Junos® OS for EX Series Ethernet Switches

Port Security for EX9200 Switches

Release
13.3

Published: 2014-06-11

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

Junos® OS for EX Series Ethernet Switches Port Security for EX9200 Switches
Release 13.3

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- EX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 2: Text and Syntax Conventions

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

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

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

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

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

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

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

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Port Security Overview

Port Security Overview

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

Juniper Networks Junos operating system (Junos OS) provides features to help secure ports on the 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 devices'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 option 82—Also known as the DHCP relay agent information option. This feature helps protect the switching device against attacks such as spoofing of IP addresses and media access control (MAC) addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.
- DHCP snooping—Filters and blocks ingress DHCP server messages on untrusted ports. Builds and maintains an IP address to MAC address binding (IP-MAC binding) database, which is called the DHCP snooping database. DHCP snooping is enabled on a VLAN

or bridge domain. The details of enabling DHCP snooping depend on the particular device.

NOTE: Most port security features depend on DHCP snooping. However, DHCP snooping is not enabled in the default switching device configurations.

- DHCPv6 snooping with Option 37—Option 37 is the DHCPv6 equivalent of Option 82 and is enabled by default when DHCPv6 snooping is enabled for a VLAN. Note that it is not available on MX Series routers.
- Dynamic ARP inspection (DAI)—Prevents ARP spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable DAI on a VLAN or bridge domain.
- Neighbor Discovery (ND) 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 ND inspection on a VLAN. Note that it is not available on MX Series routers.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. With IP source guard enabled, the source IP address in the packet sent from an untrusted access interface is validated against the source MAC address in the DHCP snooping database. The packet is forwarded if the source IP-MAC binding is valid; if the binding is not valid, the packet is discarded. You enable IP source guard on a VLAN, or bridge domain. IPv6 source guard is supported on EX Series switches, but not MX routers.

NOTE: IP source guard is not supported on the QFX Series.

- MAC limiting—Protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You can enable MAC limiting on an interface.
- MAC move limiting —(Not supported on EX9200) Tracks MAC movement and detects MAC spoofing on access ports. You enable this feature on a VLAN, 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 ports that connect to Ethernet endpoints such as user PCs and laptops, servers, and printers. Trunk ports are ports that connect to other Ethernet switches or to routers.)

Related Documentation

- *Security Features for EX Series Switches Overview*
- Understanding DHCP Snooping for Port Security on page 12
- Understanding DAI for Port Security on page 5
- Understanding IP Source Guard for Port Security on EX Series Switches on page 18
- *Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches*
- Understanding DHCP Option 82 for Port Security on Switching Devices on page 8

Understanding DAI for Port Security

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 5
- ARP Spoofing on page 5
- Dynamic ARP Inspection on page 6
- Prioritizing Inspected Packets on page 7

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.

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 switching device 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, which have the sender IP address 0.0.0.0, are validated by DAI.

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

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

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

NOTE:

- If your 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)" on page 38 for information about configuring an access interface to be a DHCP trusted port. .
- If your switching device is an EX Series switch and is not using 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.**

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 on page 3
- Understanding DHCP Snooping for Port Security on page 12
- *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 on page 25
- *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) on page 37
- *Enabling Dynamic ARP Inspection (J-Web Procedure)*

Understanding DHCP Option 82 for Port Security on Switching Devices

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 Juniper Networks Junos operating system (Junos OS) implementation of DHCP option 82 supports RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

This topic covers:

DHCP Option 82 Processing

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 9 for details about option 82 information.

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)" on page 41.
- 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)*.

When 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.
4. The switching device strips the option 82 information from the response packet.
5. The switching device forwards the response packet to the client.

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

Suboption Components of Option 82

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 or 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 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.

Switching Device Configurations That Support Option 82

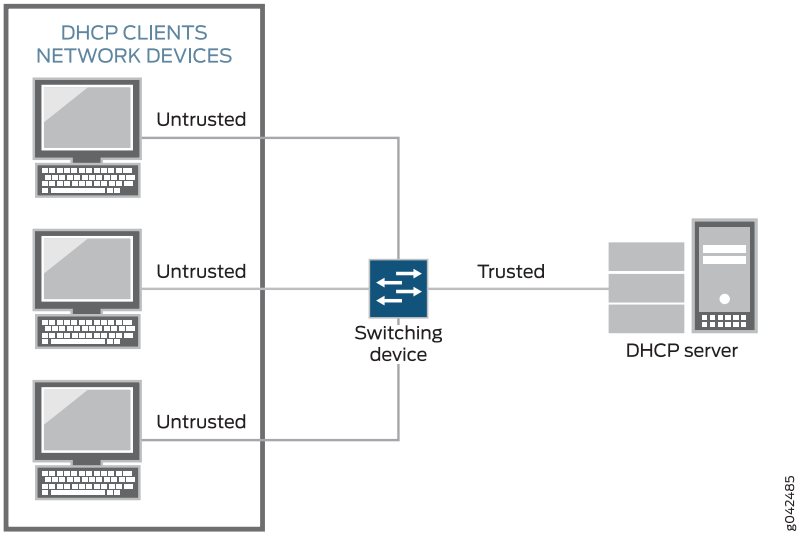
Switching device configurations that support option 82 are:

- Switching Device, Clients and DHCP Server Are on Same VLAN or Bridge Domain on page 10
- Switching Device Acts as a Relay Agent on page 10

Switching Device, Clients and DHCP Server Are on 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 1 on page 10.

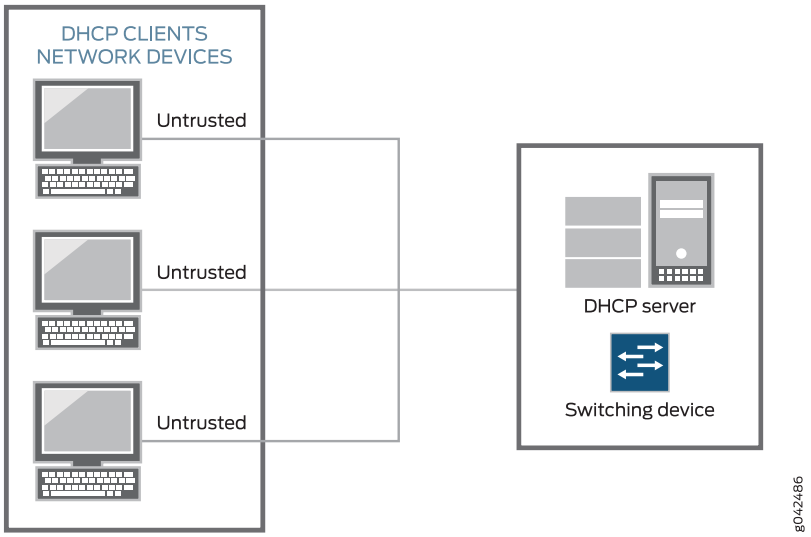
Figure 1: DHCP Clients, Switching Device, and DHCP Server Are All on Same VLAN or Bridge Domain



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 2 on page 11 illustrates a scenario for the switching device acting as an extended relay server; in this instance, the switching device relays requests to the server.

Figure 2: Switching Device Acting as an Extended Relay Server



DHCPv6 Option 37

NOTE: MX Series routers do not support DHCPv6.

Option 37 is the DHCPv6 equivalent of DHCP option 82 and is used by relay agents to identify themselves to the server. The switching device appends information about the network location of the client to DHCPv6 packets sent from the client towards the server. The option 37 value consists of an enterprise ID, VLAN ID, and the MAC address of the interface on which the switching device received the request message from the client. These fields in the header are fixed, unlike option 82 suboptions, which can be configured.

DHCPv6 option 37 is enabled automatically when DHCPv6 snooping is enabled on a VLAN. This option can be disabled for a defined set of access interfaces within the VLAN by using the **set vlans *vlan-name* forwarding-options dhcp-security group *group-name* overrides no-option37** command.

Related Documentation

- Understanding Port Security on page 3
- *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) on page 41

Understanding DHCP Snooping for Port Security

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

- DHCP Snooping Basics on page 12
- DHCP Snooping Process on page 13
- DHCP Server Access on page 14
- DHCP Snooping Table on page 17
- Static IP Address Additions to the DHCP Snooping Database on page 17
- Snooping DHCP Packets That Have Invalid IP Addresses on page 17
- Prioritizing Snooped Packets on page 18

DHCP Snooping Basics

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

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

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

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

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

Entries in the DHCP database are updated in these events:

- When a DHCP client releases an IP address (sends a DHCPRELEASE message), the associated mapping entry is deleted from the database.

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

TIP: By default, the IP-MAC bindings are lost when the 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 only from particular VLANs. Doing this prevents spoofing of DHCP server messages.

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

DHCP Snooping Process

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

NOTE: When DHCP snooping is enabled for a VLAN, all DHCP packets sent from 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 database in accordance with the type of packet received:
   - Upon receipt of a DHCPACK packet, the switch updates lease information for the IP-MAC binding in its database.
   - Upon receipt of a DHCPNACK packet, the switch deletes the placeholder.

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

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

DHCP Server Access

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

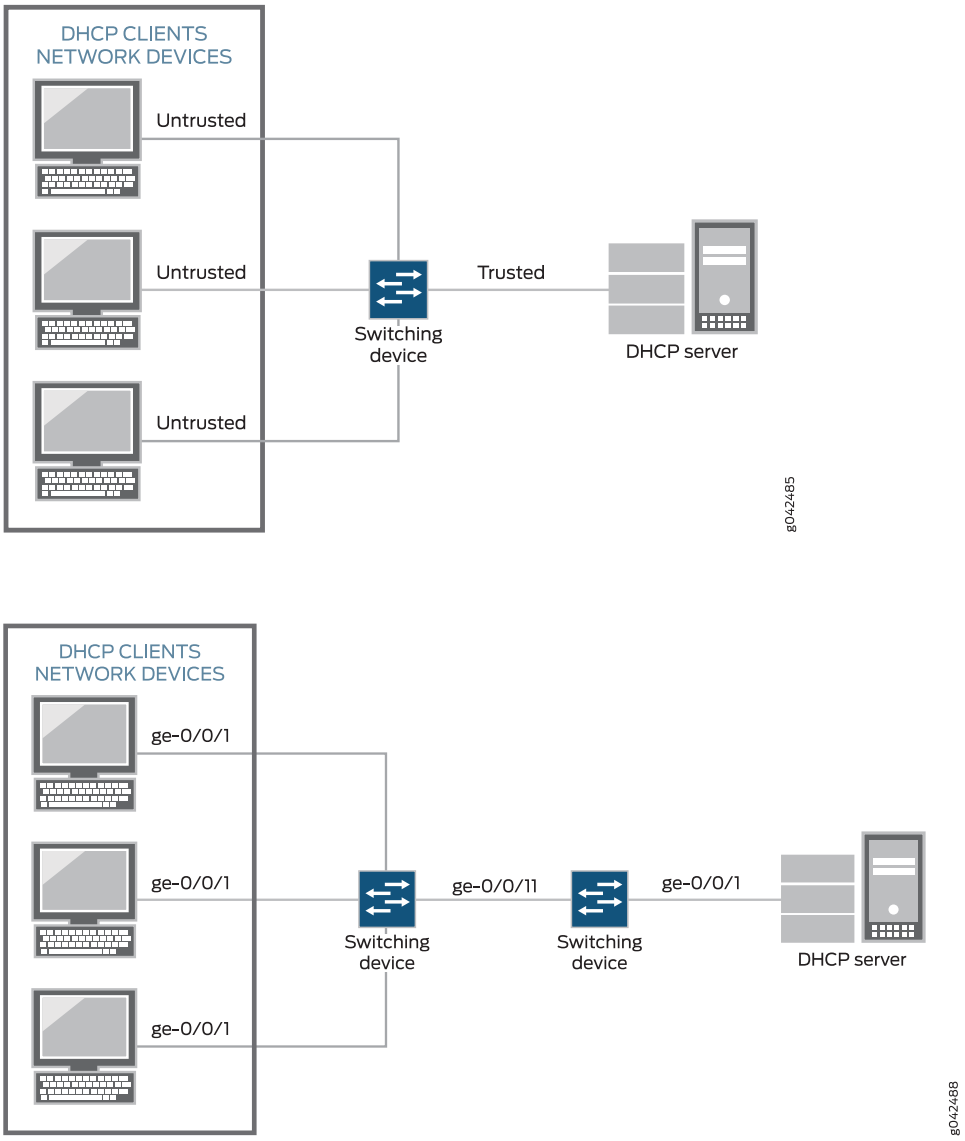
- Switching Device DHCP Clients, and DHCP Server Are All on the Same VLAN on page 14
- Switching Device Acts as DHCP Server on page 15
- Switching Device Acts as Relay Agent on page 16

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 3 on page 15.
- The server is connected to an intermediary switching device (Switching Device 2) that is connected through a trunk port to the device (Switching Device 1) that the DHCP clients are connected to. 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. See Figure 4 on page 15—in the figure, **ge-0/0/11** is a trusted trunk port.

Figure 3: DHCP Server Connected Directly to Switching Device

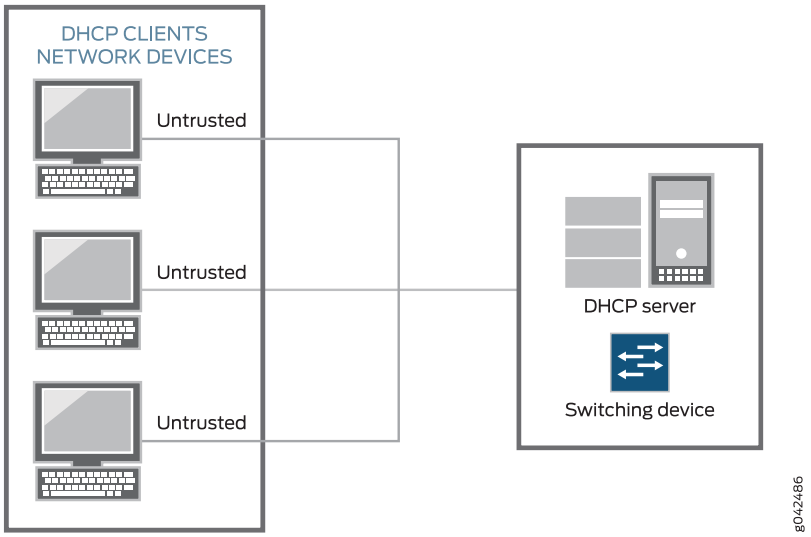


Switching Device Acts as DHCP Server

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

The switching device itself is configured as a DHCP server; this is known as a “local” configuration. See Figure 5 on page 16.

Figure 5: Switching Device Is the DHCP Server



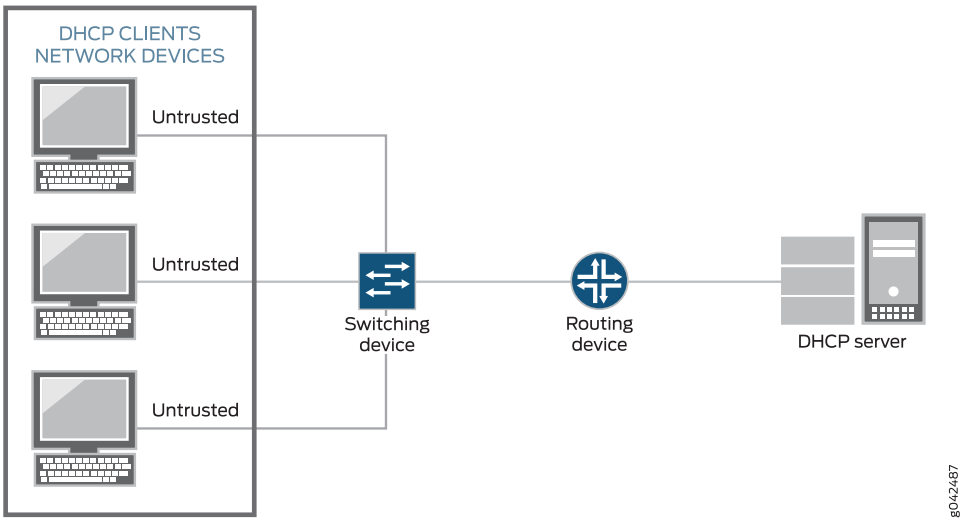
Switching Device Acts as Relay Agent

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

These two scenarios illustrate the 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 6 on page 17.

Figure 6: Switching Device Acting as Relay Agent Through Router to DHCP Server



DHCP Snooping Table

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

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

Static IP Address Additions to the DHCP Snooping Database

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

Snooping DHCP Packets That Have Invalid IP Addresses

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

Prioritizing Snooped Packets

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

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

Related Documentation

- Understanding Port Security on page 3
- Understanding Trusted DHCP Servers for Port Security on page 21
- Understanding DHCP Option 82 for Port Security on Switching Devices on page 8
- *Understanding DHCP Services for Switches*
- *DHCP/BOOTP Relay for Switches Overview*
- *Example: Configuring Basic Port Security Features*
- *Enabling DHCP Snooping (CLI Procedure)*
- *Enabling DHCP Snooping (J-Web Procedure)*
- *Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure)*

Understanding IP Source Guard for Port Security on EX Series Switches

Ethernet LAN switches are vulnerable to attacks that involve spoofing (forging) of source IP addresses or source MAC addresses. You can use the IP source guard access port security feature on Juniper Networks EX Series Ethernet Switches to mitigate the effects of these attacks.

- IP Address Spoofing on page 19
- How IP Source Guard Works on page 19
- IPv6 Source Guard on page 19
- The DHCP Snooping Table on page 20
- Typical Uses of Other Junos Operating System (Junos OS) Features with IP Source Guard on page 20

IP Address Spoofing

Hosts on access interfaces can spoof source IP addresses and source MAC addresses by flooding the switch with packets containing invalid addresses. Such attacks combined with other techniques such as TCP SYN flood attacks can result in denial-of-service (DoS) attacks. With source IP address or source MAC address spoofing, the system administrator cannot identify the source of the attack. The attacker can spoof addresses on the same subnet or on a different subnet.

How IP Source Guard Works

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 switch against entries stored in the DHCP snooping database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the switch does not forward the packet—that is, the packet is discarded.

NOTE:

- If your switch uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, DHCP snooping is enabled automatically when you enable IP source guard on a VLAN. See "Configuring IP Source Guard (CLI Procedure)" on page 35.
- If your switch is *not* using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style and you enable IP source guard on a VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to the VLAN.

IP source guard applies its checking rules to packets sent from untrusted access interfaces on those VLANs. By default, on EX Series switches, access interfaces are untrusted and trunk interfaces are trusted. IP source guard does not check packets that have been sent to the switch by devices connected to either trunk interfaces or to trusted access interfaces so that a DHCP server can be connected to that interface to provide dynamic IP addresses.

NOTE: IP source guard is not supported on trunk interfaces regardless of whether the trunk interface is trusted or untrusted.

IPv6 Source Guard

IPv6 source guard is available on switches with support for DHCPv6 snooping. DHCPv6 snooping is enabled automatically when IPv6 source guard is configured on a VLAN. To determine whether your switch supports DHCPv6 snooping, see the *EX Series Switch Software Features Overview*.

The DHCP Snooping Table

IP source guard obtains information about IP address to MAC address bindings (IP-MAC binding) from the DHCP snooping table, also known as the DHCP binding table. The DHCP snooping table is populated either through dynamic DHCP snooping or through configuration of specific static IP address to MAC address bindings. For more information about the DHCP snooping table, see *Understanding DHCP Snooping for Port Security*.

To display the DHCP snooping table, issue the operational mode command that appears in the command-line interface (CLI) for your switch.

For DHCPv4 snooping:

- (For non-ELS switches) **show ip-source-guard**
- (EX4300 switches only) show dhcp-security binding ip-source-guard

For DHCPv6 snooping:

- (EX4300 switches only) **show dhcp-security ipv6 binding**

Typical Uses of Other Junos Operating System (Junos OS) Features with IP Source Guard

You can configure IP source guard with various other features on the EX Series switch to provide access port security, including:

- VLAN tagging (used for voice VLANs)
- GRES (Graceful Routing Engine switchover)
- Virtual Chassis configurations (See *EX Series Switch Software Features Overview* for list of models that support IP Source Guard.)
- Link aggregation groups (LAGs)
- 802.1X user authentication in single supplicant, single-secure supplicant, or multiple supplicant mode.

NOTE: If you are implementing 801.X user authentication in single-secure supplicant or multiple supplicant mode, use the following configuration guidelines:

- If the 802.1X interface is part of an untagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has untagged membership. This also applies to IPv6 source guard and DHCPv6 snooping.
- If the 802.1X interface is part of a tagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has tagged membership. This also applies to IPv6 source guard and DHCPv6 snooping.

Related Documentation

- Understanding DHCP Snooping for Port Security on page 12
- Configuring IP Source Guard (CLI Procedure) on page 35
- *Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN*
- *Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 25

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 Port Security on page 12
- *Example: Configuring Basic Port Security Features*
- *Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 25
- *Enabling a Trusted DHCP Server (CLI Procedure)*
- Enabling a Trusted DHCP Server (CLI Procedure) on page 38
- *Enabling a Trusted DHCP Server (J-Web Procedure)*

PART 2

Configuration

CHAPTER 2

Configuration Examples

Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

NOTE: On EX9200 switches, DHCP snooping, DAI, and IP source guard are not supported in an MC-LAG scenario.

This example describes how to enable IP source guard and Dynamic ARP Inspection (DAI) on a specified VLAN to protect the switch 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 VLAN.

Requirements

This example uses the following hardware and software components:

- One EX4300 switch or EX9200 switch
- Junos OS Release 13.2X50-D10 or later for EX Series switches
- A DHCP server to provide IP addresses to network devices on the switch

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 switch.
- Configured the VLAN to which you are adding DHCP security features. See *Configuring VLANs for EX Series Switches (CLI Procedure)*.

Overview and Topology

Ethernet LAN switches 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 switch. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. 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 switch against entries stored in the DHCP snooping database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the switch 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 LAN. Instead of the switch 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 switch that should have gone to another device. The result is that traffic from the switch is misdirected and cannot reach its proper destination.

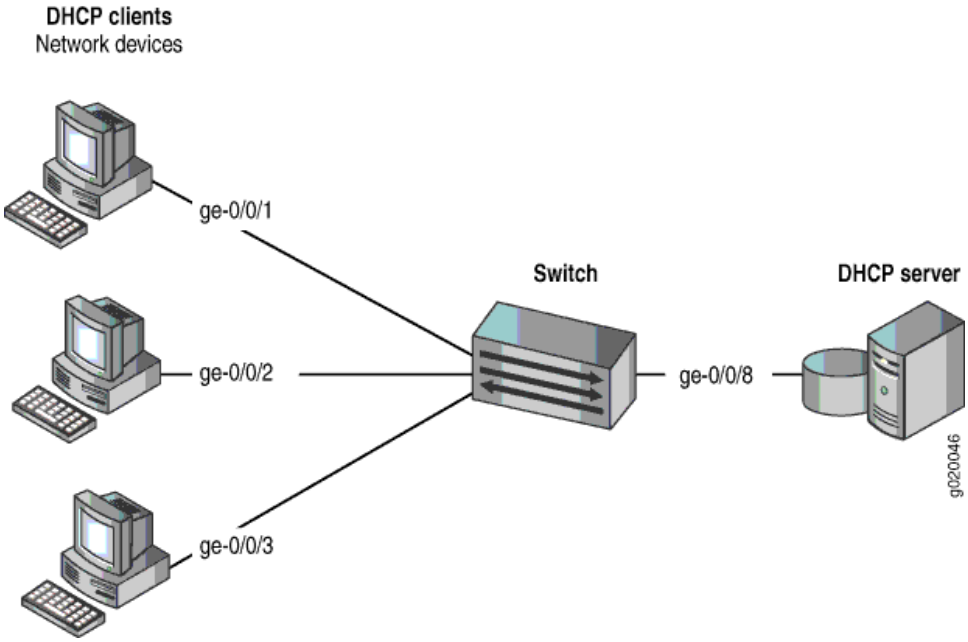
NOTE: When dynamic ARP inspection (DAI) is enabled, the switch logs the number of invalid ARP packets that it receives on each interface, along with the sender's IP and MAC addresses. You can use these log messages to discover ARP spoofing on the network.

This example shows how to configure these important port security features on a switch that is connected to a DHCP server. The setup for this example includes the VLAN **employee-vlan** on the switch. Figure 7 on page 27 illustrates the topology for this example.

NOTE:

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

Figure 7: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 3 on page 27.

Table 3: Components of the Port Security Topology

Properties	Settings
Switchhardware	One EX4300 or EX9200 switch
VLAN name and ID	**employee-vlan**, tag **20**
VLAN subnets	**192.0.2.16/28** **192.0.2.17** through **192.0.2.30** **192.0.2.31** is the subnet's broadcast address
Interfaces in **employee-vlan**	**ge-0/0/1**, **ge-0/0/2**, **ge-0/0/3**, **ge-0/0/8**
Interface connecting to DHCP server	**ge-0/0/8**

In this example, the switch 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 VLAN (**employee-vlan**) has been configured to include the specified interfaces.

Configuration

To configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping) to protect the switch against IP spoofing and ARP attacks:

CLI Quick Configuration

To quickly configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping), copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans employee-vlan forwarding-options dhcp-security ip-source-guard
set vlans employee-vlan forwarding-options dhcp-security arp-inspection
```

Step-by-Step Procedure

Configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping) on the VLAN:

1. Configure IP source guard on the VLAN:

   ```
   [edit vlans employee-vlan forwarding-options dhcp-security]
   user@switch# set ip-source-guard
   ```

2. Enable DAI on the VLAN:

   ```
   [edit vlans employee-vlan forwarding-options dhcp-security]
   user@switch# set arp-inspection
   ```

Results

Check the results of the configuration:

```
user@switch> show vlans employee-vlan forwarding-options
employee-vlan {
  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 Switch on page 28
- Verifying That IP Source Guard is Working on the VLAN on page 29
- Verifying That DAI Is Working Correctly on the Switch on page 29

Verifying That DHCP Snooping Is Working Correctly on the Switch

Purpose

Verify that DHCP snooping is working on the switch.

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

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

```
user@switch> show dhcp-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 switch has been set to trusted, the output (see 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 VLAN

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

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

```
user@switch> 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 enabled for IP source guard.

Verifying That DAI Is Working Correctly on the Switch

Purpose Verify that DAI is working on the switch.

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

Display the DAI information:

```
user@switch> show 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 switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

Related Documentation

- Configuring IP Source Guard (CLI Procedure) on page 35
- Enabling Dynamic ARP Inspection (CLI Procedure) on page 37
- *Enabling Dynamic ARP Inspection (J-Web Procedure)*

CHAPTER 3

Configuration Tasks

Configuring Port Security (CLI Procedure)

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

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

The following port security features are supported for DHCPv4:

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

The following port security features are supported for DHCPv6:

- DHCPv6 snooping
- Neighbor Discovery (ND) inspection
- IPv6 source guard
- DHCPv6 option 37

DHCP snooping for DHCPv4 and DHCPv6 is disabled in the default configuration. There is no explicit configuration for enabling DHCP snooping. If you configure any other port security features for a VLAN at the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level, then DHCP snooping and DHCPv6 snooping are automatically enabled on that VLAN.

DAI, ND inspection, IP source guard and IPv6 source guard, and DHCP option 82 are configured per VLAN. You must configure a VLAN prior to configuring these DHCP port security features. See *Configuring VLANs for EX Series Switches (CLI Procedure)*.

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

- Specifying a specific interface to have a static IP-MAC address (**static-ip** or *static-ipv6*).
- Specifying an access interface to act as a trusted interface to a DHCP server (**trusted**)
- Specifying a specific interface not to transmit DHCP (**no-option-82** or *no-option37*)

NOTE:

- If you configure any of these DHCP port security features—including configuring a group of access interfaces—for a specific VLAN, the switch software enables automatically enables DHCP snooping for that VLAN.
- If you explicitly disable DHCP snooping by setting no-dhcp-snooping or *no-dhcpv6-snooping* for a specific VLAN, the switch software automatically disables any other DHCP port security features for that VLAN.

NOTE: Trunk interfaces are trusted by default. However, on an EX9200 switch, you can override this default behavior and set a trunk interface as **untrusted.**

For additional details, see:

- Enabling Dynamic ARP Inspection (CLI Procedure) on page 37
- *Enabling IPv6 Neighbor Discovery Inspection*
- Configuring IP Source Guard (CLI Procedure) on page 35
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 41

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

- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 36
- Enabling a Trusted DHCP Server (CLI Procedure) on page 38

Related Documentation

- Understanding Port Security on page 3
- Understanding DHCP Snooping for Port Security on page 12

Configuring IP Source Guard (CLI Procedure)

NOTE: This example uses Junos OS for MX Series routers and EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switching device runs software that does not support ELS, see *Configuring IP Source Guard (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

NOTE: On EX9200 switches, IP source guard is not supported in an MC-LAG scenario.

You can use the IP source guard access port security feature on EX Series switches 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 switch does not forward the packet—that is, the packet is discarded.

You configure the IP source guard feature on a specific VLAN. When you configure IP source guard on a VLAN, the switch automatically enables DHCP snooping on that VLAN.

IPv6 source guard is supported on switches with support for DHCPv6 snooping. On these switches, configuring IP source guard or IPv6 source guard on a VLAN automatically enables DHCP snooping and DHCPv6 snooping on that VLAN.

IP source guard and IPv6 source guard can be applied only to untrusted interfaces. Access interfaces are untrusted by default.

IP source guard and IPv6 source guard can be used together with 802.1X user authentication in single supplicant, single-secure supplicant, or multiple supplicant mode.

Before you can configure IP source guard or IPv6 source guard on a VLAN, you must configure the VLAN. See *Configuring VLANs for EX Series Switches (CLI Procedure)*.

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

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set ip-source-guard
```

To configure IPv6 source guard on a specific VLAN by using the CLI:

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set ipv6-source-guard
```

Related Documentation

- *Verifying That IP Source Guard Is Working Correctly*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 25

- *Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect the Switch from IPv6 Address Spoofing*
- Understanding IP Source Guard for Port Security on EX Series Switches on page 18

Configuring Static IP Addresses for DHCP and DHCPv6 Bindings on Access Ports (CLI Procedure)

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

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*. Static IPv6 address assignment is also available for DHCPv6.

Before you can perform this procedure, you must configure the VLAN. See *Configuring VLANs for EX Series Switches (CLI Procedure)*.

To configure a static IP address to MAC address (IP-MAC) binding in the DHCP snooping database, you must first create a group of access interfaces under **[edit vlans *vlan-name* forwarding-options** dhcp-security**]**. Creating this group automatically enables DHCP snooping, which is a prerequisite for creating the DHCP snooping database. 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.

NOTE: On switches that support DHCPv6, creating the group of interfaces will automatically enable both DHCP and DHCPv6 snooping.

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

- `[edit vlans vlan-name forwarding-options dhcp-security]`
  user@switch# set group ***group-name*** **interface** ***interface-name*** static-ip ***ip-address*** mac ***mac-address***

To configure a static IPv6-MAC address binding in the DHCPv6 snooping database:

- `[edit vlans vlan-name forwarding-options dhcp-security]`
  user@switch# set group ***group-name*** **interface** ***interface-name*** **static-ipv6** ***ip-address*** mac ***mac-address***

Related Documentation

- show dhcp-security binding on page 85
- *Verifying That DHCP Snooping Is Working Correctly*

- Understanding DHCP Snooping for Port Security on page 12

Enabling Dynamic ARP Inspection (CLI Procedure)

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

NOTE: On EX9200 switches, DHCP snooping, DAI, and IP source guard are not supported in an MC-LAG scenario.

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

Before you can enable DAI on a VLAN, you must configure the VLAN. See *Configuring VLANs for EX Series Switches (CLI Procedure)*.

To enable DAI on a VLAN by using the CLI:

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set arp-inspection
```

Related Documentation

- *Enabling Dynamic ARP Inspection (J-Web Procedure)*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 25
- Understanding DAI for Port Security on page 5

Enabling a Trusted DHCP Server (CLI Procedure)

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Enabling a Trusted DHCP Server (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

You can configure any interface on a switch that connects to a DHCP server as a trusted interface (port). Configuring a DHCP server on a trusted interface protects against rogue DHCP servers sending leases.

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 VLAN, 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 VLAN. See *Configuring VLANs for EX Series Switches (CLI Procedure)*.

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

1. Configure a group within a VLAN with a specific access interface:

   ```
   [edit vlans vlan-name forwarding-options dhcp-security ]
   user@switch# 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 vlans vlan-name forwarding-options dhcp-security group group-name]
   user@switch# set overrides trusted
   ```

Related Documentation

- *Enabling a Trusted DHCP Server (J-Web Procedure)*
- Understanding Trusted DHCP Servers for Port Security on page 21

Configuring Persistent Bindings in the DHCP or DHCPv6 Snooping Database (CLI Procedure)

NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure)*. 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 switch reboots. You can configure the IP-MAC address bindings in the DHCP

snooping database to persist through switch reboots by configuring a storage location for the DHCP snooping database file. When you configure the storage location, you must specify how frequently the switch writes the database entries into the DHCP snooping database file. You can also configure the IPv6-MAC address bindings to persist through switch reboots on switches that support DHCPv6 snooping.

The DHCP snooping database of IP-MAC address bindings is created when you enable any of the port security features for a specific VLAN in the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy. On switches that support DHCPv6, enabling any of these features also creates the DHCPv6 snooping database. DHCP snooping and DHCPv6 snooping are not enabled by default.

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

- For DHCP snooping:

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

  For example:

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

- For DHCPv6 snooping:

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

  For example:

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

  For example:

  ```
  [edit system processes]
  user@switch# set dhcp-service dhcp-snooping-file tftp://test:Test123@14.1.2.1 write-interval
  60
  ```

- For DHCPv6 snooping:

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

  For example:

  ```
  [edit system processes]
  user@switch# set dhcp-service dhcpv6-snooping-file tftp://test:Test123@14.1.2.1 write-interval
  60
  ```

NOTE: Specify any requisite user credentials for the FTP server before you specify the IP address or hostname. In this example, **test** is the username and **Test123** is the password for FTP server 14.1.2.1.

Related Documentation

- Understanding DHCP Snooping for Port Security on page 12

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

NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

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

You can configure the DHCP option 82 feature in two topologies:

- The switch, DHCP clients, and DHCP server are all on the same VLAN. The switch forwards the clients' requests to the server and forwards the server's responses to the clients. This topic describes this configuration.
- The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as integrated routing and bridging (IRB) interfaces. The switch relays the clients' requests to the server and then forwards the server's responses to the clients. This configuration is described in *Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)*.

Before you configure DHCP option 82 on the switch, perform these tasks:

- Connect and configure the DHCP server.

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

- Configure a VLAN on the switch and associate the interfaces on which the clients and the server connect to the switch with that VLAN. See *Configuring VLANs for EX Series Switches (CLI Procedure)*

To configure DHCP option 82:

1. Specify DHCP option 82 for the VLAN that you configured.

   [edit vlans *vlan-name* forwarding-options dhcp-security]
   user@switch# option-82

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

   The remaining steps are optional.

2. Configure the prefix for the circuit ID suboption to include the switch's hostname or the routing instance name for the VLAN:

   [edit vlans *vlan-name* forwarding-options dhcp-security option-82]
   user@switch# 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 vlans *vlan-name* forwarding-options dhcp-security option-82]
   user@switch# 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 vlans *vlan-name* forwarding-options dhcp-security option-82]
   user@switch# set circuit-id use-vlan-id
5. Specify that the remote ID suboption is included in the DHCP option 82 information:

   [edit vlans *vlan-name* forwarding-options dhcp-security option-82]
   user@switch# 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 vlans *vlan-name* forwarding-options dhcp-security option-82]
   user@switch# set remote-id host-name
7. Specify that the remote ID suboption value contains the interface description:

   [edit vlans *vlan-name* forwarding-options dhcp-security option-82]
   user@switch# set remote-id use-interface-description
8. Specify that the remote ID suboption value contains a character string:

   [edit vlans *vlan-name* forwarding-options dhcp-security option-82]
   user@switch# 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 vlans *vlan-name* forwarding-options dhcp-security option-82]
     user@switch# set vendor-id
   - To configure that the vendor ID suboption value contains a character string value that you specify rather than **Juniper** (the default):

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]
user@switch# set vendor-id mystring
```

Related Documentation

- Understanding DHCP Option 82 for Port Security on Switching Devices on page 8
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

CHAPTER 4

Configuration Statements

[edit vlans] Configuration Statement Hierarchy on EX Series Switches

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

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

This topic lists:

- Supported Statements in the [edit vlans] Hierarchy Level on page 46
- Unsupported Statements in the [edit vlans] Hierarchy Level on page 48

Supported Statements in the [edit vlans] Hierarchy Level

The following hierarchy shows the **[edit vlans]** configuration statements supported on one or more of the EX Series switches:

```
vlans {
    vlan-name {
        description text-description;
        domain-type bridge;
        forwarding-options {
            dhcp-security {
                arp-inspection;
                group group-name {
                    interface interface-name {
                        static-ip ip-address {
                            mac mac-address;
                        }
                    }
                    overrides {
                        no-option82;
                        trusted;
                    }
                }
                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;
            }
          }
        }
        filter {
          input filter-name;
          output filter-name;
        }
        flood {
          input filter-name;
        }
      }
      l3-interface irb.logical-unit-number;
      multicast-snooping-options {
        flood-groups [group-names];
        forwarding-cache {
          threshold {
            reuse threshold;
            suppress threshold;
          }
        }
        graceful-restart {
          disable;
          restart-duration duration;
        }
        host-outbound-traffic {
          dot1p bits;
          forwarding-class forwarding-class;
        }
        multichassis-lag-replicate-state;
        nexthop-hold-time time;
        options {
          syslog {
            level level;
            mark interval;
            upto level;
          }
        }
        traceoptions {
          file filename {
            files number;
            no-world-readable;
            size file-size;
            world-readable;
          }
          flag flag {
            disable;
          }
        }
```

```
    }
    switch-options {
      interface interface-name {
        interface-mac-limit limit {
          packet-action action;
        }
        static-mac mac-address;
      }
      interface-mac-limit limit {
        packet-action action;
      }
      mac-move-limit limit {
        packet-action action;
      }
      mac-table-size limit {
        packet-action drop;
      }
      no-mac-learning;
    }
    vlan-id number;
    vlan-id-list [vlan-id | vlan-id–vlan-id];
  }
}
```

Unsupported Statements in the [edit vlans] Hierarchy Level

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

Table 4: Unsupported [edit vlans] Configuration Statements on EX Series Switches

Statement	Hierarchy Level
NOTE: Variables, such as *filename*, are not shown in the statements or hierarchies.	
mcae-mac-synchronize	**[edit vlans]**
no-irb-layer-2-copy	**[edit vlans]**

Related Documentation

- *Example: Connecting Access Switches to a Distribution Switch*

arp-inspection

Syntax

```
arp-inspection {
  forwarding-class class-name;
}
```

Hierarchy Level

- For platforms with ELS:

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

- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*)],
  [edit forwarding-options dhcp-relay]

Release Information

Statement introduced in Junos OS Release 9.0 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.)
Statement introduced in Junos OS Release 13.2 for the QFX series.

Description

Perform dynamic ARP inspection (DAI) on all VLANs or on the specified VLAN.

When DAI is enabled, the switch logs invalid ARP packets that it receives on each interface, along with the sender's IP and MAC addresses. ARP probe packets, which have the sender IP address 0.0.0.0, are validated by DAI.

NOTE: If you configure DAI at the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level:

- DAI can only be configured for a specific VLAN, not for a list or a range of VLAN IDs.
- DHCP snooping is automatically enabled on the specified VLAN.
- The **forwarding-class** statement is not available at the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level.

See "Enabling Dynamic ARP Inspection (CLI Procedure)" on page 37 for more information about this configuration.

NOTE: On EX9200 switches, DAI is not supported in an MC-LAG scenario.

The remaining statement is explained separately.

Default

Disabled.

Required Privilege Level

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

Related Documentation

- *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 on page 25
- *Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic*
- *Enabling Dynamic ARP Inspection (CLI Procedure)*
- *Enabling Dynamic ARP Inspection (J-Web Procedure)*

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 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.)
Statement introduced in Junos OS Release 14.1 for MX Series routers

Description

Configure the **circuit-id** suboption (suboption 1) of DHCP option 82 (the DHCP relay agent information option) in DHCP packets destined for a DHCP server. This suboption identifies the circuit (the interface, the VLAN, or both) on which the DHCP request arrived.

The remaining statements are explained separately.

Default

If DCHP option 82 is enabled on the switch, the circuit ID is supplied by default in the format ***interface-name*:*vlan-name*** or, on a Layer 3 interface, just ***interface-name***.

Required Privilege Level

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

Related Documentation

- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- *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) on page 41
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

dhcp-security

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 hostname;
      use-interface-description (device | logical);
      use-string string;
    }
    vendor-id {
      use-string string;
    }
  }
}
```

Hierarchy Level [edit vlans *vlan-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.

Description Configure port security features on the switch. 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

NOTE: On EX9200 switches, DHCP snooping, DAI, and IP source guard are not supported in an MC-LAG scenario.

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
- Enabling Dynamic ARP Inspection (CLI Procedure) on page 37
- Configuring IP Source Guard (CLI Procedure) on page 35
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 41
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 36

dhcp-service

Syntax
```
dhcp-service {
  dhcp-snooping-file (local_pathname | remote_URL);
    write-interval interval;
  }
```

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 configureing 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.

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 Performance (CLI Procedure) on page 38

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 device reboots by specifying a local pathname or a remote URL for the storage location of the DHCP snooping database file.

The remaining statement is explained separately.

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 Performance (CLI Procedure) on page 38
- *Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure)*
- Understanding DHCP Snooping for Port Security on page 12

group (DHCP Security)

Syntax

```
group group-name {
  interface interface-name {
    static-ip ip-address {
      mac mac-address;
    }
    static-ipv6 ip-address {
      mac mac-address;
    }
  }
  overrides {
    no-option37;
    no-option-82;
    trusted;
    untrusted;
  }
}
```

Hierarchy Level [edit vlans *vlan-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.

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. 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 (CLI Procedure) on page 36
- Enabling a Trusted DHCP Server (CLI Procedure) on page 38
- Understanding DHCP Snooping for Port Security on page 12

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 option-82 remote-id]**

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

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) on page 41
- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

interface (DHCP Security)

Syntax

```
interface interface-name {
  static-ip ip-address {
    mac mac-address;
  }
  static-ipv6 ip-address {
    mac mac-address;
  }
}
```

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

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** statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches.

Description Configure an interface for a static IPv4 or IPv6 address to MAC address binding (IP-MAC binding) or configure an interface to belong to a group within the VLAN that has DHCP security attributes that are different from the attributes of other interfaces in the VLAN.

The remaining statement is 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 (CLI Procedure) on page 36
- Enabling a Trusted DHCP Server (CLI Procedure) on page 38
- Configuring Port Security (CLI Procedure) on page 32

ip-source-guard

Syntax ip-source-guard;

Hierarchy Level

- For platforms with ELS:

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

- For platforms without ELS:

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

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.)

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

- **ip-source-guard**—Enable IP source guard checking.
- **no-ip-source-guard**—(Not available in **[edit vlans *vlan-name* forwarding-options dhcp-security]**) Disable IP source guard checking.

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

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

See "Configuring IP Source Guard (CLI Procedure)" on page 35 for more information about this configuration.

If you configure IP source guard at the **[edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*)]** hierarchy level:

- You must enable DHCP snooping on all VLANs if you configure IP source guard on all VLANs.
- You must enable DHCP snooping for the specific VLAN if you configure IP source guard on that specific VLAN. Otherwise, the default behavior of no DHCP snooping applies to that VLAN.

See *Enabling DHCP Snooping (CLI Procedure)* for more information about this configuration.

NOTE: On EX9200 switches, IP source guard is not supported in an MC-LAG scenario.

Default Disabled.

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

Related Documentation

- *Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN*
- *Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 25
- *Configuring IP Source Guard (CLI Procedure)*
- Configuring IP Source Guard (CLI Procedure) on page 35

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 MX Series routers.

Description Configure 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 for DHCP Bindings on Access Ports (CLI Procedure)*
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 36
- *Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure)*

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 MX Series routers.

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 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

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 Port Security on page 12

no-option-82

Syntax

no-option-82;

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 forMX series routers.

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*
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 41
- Understanding DHCP Option 82 for Port Security on Switching Devices on page 8
- Understanding DHCP Snooping for Port Security on page 12

overrides (DHCP Security)

Syntax overrides (trusted | untrusted |no-option37 | no-option-82);

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

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 **no-option37** option introduced in Junos OS Release 13.2X51-D20 for EX Series switches.

Description Modify selected attributes of a specific interface within a group of interfaces that is configured within a specified VLAN.

Options

no-option37—The interface specified in this group does not support DHCPv6 option 37.

no-option82—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—do not apply to the interface that is configured with the **overrides** and the **trusted** options. Access interfaces are untrusted by default.

untrusted—(Only for EX9200) The interface specified in this group is untrusted. Trunk interface 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

- Enabling a Trusted DHCP Server (CLI Procedure) on page 38
- Understanding DHCP Snooping for Port Security on page 12
- Understanding DHCP Option 82 for Port Security on Switching Devices on page 8

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 MX Series routers.

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

hostname—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]**
- 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)*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

remote-id

Syntax

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

Hierarchy Level

- For platforms with enhanced Level 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-securityoption-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 option-82]** 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

Insert the **remote-id** suboption of DHCP option 82 (also known as the DHCP relay agent information option) in DHCP request packet headers before forwarding or relaying requests to a DHCP server. This suboption provides a trusted identifier for the host system that has forwarded or relayed requests to the server.

The remaining statements are explained separately, and their availability depends on the hierarchy level at which the **remote-id** suboption is specified, as follows:

- The **prefix**, is *not* supported at the **[edit vlans *vlan-name* forwarding-options dhcp-security option-82]** hierarchy level.
- The statement **host-name** is supported *only* at the **[edit vlans *vlan-name* forwarding-options dhcp-security option-82]** hierarchy level.

Default

If 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 following are true:

- At the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level, the default keyword value is *interface-name*.
- At all other hierarchy levels, the **remote-id** default keyword value is the MAC address of the switch.

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

Related Documentation
- *Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server*
- *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 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 41
- *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.

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 MX Series routers.

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) on page 41
- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*

static-ip

Syntax

```
static-ip ip-addresses {
  vlan vlan-name;
  mac mac-address;
}
```

Hierarchy Level

- For platforms with ELS:

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

- For platforms without ELS:

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

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.)

Description

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

NOTE: The VLAN is specified at the higher hierarchy level when **static-ip** is configured at **[edit vlans *vlan-name* forwarding-options dhcp-security group *group-name* interface *interface-name*]**.

Options

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

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

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure)*
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 36

trusted

Syntax trusted;

Hierarchy Level [edit vlans *vlan-name* forwarding-options dhcp-security 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.

Description Allow DHCP responses from the specified interface. The interface is not subject to DHCP snooping, even if the VLAN is enabled for DHCP snooping.

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

Related Documentation

- Enabling a Trusted DHCP Server (CLI Procedure) on page 38
- Understanding Trusted DHCP Servers for Port Security on page 21
- Understanding DHCP Snooping for Port Security on page 12

untrusted

Syntax untrusted;

Hierarchy Level [edit vlans *vlan-name* forwarding-options dhcp-security group *group-name* overrides]

Release Information Statement introduced in Junos OS Release 13.2 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX series.

Description Override the default behavior of a trunk interface from trusted to untrusted.

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

Related Documentation

- Enabling a Trusted DHCP Server (CLI Procedure) on page 38
- Understanding Trusted DHCP Servers for Port Security on page 21
- Understanding DHCP Snooping for Port Security on page 12

use-interface-description

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

Hierarchy Level

- 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-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 MX Series routers.

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.

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.

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) on page 41
- Understanding Trusted DHCP Servers for Port Security on page 21
- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

use-string

Syntax use-string *string*;

Hierarchy Level

- For platforms with 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 MX Series routers.

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

- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- *Understanding DHCP Option 82 for Port Security on MX Series Routers*
- *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) on page 41
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

use-vlan-id

Syntax use-vlan-id;

Hierarchy Level

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

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

- For platforms without ELS:

  [edit forwarding-options helpers bootp dhcp-option82-circuit-id],
  [edit forwarding-options helpers bootp interface *interface-name* dhcp-option82-circuit-id]

- 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 MX Series routers.

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

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

Related Documentation

- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- *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) on page 41
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

vendor-id

Syntax vendor-id <*string*>;

Hierarchy Level

- For platforms with 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 MX Series routers.

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

- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- *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 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 41

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

write-interval

Syntax write-interval *seconds*;

Hierarchy Level

- For platforms with enhanced Layer 2 software (ELS) (see *Getting Started with Enhanced Layer 2 Software* for information about 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]

- For MX Series routers

  [edit system processes dhcp-service dhcp-snooping-file],

Release Information Statement introduced in Junos OS Release 9.4 for EX Series switches.
Hierarchy level **[edit system processes dhcp-service dhcp-snooping-file]** introduced in Junos OS Release 13.2X50-D10.
Hierarchy level **[edit system processes dhcp-service dhcpv6-snooping-file]** introduced in Junos OS Release 13.2X51-D20.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

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 ethernet-switching-options secure-access-port dhcp-snooping-file]** hierarchy level, see *Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure)*.
- If you are configuring **write-interval** at the **[edit system processes dhcp-service dhcp-snooping-file]** or **[edit system processes dhcp-service dhcpv6-snooping-file]** hierarchy level, see "Configuring Persistent Bindings in the DHCP or DHCPv6 Snooping Database to Improve Performance (CLI Procedure)" on page 38.

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 Port Security on page 12

PART 3

Administration

CHAPTER 5

Operational Commands

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

clear arp

Syntax

clear arp
<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 MX Series routers.

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

none—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 83
- Understanding Port Security on page 3

List of Sample Output

clear arp on page 80
clear arp logical-system ls1 on page 81

Output Fields

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

Sample Output

clear arp

```
user@host> clear arp
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
```

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 MX Series routers.

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 85
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 25
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection on MX Series Routers*
- Understanding Port Security on page 3

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 MX Series routers.

Description Display address resolution protocol (ARP) inspection statistics.

Required Privilege Level view

Related Documentation

- show dhcp-security binding on page 85
- clear dhcp-security binding on page 82
- *clear interfaces statistics*
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 25
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection on MX Series Routers*
- Understanding Port Security on page 3

List of Sample Output show dhcp-security arp inspection statistics on page 83

Output Fields Table 5 on page 83 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

Sample Output

show dhcp-security arp inspection statistics

```
user@switch> 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
```

show dhcp-security binding

Syntax

show dhcp-security binding
<interface *interface-name*>
<ip-address *ip-address*>
<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 MX Series routers.

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 88
- clear dhcp-security binding on page 82
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 25
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection on MX Series Routers*
- Understanding Port Security on page 3

List of Sample Output

show dhcp-security binding on page 86
show dhcp-security binding interface on page 86
show dhcp-security binding ip-address on page 86
show dhcp-security binding vlan on page 87

Output Fields

Table 6 on page 85 lists the output fields for the **show dhcp-security binding** command. Output fields are listed in the approximate order in which they appear.

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

Table 6: show dhcp-security binding Output Fields *(continued)*

Field Name	Field Description	Level of Output
Expires	The time, in seconds, remaining before the lease of the IP address to the MAC address expires.	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
30.1.1.10         00:10:00:20:00:01   vlan20   0       STATIC  ge-0/0/4.0

30.1.1.18         00:10:94:00:00:34   vlan20   86287   BOUND   ge-0/0/6.0

30.1.1.15         00:10:94:00:00:55   vlan20   86265   BOUND   ge-0/0/4.0

30.1.1.16         00:10:94:00:00:56   vlan20   86265   BOUND   ge-0/0/4.0

30.1.1.19         00:10:94:00:00:5b   vlan20   86287   BOUND   ge-0/0/6.0

30.1.1.20         00:10:94:00:00:5c   vlan20   86287   BOUND   ge-0/0/6.0

30.1.1.21         00:10:94:00:00:5d   vlan20   86287   BOUND   ge-0/0/6.0

30.1.1.17         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
30.1.1.18         00:10:94:00:00:34   vlan20   86282   BOUND   ge-0/0/6.0

30.1.1.19         00:10:94:00:00:5b   vlan20   86282   BOUND   ge-0/0/6.0

30.1.1.20         00:10:94:00:00:5c   vlan20   86282   BOUND   ge-0/0/6.0

30.1.1.21         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
30.1.1.18  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
30.1.1.18  00:10:94:00:00:34   vlan20       86282       BOUND       ge-0/0/6.0
```

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 MX Series routers

Description Display IP source guard database table.

Required Privilege Level view

Related Documentation

- show dhcp-security binding on page 85
- clear dhcp-security binding on page 82
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 25
- *Example: Configuring IP Source Guard and Dynamic ARP Inspection on MX Series Routers*
- Understanding Port Security on page 3

List of Sample Output show dhcp-security binding ip-source-guard on page 89

Output Fields Table 7 on page 88 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
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
30.1.1.10         00:10:00:20:00:01   vlan20   0       STATIC  ge-0/0/4.0

30.1.1.18         00:10:94:00:00:34   vlan20   86276   BOUND   ge-0/0/6.0

30.1.1.15         00:10:94:00:00:55   vlan20   86254   BOUND   ge-0/0/4.0

30.1.1.16         00:10:94:00:00:56   vlan20   86254   BOUND   ge-0/0/4.0

30.1.1.19         00:10:94:00:00:5b   vlan20   86276   BOUND   ge-0/0/6.0

30.1.1.20         00:10:94:00:00:5c   vlan20   86276   BOUND   ge-0/0/6.0

30.1.1.21         00:10:94:00:00:5d   vlan20   86276   BOUND   ge-0/0/6.0

30.1.1.17         00:10:94:00:00:68   vlan20   86254   BOUND   ge-0/0/4.0
```