Support at the **[edit system processes dhcp-service dhcpv6-snooping-file]** hierarchy level introduced in Junos OS Release 13.2X51-D20.
Statement introduced in Junos OS Release 14.1 for the MX Series.
Support at the **[edit ethernet-switching-options secure-access-port dhcpv6-snooping-file]** hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Specify how frequently the device writes the database entries from memory into the DHCP snooping database file.

- If you are configuring **write-interval** at the **[edit system processes dhcp-service dhcp-snooping-file]** or the **[edit system processes dhcp-service dhcpv6-snooping-file]** hierarchy level, see "Configuring Persistent Bindings in the DHCP or DHCPv6 Snooping Database to Improve Network Performance (CLI Procedure)" on page 36.

Options ***seconds***—Value in seconds.

Range: 60 through 86,400 seconds.

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

Related Documentation

- Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices on page 28

Copyright © 2017, Juniper Networks, Inc.

Copyright © 2017, Juniper Networks, Inc.

CHAPTER 4

Configuration Statements for Layer 2 Device Security

- action-shutdown on page 102
- bandwidth-level on page 104
- bandwidth-percentage on page 105
- icmpv4-rate-limit on page 106
- no-broadcast on page 107
- no-multicast on page 109
- no-registered-multicast on page 111
- no-unknown-unicast on page 112
- no-unregistered-multicast on page 114
- recovery-timeout on page 115
- storm-control on page 117
- storm-control-profiles on page 118

Copyright © 2017, Juniper Networks, Inc.

action-shutdown

Syntax action-shutdown;

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS):

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

- For platforms without ELS:

  [edit ethernet-switching-options storm-control]

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

Description Logically shut down or temporarily disable interfaces when the storm control level is exceeded.

To configure the shutdown action so that the interfaces are disabled temporarily, and recover automatically after a specified period of time:

- Configure both the **action-shutdown** and the **port-error-disable** statements. The interfaces recover automatically when the disable timeout expires. (The **port-error-disable** statement is not supported on QFX Series switches or MX Series routers.)
- Configure both the **action-shutdown** and the recovery-timeout statements. The interfaces recover automatically when the recovery timeout expires.

If you configure the **action-shutdown** statement and do not configure the **port-error-disable** or **recovery-timeout** statement, the interfaces that are enabled for storm control are shut down when the storm control level is exceeded and they do not recover automatically from that port-error condition.

If you do not configure the switch for autorecovery from the disabled condition, you can bring up the disabled interfaces by running one of the following commands:

- (MX Series)—Issue the clear bridge recovery-timeout
- (QFX Series)—Issue the **clear ethernet-switching recovery-timeout**
- (EX Series switches that support ELS)—Issue the **clear ethernet-switching recovery-timeout**
- (EX Series switches that do not support ELS)—Issue the **clear ethernet-switching port-error**

Copyright © 2017, Juniper Networks, Inc.

NOTE: On EX4300 switches, **action-shutdown** causes an interface to stop learning MAC addresses and it also drops all incoming packets, but does not disable the physical interface.

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

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

Related Documentation

- recovery-timeout on page 115
- clear bridge recovery-timeout on page 132
- *clear ethernet-switching recovery-timeout*
- Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers on page 60
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 59

Copyright © 2017, Juniper Networks, Inc.

bandwidth-level

Syntax bandwidth-level *kbps*;

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

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description Configure the storm control level as the bandwidth in kilobits per second of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.

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

Default On EX4300 switches—If you do not specify the storm control level using either the **bandwidth-level** or the **bandwidth-percentage** statements, the storm control level defaults to 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.

On EX9200 switches—Storm control is not enabled by default.

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

Options **bandwidth-level *kbps***—Traffic rate in kilobits per second of the combined broadcast, multicast, and unknown unicast traffic streams.

Range: 100 through 10,000,000

Range: 100 through 100,000,000 on QFX10000 Series switches

Default: None

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

Related Documentation

- bandwidth-percentage on page 105
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*

Copyright © 2017, Juniper Networks, Inc.

- Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers on page 60
- Configuring or Disabling Storm Control (CLI Procedure) on page 53

bandwidth-percentage

Syntax bandwidth-percentage *percentage*;

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

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description Configure the storm control level as the percentage of available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams on an interface. The storm control level is configured as part of the storm control profile.

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

Default On EX4300 switches—The storm control level is 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.

On EX9200 switches—Storm control is not enabled by default.

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

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

Related Documentation

- bandwidth-level on page 104
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers on page 60
- Configuring or Disabling Storm Control (CLI Procedure) on page 53

Copyright © 2017, Juniper Networks, Inc.

icmpv4-rate-limit

Syntax

```
icmpv4-rate-limit {
  bucket-size seconds;
  packet-rate pps;
}
```

Hierarchy Level [edit system internet-options]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure rate-limiting parameters for ICMPv4 messages sent.

Options

bucket-size *seconds*—Number of seconds in the rate-limiting bucket.

Range: 0 through 4294967295 seconds

Default: 5

packet-rate *pps*—Rate-limiting packets earned per second.

Range: 0 through 4294967295 pps

Default: 1000

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

Related Documentation

- *Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages*

Copyright © 2017, Juniper Networks, Inc.

no-broadcast

Syntax no-broadcast;

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

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

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

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

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

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

Related Documentation
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*

Copyright © 2017, Juniper Networks, Inc.

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers on page 60
- *Disabling or Enabling Storm Control (CLI Procedure)*
- Configuring or Disabling Storm Control (CLI Procedure) on page 53

Copyright © 2017, Juniper Networks, Inc.

no-multicast

Syntax no-multicast;

Hierarchy Level

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

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

- For platforms without ELS:

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

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

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

Default

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

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

Copyright © 2017, Juniper Networks, Inc.

Related Documentation

- no-registered-multicast on page 111
- no-unregistered-multicast on page 114
- *Disabling or Enabling Storm Control (CLI Procedure)*
- Configuring or Disabling Storm Control (CLI Procedure) on page 53

Copyright © 2017, Juniper Networks, Inc.

no-registered-multicast

Syntax no-registered-multicast;

Hierarchy Level

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

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

- For platforms without ELS:

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

Release Information Statement introduced in Junos OS Release 10.3 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10.
(See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 13.2 for the QFX series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

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

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

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

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

EX9200 switches—Storm control is not enabled by default.

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

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

Related Documentation

- no-multicast on page 109
- no-unregistered-multicast on page 114
- *Understanding Storm Control on EX Series Switches*
- Understanding Storm Control for Managing Traffic Levels on Switching Devices on page 51

Copyright © 2017, Juniper Networks, Inc.

no-unknown-unicast

Syntax no-unknown-unicast;

Hierarchy Level

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

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

- For platforms without ELS:

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

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

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

Default

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

Copyright © 2017, Juniper Networks, Inc.

Required Privilege Level

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

Related Documentation

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers on page 60
- *Disabling or Enabling Storm Control (CLI Procedure)*
- Configuring or Disabling Storm Control (CLI Procedure) on page 53

Copyright © 2017, Juniper Networks, Inc.

no-unregistered-multicast

Syntax no-unregistered-multicast;

Hierarchy Level

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

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

- For platforms without ELS:

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

Release Information Statement introduced in Junos OS Release 10.3 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10.
(See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 13.2 for the QFX series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

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

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

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

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

EX9200 switches—Storm control is not enabled by default.

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

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

Related Documentation

- no-multicast on page 109
- no-registered-multicast on page 111
- *Understanding Storm Control on EX Series Switches*
- Understanding Storm Control for Managing Traffic Levels on Switching Devices on page 51

Copyright © 2017, Juniper Networks, Inc.

recovery-timeout

Syntax recovery-timeout *seconds*;

Hierarchy Level (EX Series and QFX Series) [edit interfaces *interface-name* unit 0 family ethernet-switching]

Hierarchy Level (MX Series) [edit interfaces *interface-name* unit 0 family bridge]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for the MX Series routers.

Description Configure an interface to be temporarily disabled when MAC limiting, MAC move limiting, or rate-limiting is in effect with the action **shutdown**. This enables the affected interface to recover automatically from the error condition after the specified period of time:

- If you configure MAC limiting with the **shutdown** option and you enable **recovery-timeout**, the interface is temporarily disabled when the MAC address limit is reached. The interface will recover automatically after the number of seconds specified.
- If you enable MAC move limiting with the **shutdown** option and you enable **recovery-timeout**, the interface is temporarily disabled when the maximum number of MAC address moves is reached. The interface will recover automatically after the number of seconds specified.
- If you enable MAC move limiting with the **vlan-member-shutdown** option and you enable **recovery-timeout**, the interface is temporarily disabled when the maximum number of MAC address moves is reached. The interface will recover automatically after the number of seconds specified. If the recovery timeout is not configured, the interface will recover automatically after 180 seconds.
- If you enable storm control with the **action-shutdown** option and you enable **recovery-timeout**, the interface is temporarily disabled when applicable traffic exceeds the specified levels. Depending upon the configuration, applicable traffic can include broadcast, unknown unicast, and multicast traffic.

NOTE: The **recovery-timeout** configuration does not apply to preexisting error conditions. It impacts only error conditions that are detected after the **recovery-timeout** statement is configured and committed. To clear a preexisting error condition and restore the interface to service, use the operational mode commands **clear ethernet-switching recovery-timeout** for EX Series and QFX Series and clear bridge recovery-timeout for MX Series routers.

Copyright © 2017, Juniper Networks, Inc.

Default The interface does not automatically recover from an error condition.

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

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

Range: 10 through 3600

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

Related Documentation

- action-shutdown on page 102
- *Configuring MAC Limiting (CLI Procedure)*
- *Configuring MAC Move Limiting (CLI Procedure)*
- Configuring or Disabling Storm Control (CLI Procedure) on page 53

Copyright © 2017, Juniper Networks, Inc.

storm-control

Syntax storm-control *storm-control-profile*;

Hierarchy Level [edit interfaces *interface-name* unit *number* family ethernet-switching],
[edit interfaces *interface-name* unit *number* family bridge]
[edit interfaces *interface-name* ether-options ethernet-switch-profile]
[edit logical-systems *name* interfaces *interface-name* unit *number* family bridge]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX series.
Statement introduced in Junos OS Release 14.1 for the MX Series routers.
Starting in Junos OS release 17.4R1 for MX Series routers, support for storm control was added for logical systems.

Description Bind a storm control profile to a given interface.

On switches running ELS software, storm control is enabled by default on all switch interfaces at a level of 80 percent of the combined broadcast and unknown unicast streams. (For the equivalent statement for platforms running non-ELS software, see *storm-control*.)

NOTE: If you configure storm control on an aggregated Ethernet interface, the storm-control level is applies to each member interface individually. For example, if the aggregated interface has two members and you configure a storm-control level of 20 kbps, Junos will not detect a storm if one or both of the member interfaces receives traffic at 15 kbps because in neither of these cases does an individual member receive traffic at a rate greater than the configured storm-control level. In this example, Junos detects a storm only if at least one member interface receives traffic at greater than 20 Kbps.

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

Related Documentation

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- Understanding Storm Control for Managing Traffic Levels on Switching Devices on page 51

Copyright © 2017, Juniper Networks, Inc.

storm-control-profiles

Syntax

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

Hierarchy Level

[edit forwarding-options]
[edit logical-systems *name* forwarding-options]

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.
Starting in Junos OS release 17.4R1 for MX Series routers, support for storm control was added for logical systems.

Description

Configure a storm control profile on a switch or router. Storm control is used to prevent network outages that are caused by broadcast traffic storms. Storm control enables the switching device to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the storm control level or storm control bandwidth—is exceeded, thus preventing packets from proliferating and degrading the LAN.

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

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- Understanding Storm Control for Managing Traffic Levels on Switching Devices on page 51

Copyright © 2017, Juniper Networks, Inc.

CHAPTER 5

Operational Commands for Layer 2 Port Security

- clear arp
- clear dhcp-security binding
- show dhcp-security arp inspection statistics
- show dhcp-security binding
- show dhcp-security binding ip-source-guard

Copyright © 2017, Juniper Networks, Inc.

clear arp

Syntax

clear arp
<all>
<hostname *hostname*>
<interface *interface-name*>
<logical-system *logical-system-name*>
<vpn *vpn*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 14.1 for the MX Series.
all option introduced in Junos OS Release 14.2.

Description

Remove entries from the Address Resolution Protocol (ARP) table for the current CLI view. To clear entries for a specific logical system, you must first enter the **set cli logical-system *logical-system-name*** command, and then issue the **clear arp** command.

Options

all— Clear all entries from the ARP table.

hostname *hostname*—(Optional) Clear only the specified host entry from the ARP table.

interface *interface-name*—(Optional) Clear entries only for the specified interface from the ARP table.

logical-system *logical-system-name*—(Optional) Clear entries for only the specified logical system from the ARP table (only available in main router context).

vpn *vpn*—(Optional) Clear entries from the ARP table for the specified virtual private network (VPN).

Required Privilege Level

clear

Related Documentation

- *set cli logical-system*
- *show arp*
- show dhcp-security arp inspection statistics on page 123
- Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity on page 18

List of Sample Output

clear arp all on page 121
clear arp logical-system ls1 on page 121

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Copyright © 2017, Juniper Networks, Inc.

Sample Output

clear arp all

```
user@host> clear arp all
192.168.71.254   deleted
192.168.65.46    deleted
192.168.64.10    deleted
10.0.12.14       deleted
10.0.17.14       deleted
```

clear arp logical-system ls1

```
user@host> clear arp logical-system ls1
192.168.71.254   deleted
192.168.65.46    deleted
192.168.64.10    deleted
10.0.12.14       deleted
10.0.17.14       deleted
```

Copyright © 2017, Juniper Networks, Inc.

clear dhcp-security binding

Syntax

clear dhcp-security binding
<interface *interface-name*>
<ip-address *ip-address*>
<statistics>
<vlan *vlan-name*>

Release Information

Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Command introduced in Junos OS Release 14.1 for the MX Series.

Description

Clear the DHCP snooping database information.

Options

interface ***interface-name***—(Optional) Clear DHCP snooping database information for the specified interface.

ip-address ***ip-address***—(Optional) Clear DHCP snooping database information for the specified IP address.

statistics—(Optional) Clear all DHCP snooping database statistics.

vlan ***vlan-name***—(Optional) Clear DHCP snooping database information for the specified VLAN.

Required Privilege Level

clear

Related Documentation

- show dhcp-security binding on page 125
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 45
- Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity on page 18

Copyright © 2017, Juniper Networks, Inc.

show dhcp-security arp inspection statistics

Syntax **show dhcp-security arp inspection statistics**

Release Information Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Command introduced in Junos OS Release 14.1 for the MX Series.

Description Display Address Resolution Protocol (ARP) inspection statistics.

Required Privilege Level view

Related Documentation

- show dhcp-security binding on page 125
- clear dhcp-security binding on page 122
- *clear interfaces statistics*
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 45
- Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity on page 18

List of Sample Output show dhcp-security arp inspection statistics on page 124

Output Fields Table 5 on page 123 lists the output fields for the **show dhcp-security arp inspection statistics** command. Output fields are listed in the approximate order in which they appear.

The IP source guard database table shows the untrusted access interfaces in VLANs that have been enabled for IP source guard. The entries include the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another.

Table 5: show dhcp-security 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 that underwent ARP inspection.	All levels
ARP inspection pass	Total number of packets that passed ARP inspection.	All levels
ARP inspection fail	Total number of packets that failed ARP inspection.	All levels

Copyright © 2017, Juniper Networks, Inc.

Sample Output

show dhcp-security arp inspection statistics

```
user@device> show dhcp-security arp inspection statistics

Interface      Packets received   ARP inspection pass   ARP inspection fail
ge-0/0/30.0    7                  7                     0
ge-0/0/4.0     3                  3                     0
ge-0/0/6.0     72                 4                     68
```


Copyright © 2017, Juniper Networks, Inc.

show dhcp-security binding

Syntax

show dhcp-security binding
<**interface** *interface-name*>
<**ip-address** *ip-address*>
<**ip-source-guard** *ip-sg-name*>
<**statistics**>
<**vlan** *vlan-name*>

Release Information

Command introduced in Junos OS Release 12.1 for the QFX Series.
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Command introduced in Junos OS Release 14.1 for the MX Series.

Description

Display the DHCP snooping database information.

Options

interface ***interface-name***—(Optional) Display the DHCP snooping database information for an interface.

ip-address ***ip-address***—(Optional) Display the DHCP snooping database information for an IP address.

vlan ***vlan-name***—(Optional) Display the DHCP snooping database information for a VLAN.

Required Privilege Level

view

Related Documentation

- show dhcp-security binding ip-source-guard on page 128
- clear dhcp-security binding on page 122
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 45
- Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity on page 18

List of Sample Output

show dhcp-security binding on page 126
show dhcp-security binding interface on page 126
show dhcp-security binding ip-address on page 127
show dhcp-security binding vlan on page 127

Output Fields

Table 6 on page 126 lists the output fields for the **show dhcp-security binding** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2017, Juniper Networks, Inc.

Table 6: show dhcp-security binding Output Fields

Field Name	Field Description	Level of Output
IP Address	IP address of the network device; bound to the MAC address.	All levels
MAC address	MAC address of the network device; bound to the IP address.	All levels
VLAN	VLAN name of the network device whose MAC address is shown.	All levels
Expires	The time, in seconds, remaining before the lease of the IP address to the MAC address expires. This field is **0** for static entries.	All levels
State	Specifies whether the IP address is: • **BOUND**: Leased to the MAC address for a limited period of time. • **STATIC**: Attached to a fixed MAC address.	All levels
Interface	Interface address (port).	All levels

Sample Output

show dhcp-security binding

```
user@device> show dhcp-security binding

IP address       MAC address        Vlan     Expires State   Interface
10.1.1.10        00:10:00:20:00:01  vlan20   0       STATIC  ge-0/0/4.0

10.1.1.18        00:10:94:00:00:34  vlan20   86287   BOUND   ge-0/0/6.0

10.1.1.15        00:10:94:00:00:55  vlan20   86265   BOUND   ge-0/0/4.0

10.1.1.16        00:10:94:00:00:56  vlan20   86265   BOUND   ge-0/0/4.0

10.1.1.19        00:10:94:00:00:5b  vlan20   86287   BOUND   ge-0/0/6.0

10.1.1.20        00:10:94:00:00:5c  vlan20   86287   BOUND   ge-0/0/6.0

10.1.1.21        00:10:94:00:00:5d  vlan20   86287   BOUND   ge-0/0/6.0

10.1.1.17        00:10:94:00:00:68  vlan20   86265   BOUND   ge-0/0/4.0
```

show dhcp-security binding interface

```
user@device> show dhcp-security binding interface ge-0/0/6

IP address       MAC address        Vlan     Expires State   Interface
10.1.1.18        00:10:94:00:00:34  vlan20   86282   BOUND   ge-0/0/6.0

10.1.1.19        00:10:94:00:00:5b  vlan20   86282   BOUND   ge-0/0/6.0

10.1.1.20        00:10:94:00:00:5c  vlan20   86282   BOUND   ge-0/0/6.0
```


Copyright © 2017, Juniper Networks, Inc.

```
10.1.1.21          00:10:94:00:00:5d   vlan20   86282   BOUND   ge-0/0/6.0
```

show dhcp-security binding ip-address

```
user@device> show dhcp-security binding ip-address
IP address      MAC address         Vlan         Expires     State      Interface
10.1.1.18      00:10:94:00:00:34     vlan20       86282       BOUND      ge-0/0/6.0
```

show dhcp-security binding vlan

```
user@device> show dhcp-security binding vlan vlan20
IIP address      MAC address         Vlan         Expires     State      Interface
10.1.1.18      00:10:94:00:00:34     vlan20       86282       BOUND      ge-0/0/6.0
```

Copyright © 2017, Juniper Networks, Inc.

show dhcp-security binding ip-source-guard

Syntax **show dhcp-security binding ip-source-guard**

Release Information Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Command introduced in Junos OS Release 14.1 for the MX Series.

Description Display IP source guard database table.

Required Privilege Level view

Related Documentation

- show dhcp-security binding on page 125
- clear dhcp-security binding on page 122
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 45
- Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity on page 18

List of Sample Output show dhcp-security binding ip-source-guard on page 129

Output Fields Table 7 on page 128 lists the output fields for the **show dhcp-security binding ip-source-guard** command. Output fields are listed in the approximate order in which they appear.

The IP source guard database table shows the untrusted access interfaces in VLANs that have been enabled for IP source guard. The entries include the IP addresses and MAC addresses that are bound to one another.

Table 7: show dhcp-security binding ip-source-guard Output Fields

Field Name	Field Description	Level of Output
IP Address	IP address of the network device; bound to the MAC address.	All levels
MAC address	MAC address of the network device; bound to the IP address.	All levels
VLAN	VLAN name of the network device whose MAC address is shown.	All levels
Expires	The time, in seconds, remaining before the lease of the IP address to the MAC address expires.	All levels

Copyright © 2017, Juniper Networks, Inc.

Table 7: show dhcp-security binding ip-source-guard Output Fields *(continued)*

Field Name	Field Description	Level of Output
State	Specifies whether the IP address is: • **BOUND**: Temporarily leased to the MAC address for a limited period of time. • **STATIC**: Attached to a fixed MAC address.	All levels
Interface	Interface address (port).	All levels

Sample Output

show dhcp-security binding ip-source-guard

```
user@device> show dhcp-security binding ip-source-guard

IP address        MAC address         Vlan     Expires State   Interface
10.1.1.10         00:10:00:20:00:01   vlan20   0       STATIC  ge-0/0/4.0

10.1.1.18         00:10:94:00:00:34   vlan20   86276   BOUND   ge-0/0/6.0

10.1.1.15         00:10:94:00:00:55   vlan20   86254   BOUND   ge-0/0/4.0

10.1.1.16         00:10:94:00:00:56   vlan20   86254   BOUND   ge-0/0/4.0

10.1.1.19         00:10:94:00:00:5b   vlan20   86276   BOUND   ge-0/0/6.0

10.1.1.20         00:10:94:00:00:5c   vlan20   86276   BOUND   ge-0/0/6.0

10.1.1.21         00:10:94:00:00:5d   vlan20   86276   BOUND   ge-0/0/6.0

10.1.1.17         00:10:94:00:00:68   vlan20   86254   BOUND   ge-0/0/4.0
```

Copyright © 2017, Juniper Networks, Inc.

Copyright © 2017, Juniper Networks, Inc.

CHAPTER 6

Operational Commands for Layer 2 Device Security

- clear bridge recovery-timeout

Copyright © 2017, Juniper Networks, Inc.

clear bridge recovery-timeout

Syntax clear bridge recovery-timeout
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 14.1 for MX Series routers.

Description Clear all storm control errors from all the Ethernet switching interfaces on the switch, and restore the interfaces to service.

Options interface *interface-name*—Clear all storm control errors from the Ethernet switching interfaces on the interface specified in the command and restore this interface to service.

Required Privilege Level clear

Related Documentation
- Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 59

List of Sample Output clear bridge recovery-timeout (interface interface-name) on page 132

Sample Output

clear bridge recovery-timeout (interface interface-name)

```
user@host> clear bridge recovery-timeout interface ae0.0
user@host> clear bridge recovery-timeout interface ae0.0
```


Copyright © 2017, Juniper Networks, Inc.