Junos® OS for EX Series Ethernet Switches, Release 11.3: Port Security

Published: 2011-11-23
Revision 2

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

Junos® OS for EX Series Ethernet Switches, Release 11.3: Port Security

Revision History
November 2011—Revision 2
September 2011—Revision 1

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

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

Table of Contents

About This Topic Collection

How to Use This Guide

Complete documentation for the EX Series product family is provided on webpages at http://www.juniper.net/techpubs/en_US/release-independent/information-products/pathway-pages/ex-series/product/index.html. We have selected content from these webpages and created a number of EX Series guides that collect related topics into a book-like format so that the information is easy to print and easy to download to your local computer.

Software features for EX Series switches are listed by platform and by Junos OS release in a standalone document. See EX Series Switch Software Features Overview.

The release notes are at http://www.juniper.net/techpubs/en_US/junos11.3/information-products/topic-collections/release-notes/11.3/junos-release-notes-11.3.pdf.

List of EX Series Guides for Junos OS Release 11.3

Title	Description
Complete Hardware Guide for EX2200 Ethernet Switches	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX2200 Ethernet switches
Complete Hardware Guide for EX3200 Ethernet Switches	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3200 Ethernet switches
Complete Hardware Guide for EX3300 Ethernet Switches	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3300 Ethernet switches

Title	Description
Complete Hardware Guide for EX4200 Ethernet Switches	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX4200 Ethernet switches
Complete Hardware Guide for EX4500 Ethernet Switches	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX4500 Ethernet switches
Complete Hardware Guide for EX6210 Ethernet Switches	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX6210 Ethernet switches
Complete Hardware Guide for EX8208 Ethernet Switches	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8208 Ethernet switches
Complete Hardware Guide for EX8216 Ethernet Switches	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8216 Ethernet switches
Complete Hardware Guide for the XRE200 External Routing Engine	Component descriptions, site preparation, installation, replacement, and safety and compliance information for the XRE200 External Routing Engine
Complete Software Guide for Junos® OS for EX Series Ethernet Switches, Release 11.3	Software feature descriptions, configuration examples, and tasks for Junos OS for EX Series switches
Software Topic Collections	Software feature descriptions, configuration examples and tasks, and reference pages for configuration statements and operational commands (This information also appears in the *Complete Software Guide for Junos® OS for EX Series Ethernet Switches, Release 11.3*.)
Junos® OS for EX Series Ethernet Switches, Release 11.3: Access Control	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Configuration Management	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Class of Service	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Device Security	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Ethernet Switching	
Junos® OS for EX Series Ethernet Switches, Release 11.3: EX3300, EX4200, and EX4500 Virtual Chassis	
Junos® OS for EX Series Ethernet Switches, Release 11.3: EX8200 Virtual Chassis	

Title	Description
Junos® OS for EX Series Ethernet Switches, Release 11.3: Fibre Channel over Ethernet	
Junos® OS for EX Series Ethernet Switches, Release 11.3: High Availability	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Interfaces	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Layer 3 Protocols	
Junos® OS for EX Series Ethernet Switches, Release 11.3: MPLS	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Multicast	
Junos® OS for EX Series Switches, Release 11.3: Network Management and Monitoring	
Junos® OS for EX Series Switches, Release 11.3: Port Security	
Junos® OS for EX Series Switches, Release 11.3: Power over Ethernet	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Routing Policy and Packet Filtering	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Software Installation	
Junos® OS for EX Series Ethernet Switches, Release 11.3: Spanning-Tree Protocols	
Junos® OS for EX Series Ethernet Switches, Release 11.3: System Monitoring	
Junos® OS for EX Series Ethernet Switches, Release 11.3: System Services	
Junos® OS for EX Series Ethernet Switches, Release 11.3: System Setup	
Junos® OS for EX Series Ethernet Switches, Release 11.3: User and Access Management	
Junos® OS for EX Series Ethernet Switches, Release 11.3: User Interfaces	

Downloading Software

You can download Junos OS for EX Series switches from the Download Software area at http://www.juniper.net/customers/support/ . To download the software, you must

have a Juniper Networks user account. For information about obtaining an account, see http://www.juniper.net/entitlement/setupAccountInfo.do.

Documentation Symbols Key

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.

Text and Syntax Conventions		
Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration 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*
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; 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**.

Text and Syntax Conventions		
Convention	Description	Examples
< > (angle brackets)	Enclose 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)	Enclose a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identify 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.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web 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. Send e-mail to techpubs-comments@juniper.net with the following:

- Document URL or title
- Page number if applicable
- Software version
- Your name and company

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: https://www.juniper.net/alerts/
- 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

Port Security

CHAPTER 1

Port Security Overview

Port Security for EX Series Switches Overview

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

Juniper Networks Junos operating system (Junos OS) on Juniper Networks EX Series Ethernet Switches provides features to help secure ports on the switch. The ports can be categorized as either trusted or untrusted. You apply policies appropriate to those categories to protect against various types of attacks.

Port security features can be turned on to obtain the most robust port security level. Basic port security features are enabled in the switch's default configuration. You can configure additional features with minimal configuration steps.

Depending on the particular feature, you can configure the port security feature either on:

- A specific VLAN or all VLANs
- A specific interface or all interfaces

NOTE: If you configure one of the port security features on all VLANs or all interfaces, the switch software enables that port security feature on all VLANs and all interfaces that are not explicitly configured with other port security features.

However, if you do explicitly configure one of the port security features on a specific VLAN or on a specific interface, you must explicitly configure any additional port security features that you want to apply to that VLAN or interface. Otherwise, the switch software automatically applies the default values for the feature.

For example, if you enable DHCP snooping on all VLANs and decide to explicitly enable IP source guard only on a specific VLAN, you must also explicitly enable DHCP snooping on that specific VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

Port security features on EX Series switches are:

- DHCP snooping—Filters and blocks ingress DHCP server messages on untrusted ports; builds and maintains an IP-address/MAC-address binding database (called the DHCP snooping database). You enable this feature on VLANs.
- Dynamic ARP inspection (DAI)—Prevents ARP spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. You enable this feature on VLANs.
- MAC limiting—Protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You enable this feature on access interfaces (ports).
- MAC move limiting—Detects MAC movement and MAC spoofing on access ports. You enable this feature on VLANs.
- Trusted DHCP server—With a DHCP server on a trusted port, protects against rogue DHCP servers sending leases. You enable this feature on interfaces (ports). By default, access ports are untrusted and trunk ports are trusted. (Access ports are the switch ports that connect to Ethernet endpoints such as user PCs and laptops, servers, and printers. Trunk ports are the switch ports that connect to other Ethernet switches or to routers.)
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. You enable this feature on VLANs. 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 allowed for further processing if the source IP address to source MAC address binding is valid; if the binding is not valid, the packet is discarded.
- DHCP option 82—Also known as the DHCP relay agent information option. Helps protect the EX Series switch against attacks such as spoofing 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.

Related Documentation

- Security Features for EX Series Switches Overview
- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8
- Understanding DAI for Port Security on EX Series Switches on page 15
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 17
- Understanding IP Source Guard for Port Security on EX Series Switches on page 23
- Understanding DHCP Option 82 for Port Security on EX Series Switches on page 20
- Understanding How to Protect Access Ports on EX Series Switches from Common Attacks on page 5

Understanding How to Protect Access Ports on EX Series Switches from Common Attacks

Port security features can protect the Juniper Networks EX Series Ethernet Switch against various types of attacks. Protection methods against some common attacks are:

- Mitigation of Ethernet Switching Table Overflow Attacks on page 5
- Mitigation of Rogue DHCP Server Attacks on page 6
- Protection Against ARP Spoofing Attacks on page 6
- Protection Against DHCP Snooping Database Alteration Attacks on page 7
- Protection Against DHCP Starvation Attacks on page 7

Mitigation of Ethernet Switching Table Overflow Attacks

In an overflow attack on the Ethernet switching table, an intruder sends so many requests from new MAC addresses that the table cannot learn all the addresses. When the switch can no longer use information in the table to forward traffic, it is forced to broadcast messages. Traffic flow on the switch is disrupted, and packets are sent to all hosts on the network. In addition to overloading the network with traffic, the attacker might also be able to sniff that broadcast traffic.

To mitigate such attacks, configure both a MAC limit for learned MAC addresses and some specific allowed MAC addresses. Use the MAC limit feature to control the total number of MAC addresses that can be added to the Ethernet switching table for the specified interface or interfaces. By setting the MAC addresses that are explicitly allowed, you ensure that the addresses of network devices whose network access is critical are guaranteed to be included in the Ethernet switching table. See "Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks" on page 34.

Mitigation of Rogue DHCP Server Attacks

If an attacker sets up a rogue DHCP server to impersonate a legitimate DHCP server on the LAN, the rogue server can start issuing leases to the network's DHCP clients. The information provided to the clients by this rogue server can disrupt their network access, causing DoS. The rogue server might also assign itself as the default gateway device for the network. The attacker can then sniff the network traffic and perpetrate a man-in-the-middle attack—that is, it misdirects traffic intended for a legitimate network device to a device of its choice.

To mitigate a rogue DHCP server attack, set the interface to which that rogue server is connected as untrusted. That action will block all ingress DHCP server messages from that interface. See "Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks" on page 38.

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

5 untrusted DHCPOFFER received, interface ge-0/0/0.0[65], vlan v1[10] server ip/mac 12.12.12.1/00:00:00:00:01:12 offer ip/client mac 12.12.12.253/00:AA:BB:CC:DD:01

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

Protection Against ARP Spoofing Attacks

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

To protect against ARP spoofing on your switch, enable both DHCP snooping and dynamic ARP inspection (DAI). DHCP snooping builds and maintains the DHCP snooping table. That table contains the MAC addresses, IP addresses, lease times, binding types, VLAN information, and interface information for the untrusted interfaces on the switch. DAI uses the information in the DHCP snooping table to validate ARP packets. Invalid ARP packets are blocked and, when they are blocked, a system log message is recorded that includes the type of ARP packet and the sender's IP address and MAC address.

See "Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks" on page 44.

Protection Against DHCP Snooping Database Alteration Attacks

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

To protect against this type of alteration of the DHCP snooping database, configure MAC addresses that are explicitly allowed on the interface. See "Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks" on page 48.

Protection Against DHCP Starvation Attacks

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

To protect the switch from DHCP starvation attacks, use the MAC limiting feature. Specify the maximum number of MAC addresses that the switch can learn on the access interfaces to which those clients connect. The switch's DHCP server or servers will then be able to supply the specified number of IP addresses and leases to those clients and no more. If a DHCP starvation attack occurs after the maximum number of IP addresses has been assigned, the attack will fail. See "Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks" on page 41.

Related Documentation

- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8
- Understanding DAI for Port Security on EX Series Switches on page 15
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 17
- Understanding Trusted DHCP Servers for Port Security on EX Series Switches on page 19
- Configuring Port Security (CLI Procedure) on page 88
- Configuring Port Security (J-Web Procedure) on page 90

Understanding DHCP Snooping for Port Security on EX Series Switches

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

DHCP Snooping Basics

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

DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server (the server is connected to a trusted network port). By default, all trunk ports on the switch are trusted and all access ports are untrusted for DHCP snooping. You can modify these defaults on each of the switch's interfaces.

When DHCP snooping is enabled, the lease information from the switch (which is a DHCP client) is used to create the DHCP snooping database, a mapping of IP address to VLAN–MAC-address pairs. For each VLAN–MAC-address pair, the database stores the corresponding IP address.

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 has to acquire a new IP address, so its entry in the database, including the VLAN ID, is updated.
- When the lease time (timeout value) assigned by the DHCP server expires, the associated entry is deleted from the database.

TIP: By default, the IP-MAC bindings are lost when the switch is rebooted and DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the

dhcp-snooping-file statement to store the database file either locally or remotely.

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

You configure DHCP snooping per VLAN, not per interface (port). By default, DHCP snooping is disabled for all VLANs. You can enable DHCP snooping on all VLANs or on specific VLANs.

NOTE: If you configure DHCP for all VLANs and you enable a different port security feature on a specific VLAN, you must also explicitly enable DHCP on that VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

TIP: For private VLANs (PVLANs), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from PVLAN trunk ports are not snooped.

DHCP Snooping Process

The basic process of DHCP snooping entails the following steps:

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

NOTE: DHCPDISCOVER and DHCPOFFER packets are not snooped. The DHCP database is updated only after the DHCPREQEST 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

Switch access to the DHCP server can be configured in three ways:

- Switch, DHCP Clients, and DHCP Server Are All on the Same VLAN on page 10
- Switch Acts as DHCP Server on page 11
- Switch Acts as Relay Agent on page 12

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

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

- The server is directly connected to the same switch as the one connected to the DHCP clients (the hosts, or network devices, that are requesting IP addresses from the server). You must configure the port that connects the server to the switch as a trusted port. See Figure 1 on page 11.
- The server is directly connected to a switch that is itself directly connected through a trunk port to the switch that the DHCP clients are connected to. The trunk port is configured by default as a trusted port. The switch that the DHCP server is connected to is not configured for DHCP snooping. See Figure 2 on page 11—in the figure, **ge-0/0/11** is a trusted trunk port.

Figure 1: DHCP Server Connected Directly to Switch

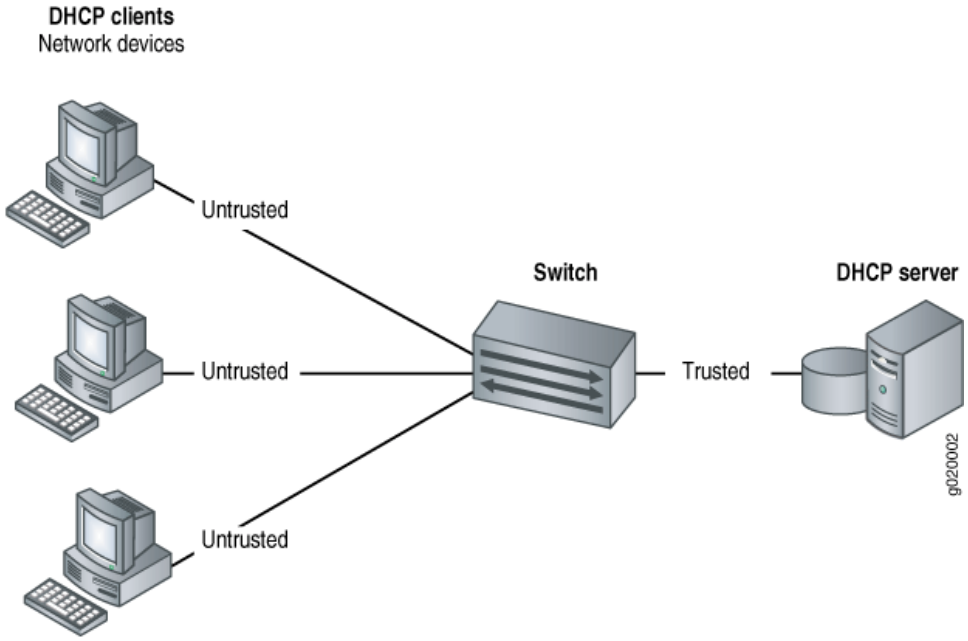
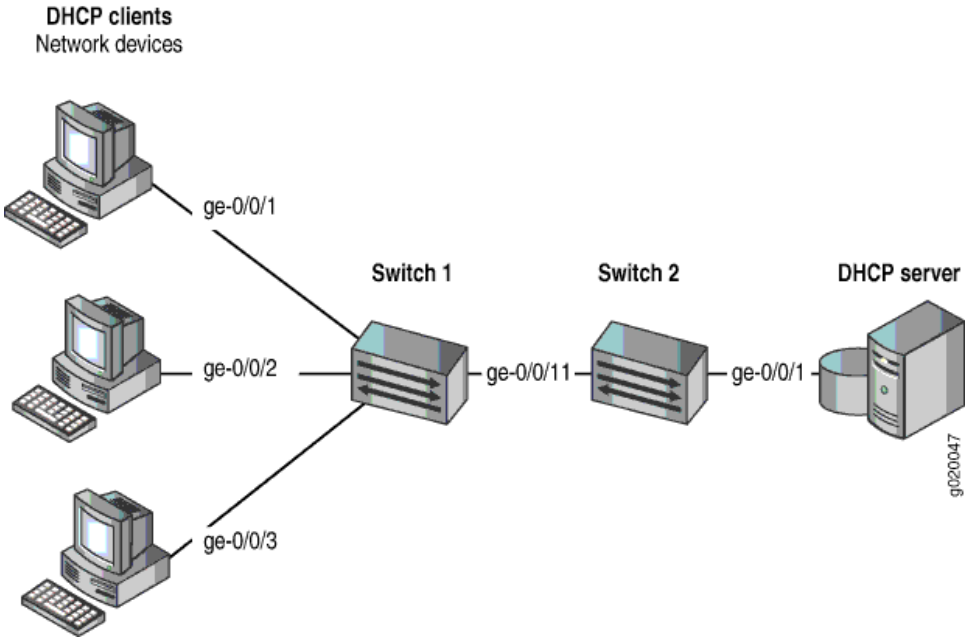


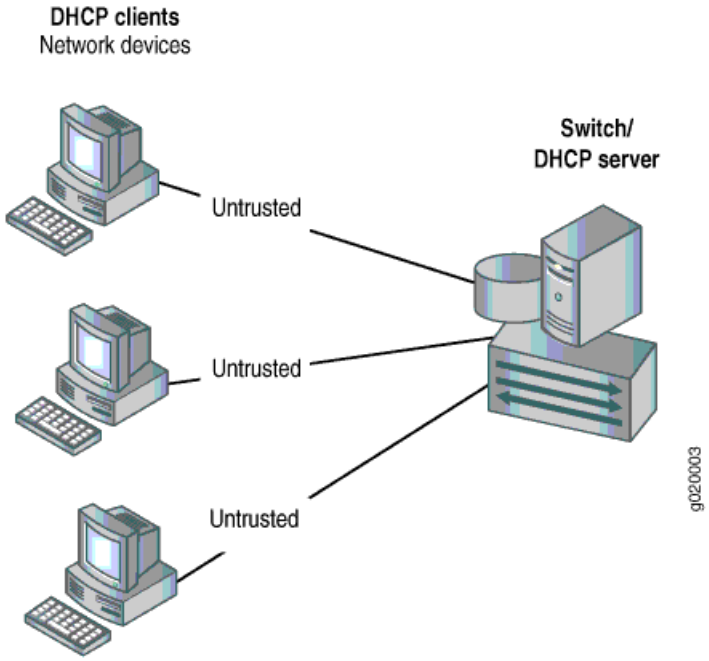
Figure 2: DHCP Server Connected Directly to Switch 2, with Switch 2 Connected to Switch 1 Through a Trusted Trunk Port



Switch Acts as DHCP Server

The switch itself is configured as a DHCP server; this is known as a “local” configuration. See Figure 3 on page 12.

Figure 3: Switch Is the DHCP Server



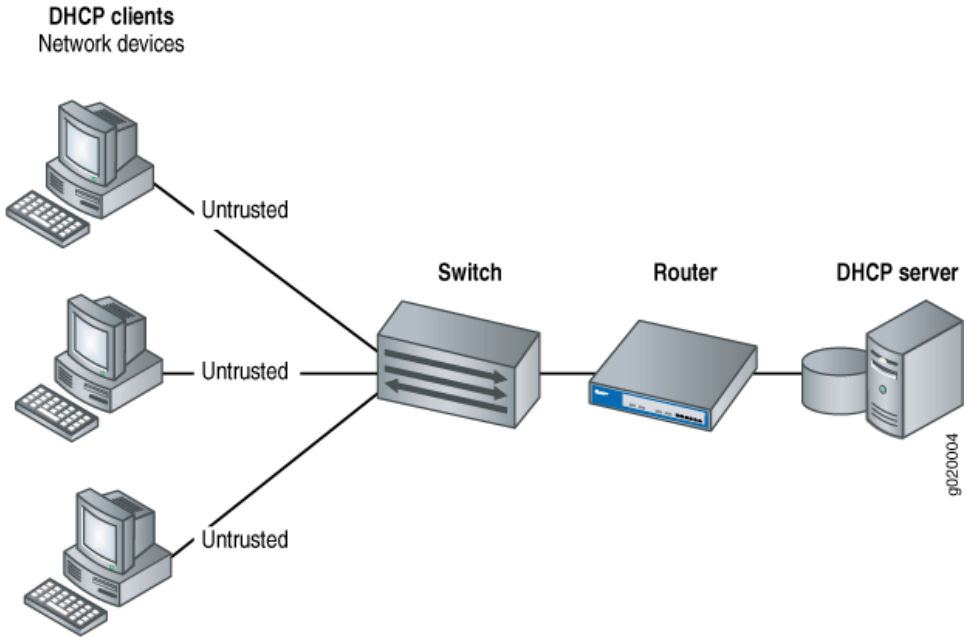
Switch Acts as Relay Agent

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

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

- The DHCP server and clients are in different VLANs.
- The switch is connected to a router that is in turn connected to the DHCP server. See Figure 4 on page 13.

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



DHCP Snooping Table

The software creates a DHCP snooping information table that displays the content of the DHCP snooping database. The table shows current IP-MAC bindings, as well as lease time, type of binding, names of associated VLANs, and associated interface. To view the table, type **show dhcp snooping binding** at the operational mode prompt:

```
user@switch> show dhcp snooping binding
DHCP Snooping Information:
MAC address        IP address   Lease (seconds)  Type     VLAN      Interface
00:05:85:3A:82:77  192.0.2.17   600              dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:79  192.0.2.18   653              dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:80  192.0.2.19   720              dynamic  employee  ge-0/0/2.0
```

Static IP Address Additions to the DHCP Snooping Database

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

Snooping DHCP Packets That Have Invalid IP Addresses

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

the switch drops the DCHP packets that request invalid IP addresses, preventing the snooping of these packets. The invalid IP addresses are:

- 0.0.0.0
- 128.0.x.x
- 191.255.x.x
- 192.0.0.x
- 223.255.255.x
- 224.x.x.x
- 240.x.x.x to 255.255.255.255

Prioritizing Snooped Packets

You can use 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, ensuring that the security procedure does not interfere with the transmittal of high-priority traffic.

Related Documentation

- Port Security for EX Series Switches Overview on page 3
- Understanding Trusted DHCP Servers for Port Security on EX Series Switches on page 19
- Understanding DHCP Option 82 for Port Security on EX Series Switches on page 20
- DHCP Services for EX Series Switches Overview
- DHCP/BOOTP Relay for EX Series Switches Overview
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 81
- Enabling DHCP Snooping (CLI Procedure) on page 92 and Enabling DHCP Snooping (J-Web Procedure) on page 94
- Troubleshooting Port Security on page 131

Understanding DAI for Port Security on EX Series Switches

Dynamic ARP inspection (DAI) protects Juniper Networks EX Series Ethernet 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. 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 to entries in the database. If the MAC address or IP address in an ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped.

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

Address Resolution Protocol

Sending IP packets on a multiaccess network requires mapping an IP address to an Ethernet media access control (MAC) address.

Ethernet LANs use Address Resolution Protocol (ARP) to map MAC addresses to IP addresses.

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

ARP Spoofing

ARP spoofing (also known as ARP poisoning or ARP cache poisoning) is one way to initiate man-in-the-middle attacks. The attacker sends an ARP packet that spoofs the MAC address of another device on the LAN. Instead of the switch sending traffic to the proper network device, 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.

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, EX Series switches examine ARP responses through DAI.

DAI on EX Series Switches

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

Juniper Networks Junos operating system (Junos OS) for EX switches uses DAI for ARP packets received on access ports because these ports are untrusted by default. Trunk ports are trusted by default, so 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. You can set an interface to be trusted for ARP packets by setting **dhcp-trusted** on that port.

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

For DAI, all ARP packets are trapped to the Routing 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

You can use 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 desired egress queue, ensuring that the security procedure does not interfere with the transmittal of high-priority traffic.

Related Documentation

- Port Security for EX Series Switches Overview on page 3
- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44

Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches

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

MAC Limiting

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

- Maximum number of MAC addresses—You configure the maximum number of dynamic MAC addresses allowed per interface or per VLAN. When the limit is exceeded, incoming packets with new MAC addresses are treated as specified by the configuration. The incoming packets with new MAC addresses can be ignored, dropped, logged, or the interface can be shut down or temporarily disabled. Note that static MAC addresses do not count toward the limit you specify for dynamic MAC addresses.
- Allowed MAC—You configure specific "allowed" MAC addresses for the access interface. Any MAC address that is not in the list of configured addresses is not learned and the switch logs the message. Allowed MAC binds MAC addresses to a VLAN so that the address does not get registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.

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

MAC Move Limiting

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

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

Actions for MAC Limiting and MAC Move Limiting

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

- **drop**—Drop the packet and generate an alarm, an SNMP trap, or a system log entry. This is the default.
- **log**—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- **none**—Take no action.
- **shutdown**—Disable the interface and generate an alarm. If you have configured the switch with the port-error-disable statement, the disabled interface or VLAN recovers automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the **clear ethernet-switching port-error** command.

See descriptions of results of these various action settings in "Verifying That MAC Limiting Is Working Correctly" on page 123.

If you have set a MAC limit to apply to all interfaces on the switch, you can override that setting for a particular interface by specifying action **none**. See "Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure)" on page 108.

MAC Addresses That Exceed the MAC Limit or MAC Move Limit

If you have configured the **port-error-disable** statement, you can view which interfaces are temporarily disabled due to exceeding the MAC limit or MAC move limit in the output for the **show ethernet-switching interfaces** command.

The log messages that indicate the MAC limit or MAC move limit has been exceeded include the offending MAC addresses that have exceeded the limit. See "Troubleshooting Port Security" on page 131 for details.

Related Documentation

- Port Security for EX Series Switches Overview on page 3
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 34

- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 41
- Configuring MAC Limiting (CLI Procedure) on page 100
- Configuring MAC Limiting (J-Web Procedure) on page 103
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118
- **no-allowed-mac-log on page 154**

Understanding Trusted DHCP Servers for Port Security on EX Series Switches

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

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

Related Documentation

- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 38
- Enabling a Trusted DHCP Server (CLI Procedure) on page 95
- Enabling a Trusted DHCP Server (J-Web Procedure) on page 96

Understanding DHCP Option 82 for Port Security on EX Series Switches

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

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

This topic covers:

DHCP Option 82 Processing

If DHCP option 82 is enabled on the switch, then when a network device—a DHCP client—that is connected to the switch on an untrusted interface sends a DHCP request, the switch inserts information about the client's network location into the packet header of that request. The switch then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or another parameter for the client. See "Suboption Components of Option 82" on page 21 for details about option 82 information.

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

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

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

NOTE: To use the DHCP option 82 feature, you must ensure that the DHCP server is configured to accept option 82. If it is not configured to accept option 82, then when it receives requests containing option 82 information, it does not use the information in setting parameters and it does not echo the information in its response message. For detailed information about configuring DHCP services, see the *Junos OS System Basics Configuration Guide*. The configuration for DHCP service on the Juniper Networks EX Series Ethernet Switch includes the **dhcp** statement at the **[edit system services]** hierarchy level.

Suboption Components of Option 82

Option 82 as implemented on the EX Series switch comprises the suboptions circuit ID, remote ID, and vendor ID. These suboptions are fields in the packet header:

- circuit ID—Identifies the circuit (interface and/or VLAN) on the switch on which the request was received. The circuit ID contains the interface name and/or VLAN name, with the two elements separated by a colon—for example, **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 switch is used as the prefix; for example, **switch1:ge-0/0/10:vlan1**, where **switch1** is the hostname.

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

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

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

Configurations of the EX Series Switch That Support Option 82

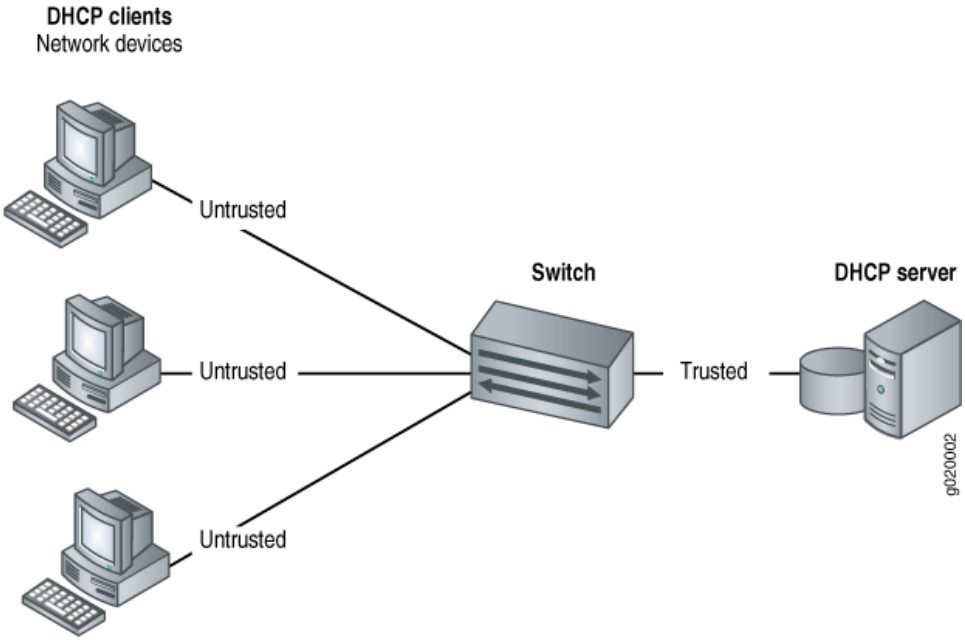
Configurations of the EX Series switch that support option 82 are:

- Switch and Clients Are on Same VLAN as DHCP Server on page 21
- Switch Acts as Relay Agent on page 22

Switch and Clients Are on Same VLAN as DHCP Server

If the DHCP clients, the switch, and the DHCP server are all on the same VLAN, the switch forwards the requests from the clients on untrusted access interfaces to the server on a trusted interface. See Figure 5 on page 22.

Figure 5: DHCP Clients, Switch, and DHCP Server Are All on Same VLAN

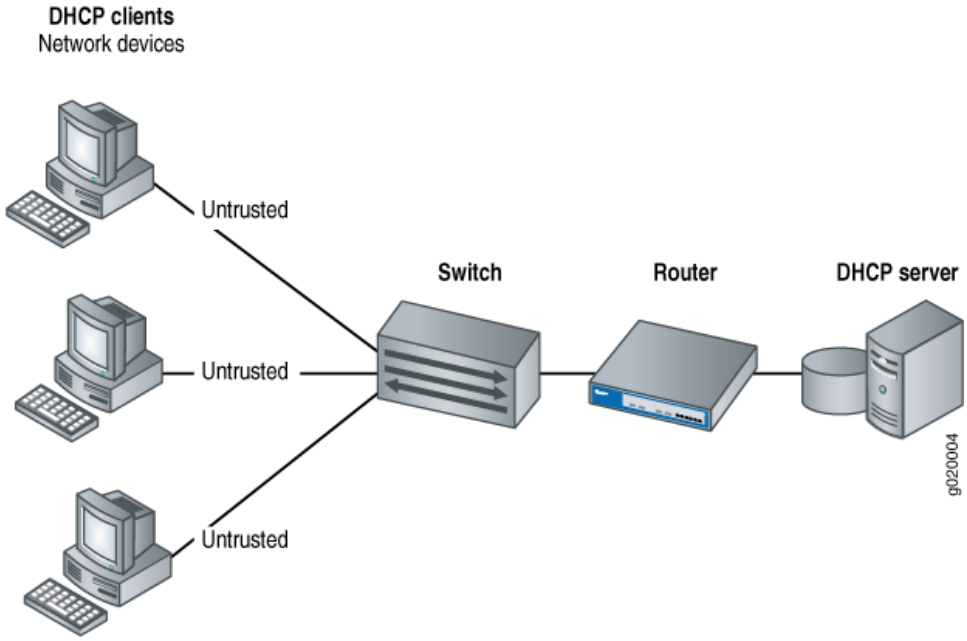


For the configuration shown in Figure 5 on page 22, you set DHCP option 82 at the **[edit ethernet-switching-options secure-access-port vlan]** hierarchy level.

Switch Acts as Relay Agent

The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as routed VLAN interfaces, or RVIs. Figure 6 on page 23 illustrates a scenario for the switch-as-relay-agent; in this instance, the switch relays requests through a router to the server.

Figure 6: Switch Relays DHCP Requests to Server



For the configuration shown in Figure 6 on page 23, you set DHCP option 82 at the **[edit forwarding-options helpers bootp]** hierarchy level.

Related Documentation

- Port Security for EX Series Switches Overview on page 3
- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112

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 24
- How IP Source Guard Works on page 24
- The IP Source Guard Database on page 24
- Typical Uses of Other Junos Operating System (Junos OS) Features with IP Source Guard on page 25

IP Address Spoofing

Hosts on access interfaces can spoof source IP addresses and/or 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.

When you configure IP source guard, you can enable it on a specific VLAN or on all VLANs. if you explicitly enable IP source guard only on a specific VLAN, you must also explicitly enable DHCP snooping on that specific VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

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—that is, interfaces configured as **dhcp-trusted** 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.**

IP source guard obtains information about IP-address/MAC-address/VLAN bindings from the DHCP snooping database. It causes the switch to validate incoming IP packets against the entries in that database.

After the DHCP snooping database has been populated either through dynamic DHCP snooping or through configuration of specific static IP address/MAC address bindings, the IP source guard feature builds its database. It then checks incoming packets from access interfaces on the VLANs on which it is enabled. If the source IP addresses and source MAC addresses match the IP source guard binding entries, the switch forwards the packets to their specified destination addresses. If there are no matches, the switch discards the packets.

The IP Source Guard Database

The IP source guard database looks like this:

```
user@switch> show ip-source-guard
```

```
IP source guard information:
Interface    Tag  IP Address   MAC Address        VLAN

ge-0/0/12.0  0    10.10.10.7   00:30:48:92:A5:9D  vlan100

ge-0/0/13.0  0    10.10.10.9   00:30:48:8D:01:3D  vlan100

ge–0/0/13.0  100  *            *                  voice
```

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.

If an untrusted access interface is associated with multiple VLANs and some of those VLANs are enabled for IP source guard and others are not, the VLANs that are not enabled for IP source guard have a star (*) in the **IP Address** and **MAC Address** fields. See the entry for the **voice** VLAN in the preceding sample output. If you are using IP source guard together with 802.1X user authentication, you must abide by additional configuration guidelines. See "Typical Uses of Other Junos Operating System (Junos OS) Features with IP Source Guard" on page 25.

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 (multiple EX4200 switches that are managed through a single management interface)
- 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.
- 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.

Related Documentation

- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8
- Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 67
- Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 59

CHAPTER 2

Examples: Port Security Configuration

Example: Configuring Basic Port Security Features on an EX Series Switch

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

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

Requirements

This example uses the following hardware and software components:

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

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

- Connected the DHCP server to the switch.
- Configured the VLAN **employee-vlan** on the switch. See Configuring VLANs for EX Series Switches (CLI Procedure).

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

Overview and Topology

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

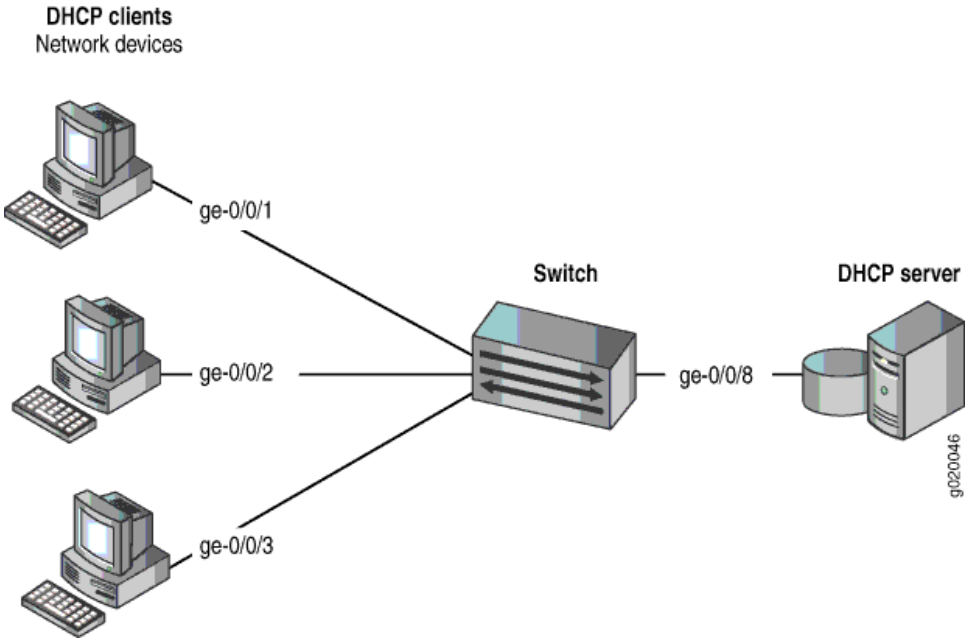
- DHCP snooping to validate DHCP server messages
- DAI to protect against MAC spoofing
- MAC limiting to constrain the number of MAC addresses the switch adds to its MAC address cache
- MAC move limiting to help prevent MAC spoofing
- Persistent MAC learning (sticky MAC) to constrain the MAC addresses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

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

The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic Configuring VLANs for EX Series Switches

(CLI Procedure). That procedure is not repeated here. Figure 7 on page 29 illustrates the topology for this example.

Figure 7: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 1 on page 29.

Table 1: Components of the Port Security Topology

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

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

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

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

Configuration

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

CLI Quick Configuration

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

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

Step-by-Step Procedure

Configure basic port security on the switch:

1. Enable DHCP snooping on the VLAN:

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

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

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

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

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

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

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

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

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

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

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

7. Configure allowed MAC addresses:

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

Results Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That DHCP Snooping Is Working Correctly on the Switch on page 31
- Verifying That DAI Is Working Correctly on the Switch on page 32
- Verifying That MAC Limiting, MAC Move Limiting, and Persistent MAC Learning Are Working Correctly on the Switch on page 32
- Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 33

Verifying That DHCP Snooping Is Working Correctly on the Switch

Purpose Verify that DHCP snooping is working on the switch.

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

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

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

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

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

Verifying That DAI Is Working Correctly on the Switch

Purpose Verify that DAI is working on the switch.

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

Display the DAI information:

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

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

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

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

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

Display the MAC addresses learned:

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

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

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

Display the MAC addresses in the table:

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

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

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

Meaning The first sample output shows that with a MAC limit of **4** for each interface, the fifth MAC address on **ge-0/0/2** was not learned because it exceeded the MAC limit. The second sample output shows that MAC addresses for three of the hosts on **ge-/0/0/2** were not learned, because the hosts had been moved back more than 5 times in one second.

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

Verifying That Allowed MAC Addresses Are Working Correctly on the Switch

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

Action Display the MAC cache information after 5 allowed MAC addresses have been configured on interface **ge-0/0/2**:

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

```
Ethernet-switching table:  5 entries, 4 learned
  VLAN                MAC address         Type         Age    Interfaces

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

Meaning Because the MAC limit value for this interface has been set to **4**, only 4 of the 5 configured allowed addresses are learned.

Related Documentation

- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 38
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 48
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 34
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 41
- Configuring Port Security (CLI Procedure) on page 88
- Configuring Port Security (J-Web Procedure) on page 90

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

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

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

- Requirements on page 35
- Overview and Topology on page 35
- Configuration on page 37
- Verification on page 37

Requirements

This example uses the following hardware and software components:

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

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

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

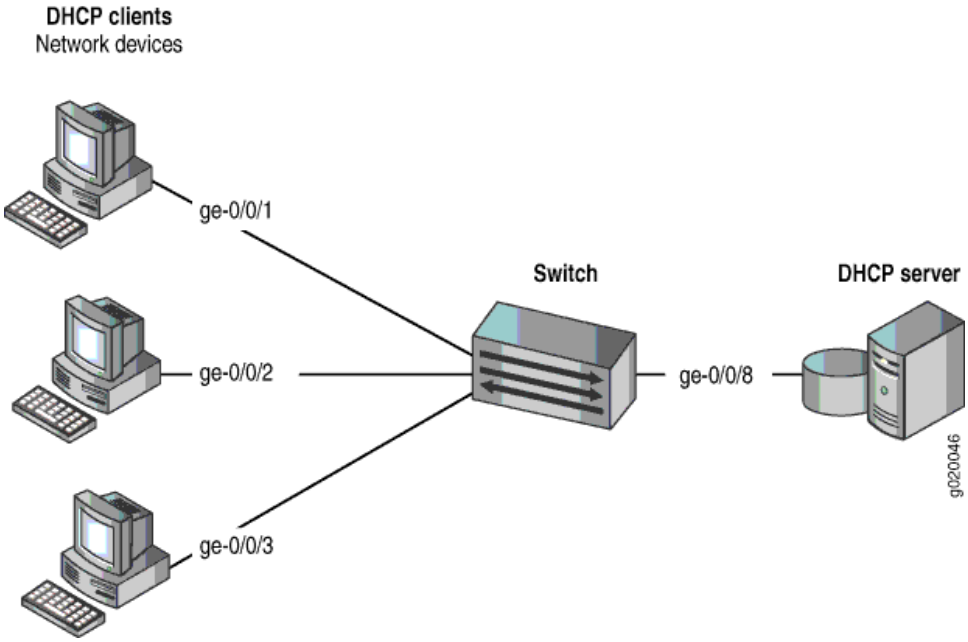
Overview and Topology

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

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

The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic Example: Setting Up Bridging with Multiple VLANs for EX Series Switches. That procedure is not repeated here. Figure 8 on page 36 illustrates the topology for this example.

Figure 8: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 2 on page 36.

Table 2: Components of the Port Security Topology

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

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

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

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

Configuration

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

CLI Quick Configuration

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

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

Step-by-Step Procedure

Configure MAC limiting and some allowed MAC addresses:

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

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

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

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

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

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

Results

Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That MAC Limiting Is Working Correctly on the Switch on page 38

Verifying That MAC Limiting Is Working Correctly on the Switch

Purpose Verify that MAC limiting is working on the switch.

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

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

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

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Configuring MAC Limiting (CLI Procedure) on page 100
- Configuring MAC Limiting (J-Web Procedure) on page 103

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

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

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

- Requirements on page 39
- Overview and Topology on page 39
- Configuration on page 40
- Verification on page 40

Requirements

This example uses the following hardware and software components:

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

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

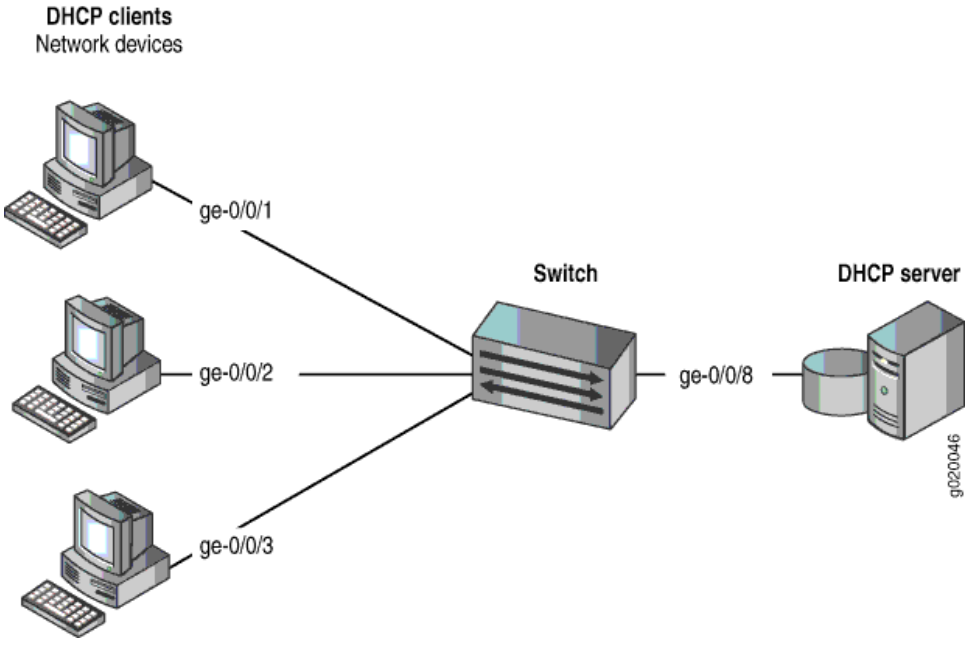
- Connected the DHCP server to the switch.
- Enabled DHCP snooping on the VLAN.
- Configured the VLAN **employee-vlan** on the switch. See Example: Setting Up Bridging with Multiple VLANs for EX Series Switches.

Overview and Topology

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

This example shows how to explicitly configure an untrusted interface on an EX3200-24P switch. Figure 9 on page 39 illustrates the topology for this example.

Figure 9: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 3 on page 40.

Table 3: Components of the Port Security Topology

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

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

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

Configuration

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

CLI Quick Configuration

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

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

Step-by-Step Procedure

To set the DHCP server interface as untrusted:

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

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

Results

Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That the DHCP Server Interface Is Untrusted on page 41

Verifying That the DHCP Server Interface Is Untrusted

Purpose Verify that the DHCP server is untrusted.

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

Display the DHCP snooping information when the port on which the DHCP server connects to the switch is not trusted.

```
user@switch> show dhcp snooping binding
```

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Enabling a Trusted DHCP Server (CLI Procedure) on page 95
- Enabling a Trusted DHCP Server (J-Web Procedure) on page 96

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

In a DHCP starvation attack, an attacker floods an Ethernet LAN with DHCP requests from spoofed (counterfeit) MAC addresses, causing the switch's overworked DHCP server to stop assigning IP addresses and lease times to legitimate DHCP clients on the switch (hence the name starvation). Requests from those clients are either dropped or directed to a rogue DHCP server set up by the attacker.

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

Requirements

This example uses the following hardware and software components:

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

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

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

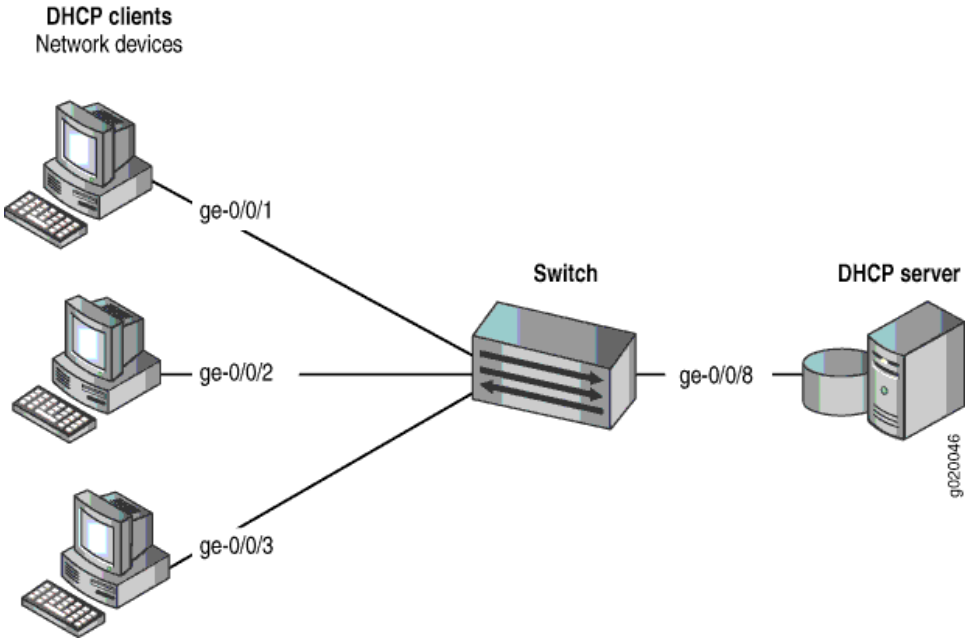
Overview and Topology

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

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

The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic Example: Setting Up Bridging with Multiple VLANs for EX Series Switches. That procedure is not repeated here. Figure 10 on page 42 illustrates the topology for this example.

Figure 10: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 4 on page 42.

Table 4: Components of the Port Security Topology

Properties	Settings
Switch hardware	
VLAN name and ID	**default**

Table 4: Components of the Port Security Topology *(continued)*

Properties	Settings
Interfaces in **employee-vlan**	**ge-0/0/1**, **ge-0/0/2**, **ge-0/0/3**, **ge-0/0/8**
Interface for DHCP server	**ge-0/0/8**

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

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

Configuration

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

CLI Quick Configuration

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

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

Step-by-Step Procedure

Configure MAC limiting:

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

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

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

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

Results

Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That MAC Limiting Is Working Correctly on the Switch on page 44

Verifying That MAC Limiting Is Working Correctly on the Switch

Purpose Verify that MAC limiting is working on the switch.

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

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

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

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

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

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Configuring MAC Limiting (CLI Procedure) on page 100
- Configuring MAC Limiting (J-Web Procedure) on page 103

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

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

NOTE: On EX Series switches, 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 describes how to configure DHCP snooping and dynamic ARP inspection (DAI), two port security features, to protect the switch against ARP spoofing attacks:

Requirements

This example uses the following hardware and software components:

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

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

- Connected the DHCP server to the switch.
- Configured the VLAN **employee-vlan** on the switch.

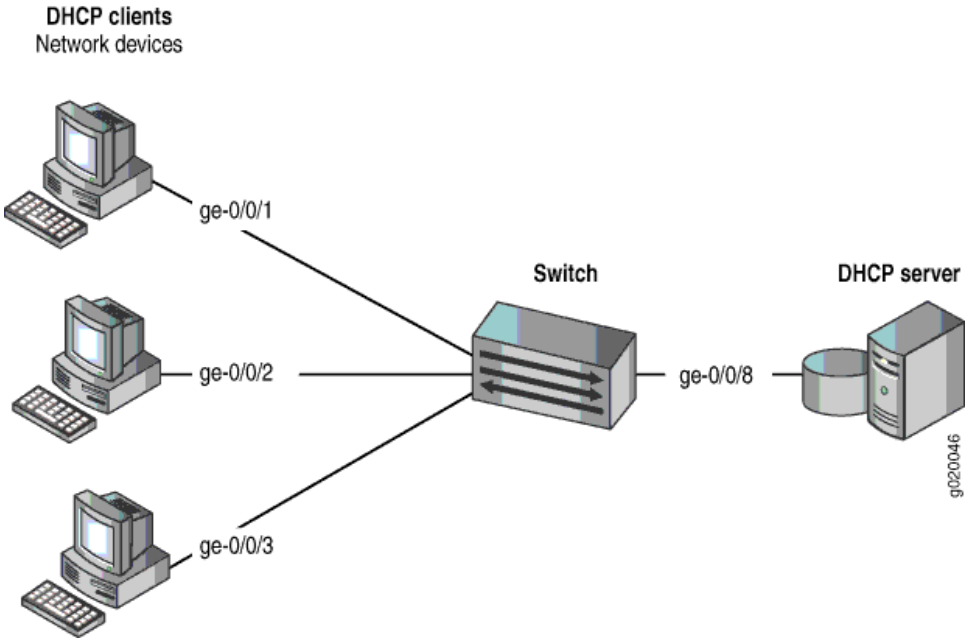
Overview and Topology

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

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

This example shows how to configure port security features on an EX3200-24P switch that is connected to a DHCP server. The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic Example: Setting Up Bridging with Multiple VLANs for EX Series Switches. That procedure is not repeated here. Figure 11 on page 46 illustrates the topology for this example.

Figure 11: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 5 on page 46.

Table 5: Components of the Port Security Topology

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

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

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

Configuration

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

CLI Quick Configuration

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

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

Step-by-Step Procedure

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

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

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

2. Enable DHCP snooping on the VLAN:

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

3. Enable DAI on the VLAN:

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

Results

Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That DHCP Snooping Is Working Correctly on the Switch on page 47
- Verifying That DAI Is Working Correctly on the Switch on page 48

Verifying That DHCP Snooping Is Working Correctly on the Switch

Purpose

Verify that DHCP snooping is working on the switch.

Action

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

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

```
user@switch> show dhcp snooping binding
```

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

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

Verifying That DAI Is Working Correctly on the Switch

Purpose Verify that DAI is working on the switch.

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

Display the DAI information:

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

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Enabling DHCP Snooping (CLI Procedure) on page 92
- Enabling DHCP Snooping (J-Web Procedure) on page 94
- Enabling Dynamic ARP Inspection (CLI Procedure) on page 96
- Enabling Dynamic ARP Inspection (J-Web Procedure) on page 98

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

In one type of attack on the DHCP snooping database, an intruder introduces a DHCP client on an untrusted access interface with a MAC address identical to that of a client on another untrusted interface. The intruder then acquires the DHCP lease of that other

client, thus changing the entries in the DHCP snooping table. Subsequently, what would have been valid ARP requests from the legitimate client are blocked.

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

Requirements

This example uses the following hardware and software components:

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

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

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

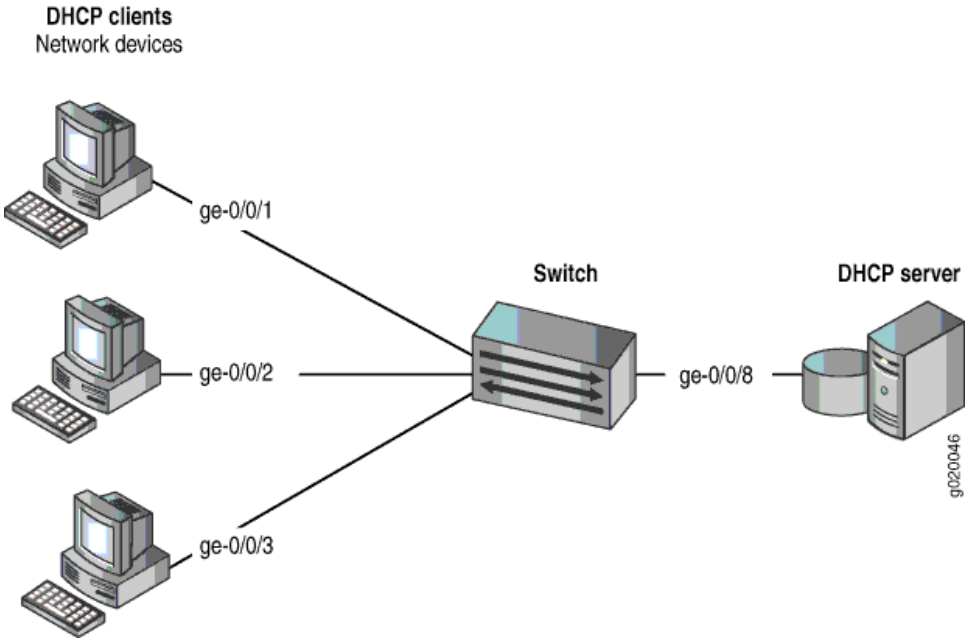
Overview and Topology

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

This example shows how to configure port security features on an EX3200-24P switch that is connected to a DHCP server.

The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic Example: Setting Up Bridging with Multiple VLANs for EX Series Switches. That procedure is not repeated here. Figure 12 on page 50 illustrates the topology for this example.

Figure 12: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 6 on page 50.

Table 6: Components of the Port Security Topology

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

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

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

Configuration

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

CLI Quick Configuration

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

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

Step-by-Step Procedure

To configure some allowed MAC addresses on an interface:

Configure the five allowed MAC addresses on an interface:

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

Results

Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 51

Verifying That Allowed MAC Addresses Are Working Correctly on the Switch

Purpose

Verify that allowed MAC addresses are working on the switch.

Action

Display the MAC cache information:

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

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

Meaning

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Configuring MAC Limiting (CLI Procedure) on page 100
- Configuring MAC Limiting (J-Web Procedure) on page 103

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

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

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

Requirements

This example uses the following hardware and software components:

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

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

- Connected the DHCP server to Switch 2.
- Configured the VLAN **employee-vlan** on the switch. See Example: Setting Up Bridging with Multiple VLANs for EX Series Switches.

Overview and Topology

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

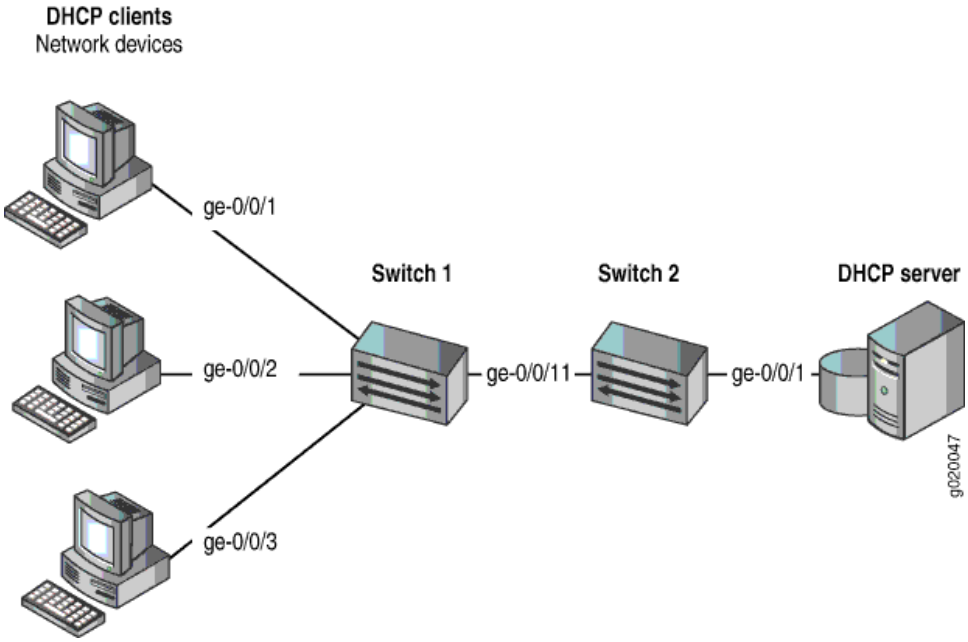
- DHCP snooping to validate DHCP server messages
- DAI to protect against ARP spoofing
- MAC limiting to constrain the number of MAC addresses the switch adds to its MAC address cache

This example shows how to configure these port security features on Switch 1. Switch 1 is connected to another switch (Switch 2) that is not configured with port security features. That second switch is connected to a DHCP server. (See Figure 13 on page 53.) Network devices (hosts) that are connected to Switch 1 will send requests for IP addresses (that is, the devices will be DHCP clients). Those requests will be transmitted from Switch 1 to Switch 2 and then to the DHCP server connected to Switch 2. Responses to the requests will be transmitted along the reverse path of the one followed by the requests.

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

Figure 13 on page 53 shows the network topology for the example.

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



The components of the topology for this example are shown in Table 7 on page 54.

Table 7: Components of Port Security Setup on Switch 1 with a DHCP Server Connected to Switch 2

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

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

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

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

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

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

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

CLI Quick Configuration

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

```
[edit]
set ethernet-switching-options secure-access-port interface ge-0/0/1 mac–limit 5
clear ethernet-switching table interface ge-0/0/1
set ethernet-switching-options secure-access-port vlan employee-vlan arp–inspection
set ethernet-switching-options secure-access-port vlan employee-vlan examine–dhcp
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members 20
```

```
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members 20
set vlans employee–vlan vlan-id 20
```

Step-by-Step Procedure

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

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

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

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

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

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

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

4. Enable DHCP snooping on the VLAN:

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

5. Enable DAI on the VLAN:

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

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

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

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

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

Results

Display the results of the configuration:

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

```
interfaces {
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members 20;
                }
            }
        }
    }
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members 20;
                }
            }
        }
    }
    ge-0/0/3 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members 20;
                }
            }
        }
    }
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members 20;
                }
            }
        }
    }
}
vlans {
    employee-vlan {
        vlan-id 20;
    }
}
```

Configuring a VLAN and Interfaces on Switch 2

To configure the VLAN and interfaces on Switch 2:

CLI Quick Configuration

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

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

Step-by-Step Procedure

To configure the VLAN and interfaces on Switch 2:

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

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

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

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

Results

Display the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That DHCP Snooping Is Working Correctly on Switch 1 on page 57
- Verifying That DAI Is Working Correctly on Switch 1 on page 58
- Verifying That MAC Limiting Is Working Correctly on Switch 1 on page 58

Verifying That DHCP Snooping Is Working Correctly on Switch 1

Purpose

Verify that DHCP snooping is working on Switch 1.

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

Display the DHCP snooping information when the interface through which Switch 2 sends the DHCP server replies to clients connected to Switch 1 is trusted. The server has provided the IP addresses and leases:

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

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

Verifying That DAI Is Working Correctly on Switch 1

Purpose Verify that DAI is working on Switch 1.

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

Display the DAI information:

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

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

Verifying That MAC Limiting Is Working Correctly on Switch 1

Purpose Verify that MAC limiting is working on Switch 1.

Action Display the MAC addresses that are learned when DHCP requests are sent from hosts on **ge-0/0/1**:

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

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

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

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Configuring Port Security (CLI Procedure) on page 88
- Configuring Port Security (J-Web Procedure) on page 90

Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces

Ethernet LAN switches are vulnerable to attacks that involve spoofing (forging) of source IP addresses or source MAC addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. You can enable the IP source guard port security feature on EX Series switches to mitigate the effects of such attacks. If IP source guard determines that a source IP address and a source MAC address in a binding in an incoming packet are not valid, the switch does not forward the packet.

You can use IP source guard in combination with other EX Series switch features to mitigate address-spoofing attacks on untrusted access interfaces. This example shows two configuration scenarios:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.2 or later for EX Series switches
- An EX4200-24P switch

- A DHCP server to provide IP addresses to network devices on the switch
- A RADIUS server to provide 802.1X authentication

Before you configure IP source guard for these scenarios, be sure you have:

- Connected the DHCP server to the switch.
- Connected the RADIUS server and configured user authentication on the RADIUS server. See Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch.
- Configured the VLANs on the switch. See Example: Setting Up Bridging with Multiple VLANs for EX Series Switches for detailed information about configuring VLANs.

Overview and Topology

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. 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.

When you configure IP source guard, you enable on it on one or more VLANs. IP source guard applies its checking rules to 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 trusted access interfaces—that is, interfaces configured with **dhcp-trusted** so that a DHCP server can be connected to that interface to provide dynamic IP addresses.

IP source guard obtains information about IP-address/MAC-address/VLAN bindings from the DHCP snooping database. It causes the switch to validate incoming IP packets against the entries in that database.

The topology for this example includes an EX-4200-24P switch, a connection to a DHCP server, and a connection to a RADIUS server for user authentication.

NOTE: The 802.1X user authentication applied in this example is for single supplicants.

You can also use IP source guard with 802.1X user authentication for single-secure supplicant or multiple supplicant mode. If you are implementing IP source guard with 802.1X authentication in single-secure supplicant or multiple supplicant mode, you must 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.
- 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.

In the first example configuration, two clients (network devices) are connected to an access switch. You configure IP source guard and 802.1X user authentication, in combination with two access port security features: DHCP snooping and dynamic ARP inspection (DAI). This setup is designed to protect the switch from IP attacks such as “ping of death” attacks, DHCP starvation, and ARP spoofing.

In the second example configuration, the switch is configured for 802.1X user authentication. If the client fails authentication, the switch redirects the client to a guest VLAN that allows this client to access a set of restricted network features. You configure IP source guard on the guest VLAN to mitigate effects of source IP spoofing.

NOTE: Control-plane rate limiting is achieved by restricting CPU control-plane protection. It can be used in conjunction with storm control (see Understanding Storm Control on EX Series Switches) to limit data-plane activity.

TIP: You can set the ip-source-guard flag in the traceoptions statement for debugging purposes.

Configuring IP Source Guard with 802.1X Authentication, DHCP Snooping, and Dynamic ARP Inspection

CLI Quick Configuration

To quickly configure IP source guard with 802.1X authentication and with other access port security features, copy the following commands and paste them into the switch terminal window:

```
[edit]
set ethernet-switching-options secure-access-port interface ge-0/0/24 dhcp-trusted
```

```
set ethernet-switching-options secure-access-port vlan data examine-dhcp
set ethernet-switching-options secure-access-port vlan data arp-inspection
set ethernet-switching-options secure-access-port vlan data ip-source-guard
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members data
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members data
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members data
set protocols lldp-med interface ge-0/0/0.0
set protocols dot1x authenticator authentication-profile-name profile52
set protocols dot1x authenticator interface ge-0/0/0.0 supplicant single
set protocols lldp-med interface ge-0/0/1.0
set protocols dot1x authenticator interface ge-0/0/1.0 supplicant single
```

Step-by-Step Procedure

To configure IP source guard with 802.1X authentication and various port security features:

1. Configure the interface on which the DHCP server is connected to the switch as a trusted interface and add that interface to the data VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/24 dhcp-trusted
user@switch# set set ge-0/0/24 unit 0 family ethernet-switching vlan members data
```

2. Associate two interfaces with the data VLAN:

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

3. Configure 802.1X user authentication and LLDP-MED on the two interfaces that you associated with the data VLAN:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/0.0
user@switch# set dot1x authenticator authentication-profile-name profile52
user@switch# set dot1x authenticator interface ge-0/0/0.0 supplicant single
user@switch# set lldp-med interface ge-0/0/1.0
user@switch# set dot1x authenticator interface ge-0/0/1.0 supplicant single
```

4. Configure three access port security features—DHCP snooping, dynamic ARP inspection (DAI), and IP source guard—on the data VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port vlan data examine-dhcp
user@switch# set secure-access-port vlan data arp-inspection
user@switch# set secure-access-port vlan data ip-source-guard
```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options]
secure-access-port {
    interface ge-0/0/24.0 {
        dhcp-trusted;
    }
    vlan data {
        arp-inspection;
        examine-dhcp;
        ip-source-guard;
    }
}
```

```
[edit interfaces]
ge-0/0/0 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members data;
            }
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members data;
            }
        }
    }
}
ge-0/0/24 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members data;
            }
        }
    }
}
```

```
[edit protocols]
lldp-med {
    interface ge-0/0/14.0;
    interface ge-0/0/0.0;
    interface ge-0/0/1.0;
}
dot1x {
    authenticator {
        authentication-profile-name profile52;
    }
    interface {
        ge-0/0/0.0 {
            supplicant single;
        }
        ge-0/0/1.0 {
            supplicant single;
        }
        ge-0/0/14.0 {
            supplicant single;
        }
    }
}
```

Configuring IP Source Guard on a Guest VLAN

CLI Quick Configuration To quickly configure IP source guard on a guest VLAN, copy the following commands and paste them into the switch terminal window:

```
[edit]
set ethernet-switching-options secure-access-port interface ge-0/0/24 dhcp-trusted
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members employee
set ethernet-switching-options secure-access-port vlan employee examine-dhcp
set ethernet-switching-options secure-access-port vlan employee ip-source-guard
set ethernet-switching-options secure-access-port interface ge-0/0/0 static-ip 11.1.1.1 mac
00:11:11:11:11:11 vlan employee
set ethernet-switching-options secure-access-port interface ge-0/0/1 static-ip 11.1.1.2 mac
00:22:22:22:22:22 vlan employee
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/1 unit 0 family ethernet-switching port-mode access
set protocols dot1x authenticator authentication-profile-name profile52
set protocols dot1x authenticator interface ge-0/0/0 supplicant single
set protocols dot1x authenticator interface ge-0/0/0 guest-vlan employee
set protocols dot1x authenticator interface ge-0/0/0 supplicant-timeout 2
set protocols dot1x authenticator interface ge-0/0/1 supplicant single
set protocols dot1x authenticator interface ge-0/0/1 guest-vlan employee
set protocols dot1x authenticator interface ge-0/0/1 supplicant-timeout 2
set vlans employee vlan-id 300
```

Step-by-Step Procedure

To configure IP source guard on a guest VLAN:

1. Configure the interface on which the DHCP server is connected to the switch as a trusted interface and add that interface to the **employee** VLAN:

   ```
   [edit ethernet-switching-options]
   user@switch# set secure-access-port interface ge-0/0/24 dhcp-trusted
   user@switch# set ge-0/0/24 unit 0 family ethernet-switching vlan members employee
   ```

2. Configure two interfaces for the access port mode:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/0 unit 0 family ethernet-switching port-mode access
   user@switch# set ge-0/0/1 unit 0 family ethernet-switching port-mode access
   ```

3. Configure DHCP snooping and IP source guard on the **employee** VLAN:

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

4. Configure a static IP address on each of two interfaces on the **employee** VLAN (optional):

   ```
   [edit ethernet-switching-options]
   user@switch# set secure-access-port interface ge-0/0/0 static-ip 11.1.1.1 mac
   00:11:11:11:11:11 vlan employee


   [edit ethernet-switching-options]
   user@switch# set secure-access-port interface ge-0/0/1 static-ip 11.1.1.2 mac
   00:22:22:22:22:22 vlan employee
   ```

5. Configure 802.1X user authentication:

   ```
   [edit protocols]
   user@switch# set dot1x authenticator authentication-profile-name profile52
   user@switch# set dot1x authenticator interface ge-0/0/0 supplicant single
   user@switch# set dot1x authenticator interface ge-0/0/1 supplicant single
   user@switch# set dot1x authenticator interface ge-0/0/0 supplicant-timeout 2
   user@switch# set dot1x authenticator interface ge-0/0/1 supplicant-timeout 2
   ```

6. Set the VLAN ID for the **employee** VLAN:

```
[edit vlans]
user@switch# set employee vlan-id 100
```

Results Check the results of the configuration:

```
[edit protocols]
  dot1x {
    authenticator {
      authentication-profile-name profile52;
    }
    interface {
      ge-0/0/0.0 {
        guest-vlan employee;
        supplicant single;
        supplicant-timeout 2;
      }
      ge-0/0/1.0 {
        guest-vlan employee;
        supplicant single;
        supplicant-timeout 2;
      }
    }
  }
}

[edit vlans]
employee {
  vlan-id 100;
}

[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
    }
  }
}
ge-0/0/24 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members employee;
      }
    }
  }
}
```

```
[edit ethernet-switching-options]
secure-access-port {
   interface ge-0/0/0.0 {
      static-ip 11.1.1.1 vlan employee mac 00:11:11:11:11:11;
   }
   interface ge-0/0/1.0 {
      static-ip 11.1.1.2 vlan employee mac 00:22:22:22:22:22;
   }
   interface ge-0/0/24.0 {
      dhcp-trusted;
   }
   vlan employee {
      examine-dhcp;
      ip-source-guard;
   }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That 802.1X User Authentication Is Working on the Interface on page 66
- Verifying the VLAN Association with the Interface on page 66
- Verifying That DHCP Snooping and IP Source Guard Are Working on the VLAN on page 66

Verifying That 802.1X User Authentication Is Working on the Interface

Purpose Verify that the 802.1X configuration is working on the interface.

Action Use the **show dot1x interface** command to view the 802.1X details.

Meaning The **Supplicant mode** output field displays the configured administrative mode for each interface.

Verifying the VLAN Association with the Interface

Purpose Verity interface states and VLAN memberships.

Action Use the show ethernet-switching interfaces command to view the Ethernet switching table entries.

Meaning The field **VLAN members** shows the associations between VLANs and interfaces. The **State** field shows whether the interfaces are up or down.

For the guest VLAN configuration, the interface is associated with the guest VLAN if and when the supplicant fails 802.1X user authentication.

Verifying That DHCP Snooping and IP Source Guard Are Working on the VLAN

Purpose Verify that DHCP snooping and IP source guard are enabled and working on the VLAN.

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

Use the **show dhcp snooping binding** command to display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. View the MAC addresses from which requests were sent and the IP addresses and leases provided by the server.

Use the **show ip-source-guard** command to view IP source guard information for the VLAN.

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires. Static IP addresses have no assigned lease time. Statically configured entries never expire.

The IP source guard database table contains the VLANs enabled for IP source guard, the untrusted access interfaces on those VLANs, the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another. If a switch interface is associated with multiple VLANs and some of those VLANs are enabled for IP source guard and others are not, the VLANs that are not enabled for IP source guard have a star (*) in the **IP Address** and **MAC Address** fields.

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch
- Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 67
- Configuring IP Source Guard (CLI Procedure) on page 109

Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN

Ethernet LAN switches are vulnerable to attacks that involve spoofing (forging) of source IP addresses or source MAC addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. You can enable the IP source guard port security feature on EX Series switches to mitigate the effects of such attacks. If IP source guard determines that a source IP address and a source MAC address in a binding in an incoming packet are not valid, the switch does not forward the packet.

If two VLANs share an interface, you can configure IP source guard on just one of the VLANs; in this example, you configure IP source guard on an untagged data VLAN but not on the tagged voice VLAN. You can use 802.1X user authentication to validate the device connections on the data VLAN.

This example describes how to configure IP source guard with 802.1X user authentication on a data VLAN, with a voice VLAN on the same interface:

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 9.2 or later for EX Series switches
- A DHCP server to provide IP addresses to network devices on the switch
- A RADIUS server to provide 802.1X authentication

Before you configure IP source guard for the data VLANs, be sure you have:

- Connected the DHCP server to the switch.
- Connected the RADIUS server to the switch and configured user authentication on the server. See Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch.
- Configured the VLANs. See Example: Setting Up Bridging with Multiple VLANs for EX Series Switches for detailed information about configuring VLANs.

Overview and Topology

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. 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.

When you configure IP source guard, you enable on it on one or more VLANs. IP source guard applies its checking rules to 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 trusted access interfaces—that is, interfaces configured with **dhcp-trusted** so that a DHCP server can be connected to that interface to provide dynamic IP addresses.

IP source guard obtains information about IP-address/MAC-address/VLAN bindings from the DHCP snooping database. It causes the switch to validate incoming IP packets against the entries in that database.

The topology for this example includes one EX-3200-24P switch, a PC and an IP phone connected on the same interface, a connection to a DHCP server, and a connection to a RADIUS server for user authentication.

NOTE: The 802.1X user authentication applied in this example is for single supplicants.

You can also use IP source guard with 802.1X user authentication for single-secure supplicant or multiple supplicant mode. If you are implementing IP source guard with 802.1X authentication in single-secure supplicant or multiple supplicant mode, you must 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.
- 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.

TIP: You can set the **ip-source-guard** flag in the **traceoptions** statement for debugging purposes.

This example shows how to configure a static IP address to be added to the DHCP snooping database.

Configuration

CLI Quick Configuration

To quickly configure IP source guard on a data VLAN, copy the following commands and paste them into the switch terminal window:

```
set ethernet-switching-options voip interface ge-0/0/14.0 vlan voice
set ethernet-switching-options secure-access-port interface ge-0/0/24.0 dhcp-trusted
set ethernet-switching-options secure-access-port interface ge-0/0/14 static-ip 11.1.1.1 mac
00:11:11:11:11:11 vlan data
set ethernet-switching-options secure-access-port vlan data examine-dhcp
set ethernet-switching-options secure-access-port vlan data ip-source-guard
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members data
set vlans voice vlan-id 100
set protocols lldp-med interface ge-0/0/14.0
set protocols dot1x authenticator authentication-profile-name profile52
set protocols dot1x authenticator interface ge-0/0/14.0 supplicant single
```

Step-by-Step Procedure

To configure IP source guard on the data VLAN:

1. Configure the VoIP interface:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/14.0 vlan voice
```

2. Configure the interface on which the DHCP server is connected to the switch as a trusted interface and add that interface to the data VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/24.0 dhcp-trusted
[edit interfaces]
user@switch# set ge-0/0/24 unit 0 family ethernet-switching vlan members data
```

3. Configure a static IP address on an interface on the data VLAN (optional)

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/14 static-ip 11.1.1.1 mac
00:11:11:11:11:11 vlan data
```

4. Configure DHCP snooping and IP source guard on the data VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port vlan data examine-dhcp
user@switch# set secure-access-port vlan data ip-source-guard
```

5. Configure 802.1X user authentication and LLDP-MED on the interface that is shared by the data VLAN and the voice VLAN:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/14.0
user@switch# set dot1x authenticator authentication-profile-name profile52
user@switch# set dot1x authenticator interface ge-0/0/14.0 supplicant single
```

6. Set the VLAN ID for the voice VLAN:

```
[edit vlans]
user@switch# set voice vlan-id 100
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options]
user@switch# show
voip {
    interface ge-0/0/14.0 {
        vlan voice;
    }
}
secure-access-port {
    interface ge-0/0/14.0 {
        static-ip 11.1.1.1 vlan data mac 00:11:11:11:11:11;
    }
    interface ge-0/0/24.0 {
        dhcp-trusted;
    }
    vlan data {
        examine-dhcp;
        ip-source-guard;
    }
}
```

```
[edit interfaces]
ge-0/0/24 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members data;
```

```
        }
      }
    }
}

[edit vlans]
voice {
   vlan-id 100;
}

[edit protocols]
lldp-med {
   interface ge-0/0/14.0;
}
dot1x {
   authenticator {
      authentication-profile-name profile52;
      interface {
         ge-0/0/14.0 {
            supplicant single;
         }
      }
   }
}
```

TIP: If you wanted to configure IP source guard on the voice VLAN as well as on the data VLAN, you would configure DHCP snooping and IP source guard exactly as you did for the data VLAN. The configuration result for the voice VLAN under **secure-access-port** would look like this:

```
secure-access-port {
   vlan voice {
      examine-dhcp;
      ip-source-guard;
   }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That 802.1X User Authentication Is Working on the Interface on page 71
- Verifying the VLAN Association with the Interface on page 72
- Verifying That DHCP Snooping and IP Source Guard Are Working on the Data VLAN on page 73

Verifying That 802.1X User Authentication Is Working on the Interface

Purpose Verify the 802.1X configuration on interface **ge-0/0/14**.

Action Verify the 802.1X configuration with the operational mode command **show dot1x interface**:

```
user@switch> show dot1x interface ge-0/0/14.0 detail
ge-0/0/14.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: <not configured>
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The **Supplicant mode** output field displays the configured administrative mode for each interface. Interface **ge-0/0/14.0** displays **Single** supplicant mode.

Verifying the VLAN Association with the Interface

Purpose Display the interface state and VLAN membership.

Action

```
user@switch> show ethernet-switching interfaces
 Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members         Blocking
ge-0/0/0.0  down     default              unblocked
ge-0/0/1.0  down     employee             unblocked
ge-0/0/2.0  down     employee             unblocked
ge-0/0/12.0 down     default              unblocked
ge-0/0/13.0 down     default              unblocked
ge-0/0/13.0 down     vlan100              unblocked
ge-0/0/14.0 up       voice                unblocked
                     data                 unblocked
ge-0/0/17.0 down     employee             unblocked
ge-0/0/23.0 down     default              unblocked
ge-0/0/24.0 down     data                 unblocked
                     employee             unblocked
                     vlan100              unblocked
                     voice                unblocked
```

Meaning The field **VLAN members** shows that the **ge-0/0/14.0** interface supports both the **data** VLAN and the **voice** VLAN. The **State** field shows that the interface is up.

Verifying That DHCP Snooping and IP Source Guard Are Working on the Data VLAN

Purpose Verify that DHCP snooping and IP source guard are enabled and working on the data VLAN.

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

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

```
user@switch>  show dhcp snooping binding
DHCP Snooping Information:
MAC address        IP address  Lease (seconds) Type     VLAN      Interface

00:05:85:3A:82:77  192.0.2.17  600             dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:79  192.0.2.18  653             dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:80  192.0.2.19  720             dynamic  employee  ge-0/0/2.0
00:05:85:3A:82:81  192.0.2.20  932             dynamic  employee  ge-0/0/2.0

                         00:30:48:92:A5:9D  10.10.10.7  720             dynamic
vlan100   ge-0/0/13.0
00:30:48:8D:01:3D  10.10.10.9  720             dynamic  data      ge-0/0/14.0
00:30:48:8D:01:5D  10.10.10.8  1230            dynamic  voice     ge-0/0/14.0
00:11:11:11:11:11  11.1.1.1    –               static   data      ge-0/0/14.0
00:05:85:27:32:88  192.0.2.22  –               static   employee  ge-0/0/17.0
00:05:85:27:32:89  192.0.2.23  –               static   employee  ge-0/0/17.0
00:05:85:27:32:90  192.0.2.27  –               static   employee  ge-0/0/17.0
```

View the IP source guard information for the data VLAN.

```
user@switch>  show ip-source-guard
IP source guard information:
Interface    Tag  IP Address   MAC Address        VLAN

ge-0/0/13.0  0    10.10.10.7   00:30:48:92:A5:9D  vlan100

ge-0/0/14.0  0    10.10.10.9   00:30:48:8D:01:3D  data
ge-0/0/14.0  0    11.1.1.1     00:11:11:11:11:11  data

ge-0/0/13.0  100  *            *                  voice
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see the preceding sample output for **show dhcp snooping binding**) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires. Static IP addresses have no assigned lease time. Statically configured entries never expire.

The IP source guard database table contains the VLANs enabled for IP source guard, the untrusted access interfaces on those VLANs, the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another. If a switch

interface is associated with multiple VLANs and some of those VLANs are enabled for IP source guard and others are not, the VLANs that are not enabled for IP source guard have a star (*) in the **IP Address** and **MAC Address** fields. See the entry for the **voice** VLAN in the preceding sample output.

Related Documentation

- Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 59
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch
- Configuring IP Source Guard (CLI Procedure) on page 109

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

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

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

Requirements

This example uses the following hardware and software components:

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

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

- Connected and configured the DHCP server.

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

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

Overview and Topology

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

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

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

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

Configuration

To configure DHCP option 82:

CLI Quick Configuration

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

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

Step-by-Step Procedure

To configure DHCP option 82:

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

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

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

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

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

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

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

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

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

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

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

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 remote-id use-string employee-switch1
   ```

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

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

Results

Check the results of the configuration:

```
[edit forwarding-options helpers bootp]
user@switch# show

  dhcp-option82 {
    circuit-id {
      prefix hostname;
```

```
        use-vlan-id;
      }
      remote-id {
        prefix mac;
        use-string employee-switch1;
      }
      vendor-id;
    }
```

Related Documentation

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server

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

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

Requirements

This example uses the following hardware and software components:

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

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

- Connected and configured the DHCP server.

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

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

Overview and Topology

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

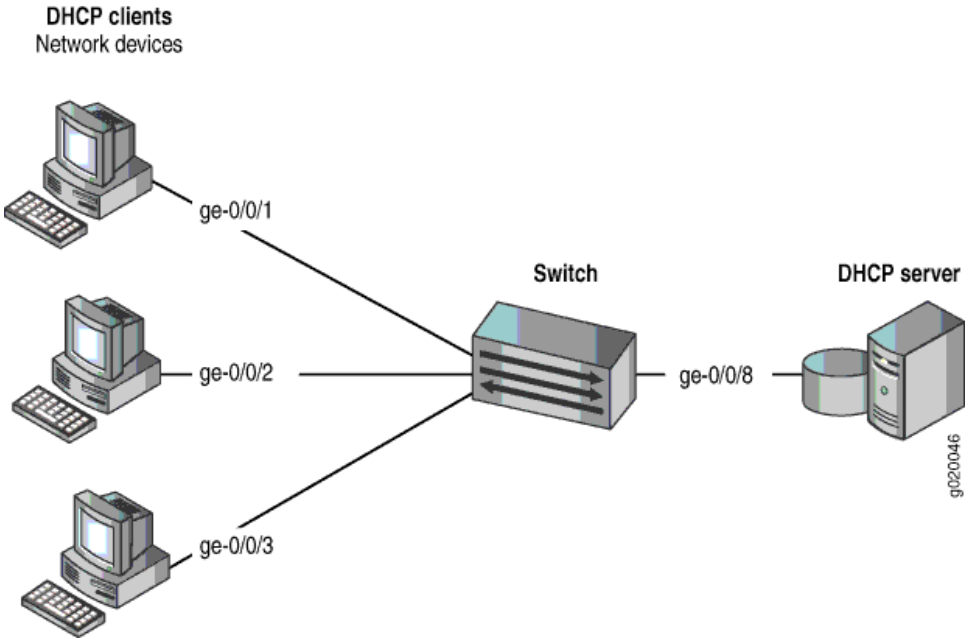
DHCP option 82 is enabled on an individual VLAN or on all VLANs on the switch.

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

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

Figure 14 on page 79 illustrates the topology for this example.

Figure 14: Network Topology for Configuring DHCP Option 82 on a Switch That Is on the Same VLAN as the DHCP Clients and the DHCP Server



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

Configuration

To configure DHCP option 82:

CLI Quick Configuration

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

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

Step-by-Step Procedure

To configure DHCP option 82:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show

  vlan employee {
    dhcp-option82 {
      circuit-id {
        prefix hostname;
        use-vlan-id;
      }
      remote-id {
        prefix mac;
        use-string employee-switch1;
      }
      vendor-id;
    }
  }
```

Related Documentation

- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic

On EX Series switches you might need to use class of service (CoS) to protect packets from critical applications from being dropped during periods of network congestion and delay and you might also need the port security features of DHCP snooping and dynamic ARP inspection (DAI) on the same ports through which those critical packets are entering and leaving. You can combine the advantages of both these features by using CoS forwarding classes and queues to prioritize snooped and inspected packets. This type of configuration places the snooped and inspected packets in the desired egress queue, ensuring that the security procedure does not interfere with the transmittal of this high-priority traffic. This is especially important for traffic that is sensitive to jitter and delay, such as voice traffic.

This example shows how to configure the switch to prioritize snooped and inspected packets in heavy network traffic.

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 11.2 or later for EX Series switches
- A DHCP server to provide IP addresses to network devices on the switch

Before you specify CoS forwarding classes for snooped and inspected packets, be sure you have:

- Connected the DHCP server to the switch.
- Configured the VLAN **VLAN200** on the switch. See Configuring VLANs for EX Series Switches (CLI Procedure).
- Configured two interfaces, **ge-0/0/1** and **ge-0/0/8**, to belong to **VLAN200**.

Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. To protect the devices from such attacks, you can configure DHCP snooping to validate DHCP server messages and DAI to protect against MAC spoofing. If you have to deal with periods of heavy network congestion and you want to ensure that sensitive traffic is not disrupted, you can combine the port security features with CoS forwarding classes to prioritize the handling of the snooped and inspected security packets.

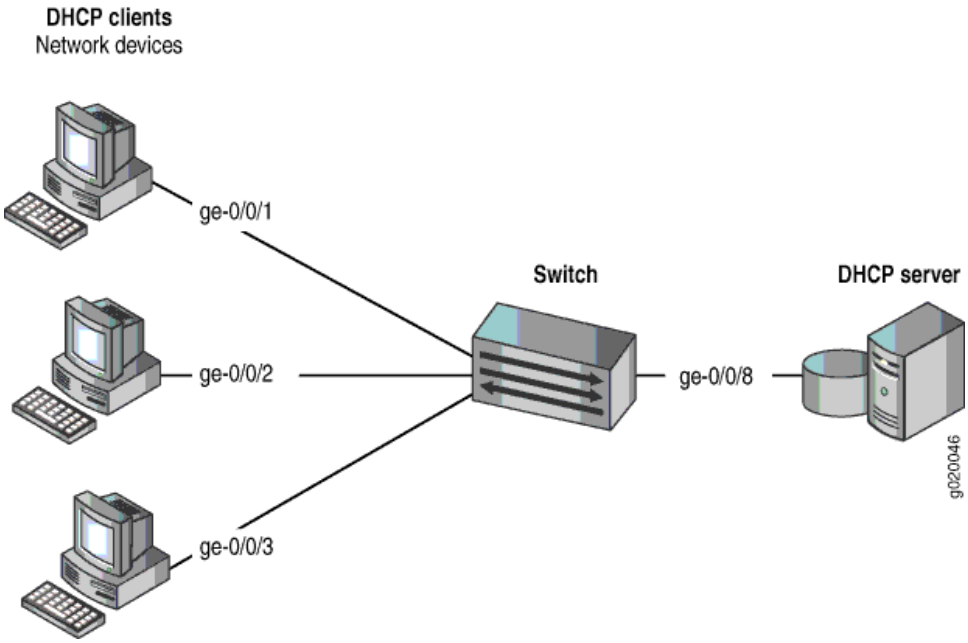
In the default switch configuration:

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

This example shows how to combine the DHCP snooping and DAI security features with prioritized forwarding of snooped and inspected packets.

The setup for this example includes the VLAN **VLAN200** on the switch. Figure 15 on page 82 illustrates the topology for this example.

Figure 15: Network Topology for Using CoS Forwarding Classes to Prioritize Snooped and Inspected Packets



The components of the topology for this example are shown in Table 1 on page 29.

Table 8: Components of the Topology for Using CoS Forwarding Classes to Prioritize Snooped and Inspected Packets

Properties	Settings
Switch hardware	EX Series switch
VLAN name	**VLAN200**
Interfaces in **VLAN200**	**ge-0/0/1**,**ge-0/0/2**,**ge-0/0/3**,**ge-0/0/8**
Interface for DHCP server	**ge-0/0/8**

In the configuration tasks for this example, you create a user-defined forwarding class **c1**, you enable DHCP snooping and DAI on VLAN200, and you assign the snooped and inspected packets to forwarding class **c1** and queue **6**. Queues 6 and 7 are reserved for high priority, control packets. The packets that are subjected to DHCP snooping and DAI are control (not data) packets; therefore, it is appropriate to place these snooped and inspected high-priority control packets in queue 6. (Queue 7 is higher priority than queue 6 and can also be used for this purpose.)

Configuration

To configure DHCP snooping and DAI on VLAN200, and to prioritize the snooped and inspected packets:

CLI Quick Configuration

To quickly configure DHCP snooping and DAI with prioritized forwarding of snooped and inspected packets, copy the following commands and paste them into the switch terminal window:

```
[edit]
set class-of-service forwarding-classes class c1 queue 6
set ethernet-switching-options security-access-port vlan VLAN200 examine-dhcp
forwarding-class c1
set ethernet-switching-options security-access-port vlan VLAN200 arp-inspection
forwarding-class c1
```

Step-by-Step Procedure

Configure DHCP and DAI with prioritized forwarding of snooped and inspected packets:

1. Create a user-defined forwarding class to be used for prioritizing the snooped and inspected packets.

   ```
   [edit class-of-service]
   user@switch# set forwarding-classes class c1 queue 6
   ```

2. Enable DHCP snooping on the VLAN and apply forwarding class **c1** to the snooped packets:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan VLAN200 examine-dhcp forwarding-class c1
   ```

3. Enable DAI on the VLAN and apply forwarding class **c1** to the inspected packets:

   ```
   [edit ethernet-switching-options secure-access-port]
   user@switch# set vlan VLAN200 arp-inspection forwarding-class c1
   ```

Results Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
vlan VLAN200 {
   arp-inspection forwarding-class c1;
   examine-dhcp forwarding-class c1;
}
[edit class-of-service]
user@switch# show
}
   forwarding-classes {
      class c1 queue-num 6;
   }
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That Prioritized Forwarding Is Working Correctly on the Snooped Packets on page 84
- Verifying That Prioritized Forwarding Is Working Correctly on the DAI Inspected Packets on page 84

Verifying That Prioritized Forwarding Is Working Correctly on the Snooped Packets

Purpose Verify that prioritized forwarding is working on the DHCP snooped packets.

Action Send some DHCP requests from network devices to the switch. Display the output queue for one of the interfaces in VLAN200 to make sure that the packets are being transmitted in the designated queue:

```
user@switch> show interfaces ge- 0/0/1 extensive
Egress queues: 8 supported, 5 in use
  Queue counters:       Queued packets  Transmitted packets   Dropped packets
    0 best-effort                    0                    0                 0
    1 assured-forw                   0                    0                 0
    5 expedited-fo                   0                    0                 0
    6 c1                             0                 3209                 0
    7 network-cont                   0               126371                 0
```

Meaning The command output shows that packets have been transmitted on forwarding class **c1** queue 6.

Continue testing by changing the setting of **examine-dhcp forwarding-class** to use one of the default queues, such as best-effort, and repeat the **show interfaces** command to compare the difference in the output. You can tell that the setting is working correctly by seeing the difference in the number of transmitted packets reported for forwarding class **c1** queue 6.

Verifying That Prioritized Forwarding Is Working Correctly on the DAI Inspected Packets

Purpose Verify that prioritized forwarding is working on the DAI inspected packets.

Action Send some ARP requests from network devices to the switch. Display the output queue for one of the interfaces in VLAN200 to make sure that the packets are being transmitted in the designated queue:

```
user@switch> show interfaces ge-0/0/1 extensive
Egress queues: 8 supported, 5 in use
  Queue counters:       Queued packets  Transmitted packets   Dropped packets
    0 best-effort                    0                    0                 0
    1 assured-forw                   0                    0                 0
    5 expedited-fo                   0                    0                 0
    6 c1                             0                 3209                 0
    7 network-cont                   0               126371                 0
```

Meaning The command output shows that packets have been transmitted on forwarding class **c1** queue 6.

Continue testing by changing the setting of **arp-inspection forwarding-class** to use one of the default queues, such as best-effort, and repeat the **show interfaces** command to compare the difference in the output. You can tell that the setting is working correctly by seeing the difference in the number of transmitted packets reported for forwarding class **c1** queue 6.

Related Documentation

- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44

CHAPTER 3

Configuring Port Security

Configuring Port Security (CLI Procedure)

Ethernet LANs are vulnerable to attacks such as address spoofing and Layer 2 denial of service (DoS) on network devices. Port security features such as DHCP snooping, DAI (dynamic ARP inspection), MAC limiting, and MAC move limiting, as well as trusted DHCP server, help protect the access ports on your EX Series switch against the losses of information and productivity that can result from such attacks.

Depending on the particular feature, you can configure the port security feature either on:

- A specific VLAN or all VLANs
- A specific interface or all interfaces

NOTE: If you configure one of the port security features on all VLANs or all interfaces, the switch software enables that port security feature on all VLANs and all interfaces that are not explicitly configured with other port security features.

However, if you do explicitly configure one of the port security features on a specific VLAN or on a specific interface, you must explicitly configure any additional port security features that you want to apply to that VLAN or interface. Otherwise, the switch software automatically applies the default values for the feature.

For example, if you enable DHCP snooping on all VLANs and decide to explicitly enable IP source guard only on a specific VLAN, you must also explicitly enable DHCP snooping on that specific VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

To configure port security features using the CLI:

1. Enable DHCP snooping:
   - On a specific VLAN:

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

   - On all VLANs:

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

2. Enable DAI:
   - On a single VLAN (here, the VLAN is **employee-vlan**):

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

- On all VLANs:

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

3. Limit the number of dynamic MAC addresses and specify the action to take if the limit is exceeded—for example, set a MAC limit of **5** with an action of **drop**:

   - On a single interface (here, the interface is **ge-0/0/1**):

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

   - On all interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all mac–limit 5 action drop
```

4. Specify allowed MAC addresses:

   - On a single interface (here, the interface is **ge-0/0/2**):

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

   - On all interfaces:

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

5. Limit the number of times a MAC address can move from its original interface in one second—for example, set a MAC move limit of **5** with an action of **drop** if the limit is exceeded:

   - On a single VLAN (here, the VLAN is **employee-vlan**):

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

   - On all VLANs:

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

6. Configure a trusted DHCP server on an interface (here, the interface is **ge-0/0/8**):

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

Related Documentation

- Configuring Port Security (J-Web Procedure) on page 90
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27

- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Monitoring Port Security on page 119
- Port Security for EX Series Switches Overview on page 3

Configuring Port Security (J-Web Procedure)

To configure port security on an EX Series switch using the J-Web interface:

1. Select **Configure** > **Security** > **Port Security**.

   The **VLAN List** table lists all the VLAN names, VLAN identifiers, port members, and port security VLAN features.

   The **Interface List** table lists all the ports and indicates whether security features have been enabled on the ports.

   NOTE: After you make changes to the configuration in this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one:

   - **Edit**—Click this option to modify the security features for the selected port or VLAN.

     Enter information as specified in Table 9 on page 90 to modify Port Security settings on VLANs.

     Enter information as specified in Table 10 on page 91 to modify Port Security settings on interfaces.

   - **Activate/Deactivate**—Click this option to enable or disable security on the switch.

Table 9: Port Security Settings on VLANs

Field	Function	Your Action
Enable DHCP Snooping on VLAN	Allows the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. Builds and maintains a database of valid IP addresses/MAC address bindings. (By default, access ports are untrusted and trunk ports are trusted.)	Select to enable DHCP snooping on a specified VLAN or all VLANs. TIP: For private VLANs (PVLANs), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from PVLAN trunk ports are not snooped.
Enable ARP Inspection on VLAN	Uses information in the DHCP snooping database to validate ARP packets on the LAN and protect against ARP cache poisoning.	Select to enable ARP inspection on a specified VLAN or all VLANs. (Configure any port on which you do not want ARP inspection to occur as a trusted DHCP server port.)

Table 9: Port Security Settings on VLANs *(continued)*

Field	Function	Your Action
MAC Movement	Specifies the number of times per second that a MAC address can move to a new interface.	Enter a number. The default is unlimited.
MAC Movement Action	Specifies the action to be taken if the MAC move limit is exceeded.	Select one: • **Log**—Generate a system log entry, an SNMP trap, or an alarm. • **Drop**—Drop the packets and generate a system log entry, an SNMP trap, or an alarm (default). • **Shutdown**—Shut down the VLAN and generate an alarm. You can mitigate the effect of this option by configuring autorecovery from the disabled state and specifying a **disable timeout** value. See "Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)" on page 118. • **None**—No action to be taken.

Table 10: Port Security on Interfaces

Field	Function	Your Action
Trust DHCP	Specifies trusting DHCP packets on the selected interface. By default, trunk ports are **dhcp-trusted**.	Select to enable DHCP trust.
MAC Limit	Specifies the number of MAC addresses that can be learned on a single Layer 2 access port. This option is not valid for trunk ports.	Enter a number.
MAC Limit Action	Specifies the action to be taken if the MAC limit is exceeded. This option is not valid for trunk ports.	Select one: • **Log**—Generate a system log entry, an SNMP trap, or an alarm. • **Drop**—Drop the packets and generate a system log entry, an SNMP trap, or an alarm. (Default) • **Shutdown**—Shut down the interface and generate an alarm. You can mitigate the effect of this option by configuring autorecovery from the disabled state and specifying a **disable timeout** value. See "Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)" on page 118 • **None**—No action to be taken.
Allowed MAC List	Specifies the MAC addresses that are allowed for the interface.	To add a MAC address: 1. Click **Add**. 2. Enter the MAC address. 3. Click **OK**.

Related Documentation

- Configuring Port Security (CLI Procedure) on page 88
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Monitoring Port Security on page 119
- Port Security for EX Series Switches Overview on page 3

Enabling DHCP Snooping (CLI Procedure)

DHCP snooping allows the switch to monitor and control DHCP messages received from untrusted devices connected to the EX Series switch. It builds and maintains a database of valid IP-address/MAC-address (IP-MAC) bindings called the DHCP snooping database.

NOTE: If you configure DHCP snooping for all VLANs and you enable a different port security feature on a specific VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

This topic describes:

- Enabling DHCP Snooping on page 93
- Applying CoS Forwarding Classes to Prioritize Snooped Packets on page 93

Enabling DHCP Snooping

You configure DHCP snooping per VLAN, not per interface (port). By default, DHCP snooping is disabled for all VLANs. You can enable DHCP snooping on all VLANs or on specific VLANs.

To enable DHCP snooping on a VLAN or all VLANs:

- On a specific VLAN:

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

- On all VLANs:

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

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

TIP: For private VLANs (PVLANs), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from PVLAN trunk ports are not snooped.

Applying CoS Forwarding Classes to Prioritize Snooped Packets

On EX Series switches you might need to use class of service (CoS) to protect packets from critical applications from being dropped during periods of network congestion and delay and you might also need the port security features of DHCP snooping on the same ports through which those critical packets are entering and leaving.

To apply CoS forwarding classes and queues to snooped packets:

1. Create a user-defined forwarding class to be used for prioritizing snooped packets:

```
[edit class-of-service]
user@switch# set forwarding-classes class class-name queue queue-number
```

2. Enable DHCP snooping on a specific VLAN or on all VLANs and apply the desired forwarding class on the snooped packets:

   - On a specific VLAN:

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

   - On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all examine-dhcp forwarding-class class-name
```

Related Documentation

- Enabling DHCP Snooping (J-Web Procedure) on page 94
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44
- Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 81
- Verifying That DHCP Snooping Is Working Correctly on page 120
- Monitoring Port Security on page 119
- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8

Enabling DHCP Snooping (J-Web Procedure)

DHCP snooping allows the EX Series switch to monitor and control DHCP messages received from untrusted devices connected to the switch. It builds and maintains a database of valid IP-address/MAC-address (IP-MAC) bindings called the DHCP snooping database.

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

To enable DHCP snooping on one or more VLANs by using the J-Web interface:

1. Select **Configure>Security>Port Security**.
2. Select one or more VLANs from the VLAN list.
3. Click the **Edit** button. If a message appears asking if you want to enable port security, click **Yes**.
4. Select the **Enable DHCP Snooping on VLAN** check box and then click **OK**.
5. Click **OK** after the command has been successfully delivered.

NOTE: You can enable or disable port security on the switch at any time by clicking the **Activate** or **Deactivate** button on the Port Security Configuration page. If security status is shown as **Disabled** when you try to edit settings for any VLANs or interfaces (ports), the message asking if you want to enable port security appears.

Related Documentation

- Enabling DHCP Snooping (CLI Procedure) on page 92
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44
- Verifying That DHCP Snooping Is Working Correctly on page 120
- Monitoring Port Security on page 119
- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8

Enabling a Trusted DHCP Server (CLI Procedure)

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

You configure a trusted DHCP server on an interface, not on a VLAN. By default, all access interfaces are untrusted and all trunk interfaces are trusted.

To configure a trusted interface for a DHCP server by using the CLI (here, the interface is **ge-0/0/8**):

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

Related Documentation

- Enabling a Trusted DHCP Server (J-Web Procedure) on page 96
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 38
- Verifying That a Trusted DHCP Server Is Working Correctly on page 121
- Monitoring Port Security on page 119
- Understanding Trusted DHCP Servers for Port Security on EX Series Switches on page 19

Enabling a Trusted DHCP Server (J-Web Procedure)

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

You configure a trusted DHCP server on an interface, not on a VLAN. By default, all access interfaces are untrusted and all trunk interfaces are trusted.

To enable a trusted DHCP server on one or more interfaces by using the J-Web interface:

1. Select **Configure>Security>Port Security**.
2. Select one or more interfaces from the Port list.
3. Click the **Edit** button. If a message appears asking if you want to enable port security, click **Yes**.
4. Select the **Trust DHCP** check box and then click **OK**.
5. Click **OK** after the command has been successfully delivered.

NOTE: You can enable or disable port security on the switch at any time by clicking the **Activate** or **Deactivate** button on the Port Security Configuration page. If security status is shown as **Disabled** when you try to edit settings for any VLANs or interfaces (ports), the message asking if you want to enable port security appears.

Related Documentation

- Enabling a Trusted DHCP Server (CLI Procedure) on page 95
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 38
- Verifying That a Trusted DHCP Server Is Working Correctly on page 121
- Monitoring Port Security on page 119
- Understanding Trusted DHCP Servers for Port Security on EX Series Switches on page 19

Enabling Dynamic ARP Inspection (CLI Procedure)

Dynamic ARP inspection (DAI) protects EX Series switches against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping

database on the switch to validate ARP packets and to protect against ARP cache poisoning.

This topic describes:

- Enabling DAI on page 97
- Applying CoS Forwarding Classes to Prioritize Inspected Packets on page 97

Enabling DAI

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

To enable DAI on a VLAN or all VLANs:

- On a single VLAN:

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

- On all VLANs:

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

Applying CoS Forwarding Classes to Prioritize Inspected Packets

On EX Series switches you might need to use class of service (CoS) to protect packets from critical applications from being dropped during periods of network congestion and delay and you might also need the port security features of DHCP snooping on the same ports through which those critical packets are entering and leaving.

To apply CoS forwarding classes and queues to DAI packets:

1. Create a user-defined forwarding class to be used for prioritizing DAI packets:

```
[edit class-of-service]
user@switch# set forwarding-classes class class-name queue queue-number
```

2. Enable DAI on a specific VLAN or on all VLANs and apply the desired forwarding class on the DAI packets:

   - On a specific VLAN:

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

   - On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all arp-inspection forwarding-class class-name
```

Related Documentation

- Enabling Dynamic ARP Inspection (J-Web Procedure) on page 98
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27

- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44
- Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 81
- Verifying That DAI Is Working Correctly on page 122
- Monitoring Port Security on page 119
- Understanding DAI for Port Security on EX Series Switches on page 15

Enabling Dynamic ARP Inspection (J-Web Procedure)

Dynamic ARP inspection (DAI) protects EX Series 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.

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

To enable DAI on one or more VLANs by using the J-Web interface:

1. Select **Configure>Security>Port Security**.
2. Select one or more VLANs from the VLAN list.
3. Click the **Edit** button. If a message appears asking if you want to enable port security, click **Yes**.
4. Select the **Enable ARP Inspection on VLAN** check box and then click **OK**.
5. Click **OK** after the command has been successfully delivered.

NOTE: You can enable or disable port security on the switch at any time by clicking the **Activate** or **Deactivate** button on the Port Security Configuration page. If security status is shown as **Disabled** when you try to edit settings for any VLANs or interfaces (ports), the message asking if you want to enable port security appears.

Related Documentation

- Enabling Dynamic ARP Inspection (CLI Procedure) on page 96
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44

- Verifying That DAI Is Working Correctly on page 122
- Monitoring Port Security on page 119
- Understanding DAI for Port Security on EX Series Switches on page 15

Configuring MAC Limiting (CLI Procedure)

MAC limiting restricts the MAC addresses that can be learned and added to the MAC address forwarding table. You can impose a limit on either a single Layer 2 access interface, on all the Layer 2 access interfaces on the switch, or on a specific VLAN. There are two ways you can limit the MAC addresses added to the MAC address forwarding table:

- Limit the number of MAC addresses added to the table—Configure the maximum number of dynamic MAC addresses that can be added to the MAC address forwarding table. This limit can be set either for the entire switch, for one interface, or for one VLAN. When this limit is exceeded, incoming packets with new MAC addresses are either dropped, logged, ignored, or the interface is shut down. Note that only learned MAC addresses, not static MAC addresses, count toward the limit you specify for dynamic MAC addresses.
- Allow only named MAC addresses to be added to the table—Configure specific "allowed" MAC addresses for an access interface. Any MAC address that is not in the list of configured addresses is not learned and the switch logs a corresponding message. Using this allowed MAC option binds MAC addresses to a VLAN so that the address is not registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.

NOTE: If you do not want the switch to log messages received for invalid MAC addresses, disable that logging using the command **no-allowed-mac-log** .

When the configured limit of MAC addresses is exceeded, any one of the following actions can be performed :

- **drop**—Drop the packet and generate an alarm, an SNMP trap, or a system log entry. This is the default.
- **log**—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- **none**—Take no action.
- **shutdown**—Disable the interface or VLAN and generate an alarm. If you have configured the switch with the port-error-disable statement, the disabled interface (or VLAN) recovers automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces or VLAN using the command **clear ethernet-switching port-error** .

To configure MAC limiting, using the CLI:

1. Limit the number of dynamic MAC addresses to**5**.

Because no action is specified, the switch performs the default action **drop** if the limit is exceeded:

- Limit a single interface (here, the interface is **ge-0/0/1**):

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

- Limit all interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all mac–limit 5
```

- Limit a specific VLAN:

```
[edit vlans]
user@switch# set vlan-abc mac–limit 20
```

NOTE: Do not set the mac-limit to 1. The first learned MAC address is often inserted into the forwarding database automatically (for instance, for Routed VLAN Interfaces the first MAC address inserted into the forwarding database is the MAC address of the RVI. For Aggregated Ethernet bundles using LACP, the first MAC address inserted into the forwarding database in the forwarding table is the source address of the protocol packet). The switch will therefore not learn MAC addresses other than the automatic addresses when the mac-limit is set to 1, and this will cause problems with MAC learning and forwarding.

NOTE: You must clear existing entries in the MAC address forwarding table that correspond to the change you make with the command mac-limit. For example, if you change the limit on an interface, clear the MAC address forwarding table entries for that interface. If you change the limit on all interfaces and VLANs, clear all MAC address forwarding table entries. If you change the limit on a VLAN, clear the MAC address forwarding table entries for that VLAN. This action is performed in the next step.

2. Clear the current MAC address forwarding table entries for the MAC limited entity, either the interface, all entries, or a VLAN :

   - Clear MAC address entries from a specific interface (here, the interface is **ge-0/0/1**) in the forwarding table:

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

   - Clear all MAC address entries in the forwarding table:

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

- Clear MAC address entries from a specific VLAN (here, the VLAN is **vlan-abc**) in the forwarding table:

```
user@switch1# clear ethernet-switching-table vlan vlan-abc
```

3. Specify specific allowed MAC addresses:

   - On a single interface (here, the interface is **ge-0/0/2**):

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

   - On all interfaces:

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

Related Documentation

- Configuring MAC Limiting (J-Web Procedure) on page 103
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 34
- Verifying That MAC Limiting Is Working Correctly on page 123
- Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure) on page 108
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 17
- **no-allowed-mac-log on page 154**

Configuring MAC Limiting (J-Web Procedure)

MAC limiting protects against flooding of the Ethernet switching table on an EX Series switch. MAC limiting sets a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface (port).

Junos OS provides two MAC limiting methods:

- Maximum number of dynamic MAC addresses allowed per interface—If the limit is exceeded, incoming packets with new MAC addresses are dropped.
- Specific "allowed" MAC addresses for the access interface—Any MAC address that is not in the list of configured addresses is not learned.

You configure MAC limiting for each interface, not for each VLAN. You can specify the maximum number of dynamic MAC addresses that can be learned on a single Layer 2 access interface or on all Layer 2 access interfaces. The default action that the switch will take if that maximum number is exceeded is **drop**—drop the packet and generate an alarm, an SNMP trap, or a system log entry.

To enable MAC limiting on one or more interfaces using the J-Web interface:

1. Select **Configure>Security>Port Security**.
2. Select one or more interfaces from the **Interface List**.
3. Click the **Edit** button. If a message appears asking whether you want to enable port security, click **Yes**.
4. To set a dynamic MAC limit:
    1. Type a limit value in the **MAC Limit** box.
    2. Select an action from the **MAC Limit Action** box (optional). The switch takes this action when the MAC limit is exceeded. If you do not select an action, the switch applies the default action, **drop**.
        - Log—Generate a system log entry, an SNMP trap, or an alarm.
        - Drop—Drop the packets and generate a system log entry, an SNMP trap, or an alarm. (Default)
        - Shutdown—Shut down the VLAN and generate an alarm. You can mitigate the effect of this option by configuring the switch for autorecovery from the disabled state and specifying a **disable timeout** value. See "Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)" on page 118. If you have not configured autorecovery from the disabled state, you can bring up the interfaces by running the **clear ethernet-switching port-error** command.
        - None— No action to be taken.
5. To add allowed MAC addresses:

1. Click **Add**.
2. Type the allowed MAC address and click **OK**.

   Repeat this step to add more allowed MAC addresses.

6. Click **OK** when you have finished setting MAC limits.
7. Click **OK** after the configuration has been successfully delivered.

NOTE: You can enable or disable port security on the switch at any time by clicking the **Activate** or **Deactivate** button on the Port Security Configuration page. If security status is shown as **Disabled** when you try to edit settings for any VLANs or interfaces (ports), a message asking whether you want to enable port security appears.

Related Documentation

- Configuring MAC Limiting (CLI Procedure) on page 100
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 48
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 34
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 41
- Verifying That MAC Limiting Is Working Correctly on page 123
- Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure) on page 108
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 17

Configuring MAC Move Limiting (CLI Procedure)

When MAC move is configured, MAC address movements are tracked by the switch and, if a MAC address changes more than the configured number of times within one second, the changes to MAC addresses are either dropped, logged, ignored, or the interface is shut down.

NOTE: Although you enable this feature on VLANs, the MAC move limitation pertains to the number of movements for each individual MAC address rather than the total number of MAC address moves in the VLAN. For example, If the MAC move limit is set to 1, the switch allows an unlimited number of MAC address movements within the VLAN as long as the same MAC address does not change more than once.

You configure MAC move limiting per VLAN, not per interface (port). In the default configuration, the number of MAC moves permitted is unlimited.

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

- **drop**—Drop the packet and generate an alarm, an SNMP trap, or a system log entry. This is the default.
- **log**—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- **none**—Take no action.
- **shutdown**—Disable the interfaces in the VLAN and generate an alarm. If you have configured the switch with the port-error-disable statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the **clear ethernet-switching port-error** command.

To configure a MAC move limit for MAC addresses within a specific VLAN or for MAC addresses within all VLANs, using the CLI:

- On a single VLAN: To limit the number of MAC address movements that can be made by an individual MAC address within the VLAN **employee-vlan**, set a MAC move limit of **5**:

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

  The action is not specified, so the switch performs the default action **drop** if it tracks that an individual MAC address within the **employee-vlan** has moved more than 5 times within one second.

- On all VLANs: To limit the number of MAC movements that can be made by individual MAC addresses within all VLANs, set a MAC move limit of **5**:

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

  The action is not specified, so the switch performs the default action **drop** if it tracks that an individual MAC address within any of the VLANs has moved more than 5 times within one second.

Related Documentation

- Configuring MAC Move Limiting (J-Web Procedure) on page 107
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Verifying That MAC Move Limiting Is Working Correctly on page 127
- Monitoring Port Security on page 119
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 17

Configuring MAC Move Limiting (J-Web Procedure)

MAC move limiting detects MAC address movement and MAC address spoofing on access ports. MAC address movements are tracked, and if a MAC address moves more than the configured number of times within one second, the configured (or default) action is performed. You enable this feature on VLANs.

NOTE: Although you enable this feature on VLANs, the MAC move limitation pertains to the number of movements for each individual MAC address rather than the total number of MAC address moves in the VLAN. For example, If the MAC move limit is set to 1, the switch allows an unlimited number of MAC address movements within the VLAN as long as the same MAC address does not move more than once.

In the default configuration, the MAC move limit within each VLAN is unlimited; the default action that the switch will take if the specified MAC move limit is exceeded is **drop**.

To enable MAC move limiting for MAC addresses within one or more VLANs by using the J-Web interface:

1. Select **Configure>Security>Port Security**.
2. Select one or more VLANs from the **VLAN List**.
3. Click the **Edit** button. If a message appears asking whether you want to enable port security, click **Yes**.
4. To set a MAC move limit:
    1. Type a limit value in the **MAC Movement** box.
    2. Select an action from the **MAC Movement Action** box (optional). The switch takes this action when an individual MAC address exceeds the MAC move limit. If you do not select an action, the switch applies the default action, **drop**.

       Select one:

       - Log—Generate a system log entry, an SNMP trap, or an alarm.
       - Drop—Drop the packets and generate a system log entry, an SNMP trap, or an alarm. (Default)
       - Shutdown—Shut down the VLAN and generate an alarm. You can mitigate the effect of this option by configuring the switch for autorecovery from the disabled state and specifying a **disable timeout** value. See "Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)" on page 118. If you have not configured autorecovery from the disabled state, you can bring up the interfaces by running the **clear ethernet-switching port-error** command.
       - None— No action to be taken.

3. Click **OK**.

5. Click **OK** after the configuration has been successfully delivered.

NOTE: You can enable or disable port security on the switch at any time by clicking the **Activate** or **Deactivate** button on the Port Security Configuration page. If security status is shown as **Disabled** when you try to edit settings for any VLANs, a message asking whether you want to enable port security appears.

Related Documentation

- Configuring MAC Move Limiting (CLI Procedure) on page 105
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Verifying That MAC Move Limiting Is Working Correctly on page 127
- Monitoring Port Security on page 119
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 17

Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure)

If you set a MAC limit in your port security settings to apply to all interfaces on the EX Series switch, you can override that setting for a particular interface by specifying action **none**.

To use the **none** action to override a MAC limit setting:

1. Set the MAC limit—for example, a limit of **5** with action **drop**:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all mac-limit 5 action drop
```

2. Then change the action for one interface (here, **ge-0/0/2**) with this command. You don't need to specify a limit value.

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge–0/0/2 mac-limit action none
```

Related Documentation

- Configuring MAC Limiting (CLI Procedure) on page 100
- Configuring MAC Limiting (J-Web Procedure) on page 103
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Verifying That MAC Limiting Is Working Correctly on page 123

Configuring IP Source Guard (CLI Procedure)

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, it ensures that the switch does not forward the packet—that is, the packet is discarded.

You enable the IP source guard feature on VLANs. You can enable it on a specific VLAN, on all VLANs, or on a VLAN range.

NOTE: IP source guard applies only to access interfaces and only to untrusted interfaces. If you enable IP source guard on a VLAN that includes trunk interfaces or an interface set to dhcp-trusted, the CLI shows an error when you try to commit the configuration.

NOTE: You can use IP source guard together with 802.1X user authentication in single supplicant, single-secure supplicant or multiple supplicant mode.

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.
- 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.

Before you configure IP source guard, be sure that you have:

Explicitly enabled DHCP snooping on the specific VLAN or specific VLANs on which you will configure IP source guard. See "Enabling DHCP Snooping (CLI Procedure)" on page 92. If you configure IP source guard on specific VLANs rather than on all VLANs, you must also enable DHCP snooping explcitly on those VLANs. Otherwise, the default value of no DHCP snooping applies to that VLAN.

To enable IP source guard on a VLAN, all VLANs, or a VLAN range (a series of tagged VLANs) by using the CLI:

NOTE: Replace values displayed in italics with values for your configuration.

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch#set vlan default ip-source-guard
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all ip-source-guard
```

- On a VLAN range:

  1. Set the VLAN range (the VLAN name is **employee**):

```
[edit vlans]
user@switch# set employeevlan-range 100-101
```

  2. Associate an interface with a VLAN-range number (**100** in the following example) and set the port mode to **access**:

```
[edit interfaces]
user@switch# set ge-0/0/6 unit 0 family ethernet-switching port-mode access vlan
members100
```

  3. Enable IP source guard on the VLAN **employee**:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan employee ip-source-guard
```

NOTE: You can use the **no-ip-source-guard** statement to disable IP source guard for a specific VLAN after you have enabled the feature for all VLANs.

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Related Documentation

- Verifying That IP Source Guard Is Working Correctly on page 128
- Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 67
- Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 59
- Understanding IP Source Guard for Port Security on EX Series Switches on page 23

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

You can add static (fixed) IP addresses and bind them to fixed MAC addresses in the DHCP snooping database. These bindings are labeled as “static” in the database, while those bindings that have been added through the process of DHCP snooping are labeled “dynamic.”

To configure a static IP address/MAC address binding in the DHCP snooping database (replace **ge-0/0/2**, **10.0.10.12**, **data-vlan**, and **00:05:85:3A:82:80** with values for your configuration):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/2 static-ip 10.0.10.12 vlan data-vlan mac 00:05:85:3A:82:80
```

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Related Documentation

- Verifying That DHCP Snooping Is Working Correctly on page 120
- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8

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

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

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

- The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as routed VLAN interfaces, or RVIs. The switch relays the clients' requests to the server and then forwards the server's replies to the clients. This topic describes this configuration.
- The switch, DHCP clients, and DHCP server are all on the same VLAN. The switch forwards the clients' requests to the server and forwards the server's replies to the clients. This configuration is described in "Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)" on page 115.

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

- Connect and configure the DHCP server.

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

- Configure the VLAN on the switch and associate the interfaces on which the clients connect to the switch with that VLAN.
- Configure the routed VLAN interface (RVI) to allow the switch to relay packets to the server and receive packets from the server. See Configuring Routed VLAN Interfaces (CLI Procedure).
- Configure the switch as a BOOTP relay agent. See DHCP/BOOTP Relay for EX Series Switches Overview.

To configure DHCP option 82:

NOTE: Replace values displayed in italics with values for your configuration.

1. Specify DHCP option 82 for the BOOTP server:

   - On all interfaces that connect to the server:

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

   - On a specific interface that connects to the server:

     ```
     [edit forwarding-options helpers bootp]
     user@switch# set interface ge-0/0/10 dhcp-option82
     ```

     The remaining steps are optional. They show configurations for all interfaces; include the specific interface designation to configure any of the following options on a specific interface:

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

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

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

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 circuit-id use-interface-description
   ```

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

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

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

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

6. To configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

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

7. To specify that the prefix for the remote ID suboption is the hostname of the switch rather than the MAC address of the switch (the default):

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

8. To specify that the remote ID suboption value contains the interface description:

   ```
   [edit forwarding-options helpers bootp]
   user@switch# set dhcp-option82 remote-id use-interface-description
   ```

9. To specify that the remote ID suboption value contains a character string:

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id use-string mystring
```

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

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

11. To specify that the vendor ID suboption value contains a character string value that you specify rather than **Juniper** (the default):

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

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Related Documentation

- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- [edit forwarding-options] Configuration Statement Hierarchy on page 136
- Understanding DHCP Option 82 for Port Security on EX Series Switches on page 20
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

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

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

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

- The switch, DHCP clients, and DHCP server are all on the same VLAN. The switch forwards the clients' requests to the server and forwards the server's replies to the clients. This topic describes this configuration.
- The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as routed VLAN interfaces, or RVIs. The switch relays the clients' requests to the server and then forwards the server's replies to the clients. This configuration is described in "Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)" on page 112.

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

- Connect and configure the DHCP server.

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

- Configure a VLAN on the switch and associate the interfaces on which the clients and the server connect to the switch with that VLAN.

To configure DHCP option 82:

NOTE: Replace values displayed in italics with values for your configuration.

1. Specify DHCP option 82 for all VLANs associated with the switch or for a specified VLAN. (You can also configure the feature for a VLAN range.)

   - On a specific VLAN:

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

   - On all VLANs:

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

   The remaining steps are optional.

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

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

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

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

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

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

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

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

6. To configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

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

7. To specify that the prefix for the remote ID suboption is the hostname of the switch rather than the MAC address of the switch (the default):

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

8. To specify that the remote ID suboption value contains the interface description:

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

9. To specify that the remote ID suboption value contains a character string:

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

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

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

11. To specify that the vendor ID suboption value contains a character string value that you specify rather than **Juniper** (the default):

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

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Related Documentation

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Understanding DHCP Option 82 for Port Security on EX Series Switches on page 20
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

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

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

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

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

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

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

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Configuring MAC Limiting (CLI Procedure) on page 100
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 17
- Understanding Storm Control on EX Series Switches

CHAPTER 4

Verifying Port Security

Monitoring Port Security

Purpose Use the monitoring functionality to view these port security details:

- DHCP snooping database for a VLAN or all VLANs
- ARP inspection details for all interfaces

Action To monitor port security in the J-Web interface, select **Monitor** > **Security** > **Port Security**.

To monitor and manipulate the DHCP snooping database and ARP inspection statistics in the CLI, enter the following commands:

- **show dhcp snooping binding**
- **clear dhcp snooping binding**—In addition to clearing the whole database, you can clear database entries for specified VLANs or MAC addresses.
- **show arp inspection statistics**
- **clear arp inspection statistics**

Meaning The J-Web Port Security Monitoring page comprises two sections:

- DHCP Snooping—Displays the DHCP snooping database for all the VLANs for which DHCP snooping is enabled. To view the DHCP snooping database for a specific VLAN, select the specific VLAN from the list.

- ARP Inspection—Displays the ARP inspection details for all interfaces. The information includes details of the number of packets that passed ARP inspection and the number of packets that failed the inspection. The pie chart graphically represents these statistics when you select an interface. To view ARP inspection statistics for a specific interface, select the interface from the list.

You have the following options on the page:

- Clear ALL—Clears the DHCP snooping database, either for all VLANs if the option **ALL** has been selected in the Select VLANs list or for the specific VLAN that has been selected in that list.
- Clear—Deletes a specific IP address from the DHCP snooping database.

To clear ARP statistics on the page, click **Clear All** in the ARP Statistics section.

Use the CLI commands to show and clear DHCP snooping database and ARP inspection statistics details.

Related Documentation

- Configuring Port Security (CLI Procedure) on page 88
- Configuring Port Security (J-Web Procedure) on page 90
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27

Verifying That DHCP Snooping Is Working Correctly

Purpose Verify that DHCP snooping is working on the switch and that the DHCP snooping database is correctly populated with both dynamic and static bindings.

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

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

```
user@switch>  show dhcp snooping binding
DHCP Snooping Information:
MAC address        IP address  Lease (seconds) Type     VLAN      Interface

00:05:85:3A:82:77  192.0.2.17  600             dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:79  192.0.2.18  653             dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:80  192.0.2.19  720             dynamic  employee  ge-0/0/2.0
00:05:85:3A:82:81  192.0.2.20  932             dynamic  employee  ge-0/0/2.0
00:05:85:3A:82:83  192.0.2.21  1230            dynamic  employee  ge-0/0/2.0
00:05:85:27:32:88  192.0.2.22  –               static   data      ge-0/0/4.0
```

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

expires. Static IP addresses have no assigned lease time. The statically configured entry never expires.

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

Related Documentation

- Enabling DHCP Snooping (CLI Procedure) on page 92
- Enabling DHCP Snooping (J-Web Procedure) on page 94
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 111
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44
- Monitoring Port Security on page 119
- Troubleshooting Port Security on page 131

Verifying That a Trusted DHCP Server Is Working Correctly

Purpose Verify that a DHCP trusted server is working on the switch. See what happens when the DHCP server is trusted and then untrusted.

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

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

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

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

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

Related Documentation

- Enabling a Trusted DHCP Server (CLI Procedure) on page 95
- Enabling a Trusted DHCP Server (J-Web Procedure) on page 96
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 38
- Monitoring Port Security on page 119
- Troubleshooting Port Security on page 131

Verifying That DAI Is Working Correctly

Purpose Verify that dynamic ARP inspection (DAI) is working on the switch.

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

Display the DAI information:

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

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

Related Documentation

- Enabling Dynamic ARP Inspection (CLI Procedure) on page 96
- Enabling Dynamic ARP Inspection (J-Web Procedure) on page 98
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44
- Monitoring Port Security on page 119

Verifying That MAC Limiting Is Working Correctly

MAC limiting protects against flooding of the Ethernet switching table. MAC limiting sets a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface (port).

Junos OS provides two MAC limiting methods:

- Maximum number of dynamic MAC addresses allowed per interface—When the limit is exceeded, incoming packets with new MAC addresses are dropped.
- Specific "allowed" MAC addresses for the access interface—Any MAC address that is not in the list of configured addresses is not learned.

To verify MAC limiting configurations:

1. Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly on page 123
2. Verifying That Allowed MAC Addresses Are Working Correctly on page 124
3. Verifying Results of Various Action Settings When the MAC Limit Is Exceeded on page 124
4. Customizing the Ethernet Switching Table Display to View Information for a Specific Interface on page 126

Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly

Purpose Verify that MAC limiting for dynamic MAC addresses is working on the switch.

Action Display the MAC addresses that have been learned. The following sample output shows the results when two packets were sent from hosts on **ge-0/0/1** and five packets requests were sent from hosts on **ge-0/0/2**, with both interfaces set to a MAC limit of **4** with the action **drop**:

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

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

Meaning The sample output shows that with a MAC limit of **4** for each interface, the packet for a fifth MAC address on **ge-0/0/2** was dropped because it exceeded the MAC limit. The address was not learned, and thus an asterisk (*) rather than an address appears in the **MAC address** column in the first line of the sample output.

Verifying That Allowed MAC Addresses Are Working Correctly

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

Action Display the MAC cache information after allowed MAC addresses have been configured on an interface. The following sample shows the MAC cache after 5 allowed MAC addresses had been configured on interface **ge/0/0/2**. In this instance, the interface was also set to a dynamic MAC limit of **4** with action **drop**.

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

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

Meaning Because the MAC limit value for this interface had been set to **4**, only four of the five configured allowed addresses were learned and thus added to the MAC cache. Because the fifth address was not learned, an asterisk (*) rather than an address appears in the **MAC address** column in the last line of the sample output.

Verifying Results of Various Action Settings When the MAC Limit Is Exceeded

Purpose Verify the results provided by the various action settings for MAC limits—**drop**, **log**, **none**, and **shutdown**—when the limits are exceeded.

Action Display the results of the various action settings.

NOTE: You can view log messages by using the **show log messages** command. You can also have the log messages displayed by configuring the monitor start messages with the **monitor start messages** command.

- **drop** action—For MAC limiting configured with a **drop** action and with the MAC limit set to **5**:

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

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


  employee-vlan       *                   Flood          -    ge-0/0/2.0

  employee-vlan       00:05:85:3A:82:80   Learn          0    ge-0/0/2.0

  employee-vlan       00:05:85:3A:82:81   Learn          0    ge-0/0/2.0

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

```
  employee-vlan        00:05:85:3A:82:85   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:88   Learn          0    ge-0/0/2.0
```

- **log** action—For MAC limiting configured with a **log** action and with MAC limit set to **5**:

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

Ethernet-switching table: 74 entries, 73 learned
  VLAN                 MAC address         Type         Age    Interfaces

  employee-vlan        *                   Flood          -    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:80   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:81   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:82   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:83   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:84   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:85   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:87   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:88   Learn          0    ge-0/0/2.0

  . . .
```

- **shutdown** action—For MAC limiting configured with a **shutdown** action and with MAC limit set to **3**:

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

Ethernet-switching table: 4 entries, 3 learned
  VLAN                 MAC address         Type         Age    Interfaces

  employee-vlan        *                   Flood          -    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:82   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:84   Learn          0    ge-0/0/2.0

  employee-vlan        00:05:85:3A:82:87   Learn          0    ge-0/0/2.0
```

- **none** action—If you set a MAC limit to apply to all interfaces on the switch, you can override that setting for a particular interface by specifying this action for that interface. See "Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure)" on page 108.

Meaning For the **drop** action results—The sixth MAC address exceeded the MAC limit. The request packet for that address was dropped. Only five MAC addresses have been learned on **ge-0/0/2**.

For the **log** action results—The sixth MAC address exceeded the MAC limit. No MAC addresses were blocked.

For the **shutdown** action results—The fourth MAC address exceeded the MAC limit. Only three MAC addresses have been learned on **ge-0/0/2**. The interface **ge-0/0/1** is shut down.

For more information about interfaces that have been shut down, use the **show ethernet-switching interfaces** command.

```
user@switch> show ethernet-switching interfaces
Interface    State  VLAN members        Tag   Tagging  Blocking


bme0.32770   down   mgmt                      untagged unblocked

ge-1/0/0.0   down   v1                        untagged MAC limit exceeded

ge-1/0/1.0   up     v1                        untagged unblocked

ge-1/0/2.0   up     v1                        untagged unblocked

me0.0        up     mgmt                      untagged unblocked
```

NOTE: You can configure the switch to recover automatically from this type of error condition by specifying the **port-error-disable** statement with a **disable timeout** value. The switch automatically restores the disabled interface to service when the disable timeout expires. The **port-error-disable** configuration does not apply to pre-existing error conditions. It impacts only error conditions that are detected after **port-error-disable** has been enabled and committed. To clear a pre-existing error condition and restore the interface to service, use the **clear ethernet-switching port-error** command.

Customizing the Ethernet Switching Table Display to View Information for a Specific Interface

Purpose You can use the **show ethernet-switching table** command to view information for a specific interface.

Action For example, to display the MAC addresses that have been learned on **ge-0/0/2** interface, type:

```
user@switch> show ethernet-switching table interface ge-0/0/2.0
Ethernet-switching table: 1 unicast entries

  VLAN              MAC address       Type         Age Interfaces

  v1                *                 Flood          - All-members

  v1                00:00:06:00:00:00 Learn          0 ge-2/0/0.0
```

Meaning The MAC limit value for **ge-0/0/2** had been set to **1**, and the output shows that only one MAC address was learned and thus added to the MAC cache. An asterisk (*) rather than an address appears in the **MAC address** column in the first line of the sample output.

Related Documentation

- Configuring MAC Limiting (CLI Procedure) on page 100
- Configuring MAC Limiting (J-Web Procedure) on page 103
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 48
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 34
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 41
- Monitoring Port Security on page 119

Verifying That MAC Move Limiting Is Working Correctly

Purpose Verify that MAC move limiting is working on the switch.

Action Display the MAC addresses in the Ethernet switching table when MAC move limiting has been configured for a VLAN. The following sample shows the results after two of the hosts on **ge-0/0/2** sent packets after the MAC addresses for those hosts had moved to other interfaces more than five times in 1 second. The VLAN, **employee-vlan**, was set to a MAC move limit of **5** with the action **drop**:

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

Ethernet-switching table:  7 entries, 4 learned
  VLAN                MAC address         Type         Age    Interfaces

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

Meaning The last two lines of the sample output show that MAC addresses for two hosts on **ge-0/0/2** were not learned, because the hosts had been moved back and forth from the original interfaces more than five times in 1 second.

NOTE: For descriptions of the results of the various action settings—**drop**, **log**, **none**, and **shutdown**—see "Verifying That MAC Limiting Is Working Correctly" on page 123.

Related Documentation

- Configuring MAC Move Limiting (CLI Procedure) on page 105
- Configuring MAC Move Limiting (J-Web Procedure) on page 107
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Monitoring Port Security on page 119

Verifying That IP Source Guard Is Working Correctly

Purpose Verify that IP source guard is enabled and is mitigating the effects of any source IP spoofing attacks on the EX Series switch.

Action Display the IP source guard database.

```
user@switch> show ip-source-guard
IP source guard information:
Interface    Tag  IP Address   MAC Address        VLAN

ge-0/0/12.0  0    10.10.10.7   00:30:48:92:A5:9D  vlan100

ge-0/0/13.0  0    10.10.10.9   00:30:48:8D:01:3D  vlan100

ge-0/0/13.0  100  *            *                  voice
```

Meaning The IP source guard database table contains the VLANs enabled for IP source guard, the untrusted access interfaces on those VLANs, the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another. If a switch interface is associated with multiple VLANs and some of those VLANs are enabled for IP source guard and others are not, the VLANs that are not enabled for IP source guard have a star (*) in the **IP Address** and **MAC Address** fields. See the entry for the **voice** VLAN in the preceding sample output.

Related Documentation

- Configuring IP Source Guard (CLI Procedure) on page 109

Verifying That the Port Error Disable Setting Is Working Correctly

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

Action Display information about interfaces:

```
user@switch>  show ethernet-switching interfaces
Interface   State    VLAN members          Blocking
ge-0/0/0.0  up       T1122                 unblocked
ge-0/0/1.0  down     default               MAC limit exceeded
ge-0/0/2.0  down     default               MAC move limit exceeded
ge-0/0/3.0  down     default               Storm control in effect
ge-0/0/4.0  down     default               unblocked
ge-0/0/5.0  down     default               unblocked
ge-0/0/6.0  down     default               unblocked
```

```
ge-0/0/7.0  down     default              unblocked
ge-0/0/8.0  down     default              unblocked
ge-0/0/9.0  up       T111                 unblocked
ge-0/0/10.0 down     default              unblocked
ge-0/0/11.0 down     default              unblocked
ge-0/0/12.0 down     default              unblocked
ge-0/0/13.0 down     default              unblocked
ge-0/0/14.0 down     default              unblocked
ge-0/0/15.0 down     default              unblocked
ge-0/0/16.0 down     default              unblocked
ge-0/0/17.0 down     default              unblocked
ge-0/0/18.0 down     default              unblocked
ge-0/0/19.0 up       T111                 unblocked
ge-0/1/0.0  down     default              unblocked
ge-0/1/1.0  down     default              unblocked
ge-0/1/2.0  down     default              unblocked
ge-0/1/3.0  down     default              unblocked
```

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

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

Related Documentation

- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118

CHAPTER 5

Troubleshooting Port Security

Troubleshooting Port Security

Troubleshooting issues for port security on EX Series switches:

MAC Addresses That Exceed the MAC Limit or MAC Move Limit Are Not Listed in the Ethernet Switching Table

Problem You see log messages telling you that the MAC limit or MAC move limit has been exceeded, but the specific offending MAC addresses that have been exceeding the limit are not listed in the Ethernet switching table.

Solution

1. Set the MAC limit or MAC move limit action to **log**.

```
[edit ethernet-switching-options secure-access port]
user@switch# set interface ge-0/0/2 mac-limit 5 action log
```

2. Allow some MAC address requests to come in.
3. View the entries in the Ethernet switching table:

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

Multiple DHCP Server Packets Have Been Received on Untrusted Interfaces

Problem You see log messages that DHCP server packets were received on an untrusted interface—for example:

```
5 untrusted DHCPOFFER received, interface ge-0/0/0.0[65], vlan v1[10] server
ip/mac 12.12.12.1/00:00:00:00:01:12 offer ip/client mac
12.12.12.253/00:AA:BB:CC:DD:01
```

These messages can signal the presence of a malicious DHCP server on the network.

Solution Configure a firewall filter to block the IP address or MAC address of the malicious DHCP server. See Configuring Firewall Filters (CLI Procedure).

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Verifying That a Trusted DHCP Server Is Working Correctly on page 121
- Verifying That MAC Limiting Is Working Correctly on page 123
- Enabling a Trusted DHCP Server (CLI Procedure) on page 95
- Configuring MAC Limiting (CLI Procedure) on page 100

CHAPTER 6

Configuration Statements for Port Security

[edit ethernet-switching-options] Configuration Statement Hierarchy

```
ethernet-switching-options {
  analyzer {
    name {
      loss-priority priority;
      ratio number;
      input {
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
        egress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      }
      output {
        interface interface-name;
        vlan (vlan-id | vlan-name) {
          no-tag;
        }
      }
    }
  }
  bpdu-block {
    disable-timeout timeout;
    interface (all | [interface-name]);
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100);
  }
  interfaces interface-name {
    no-mac-learning;
  }
```

```
mac-notification {
    notification-interval seconds;
}
mac-table-aging-time seconds;
nonstop-bridging;
port-error-disable {
    disable-timeout timeout;
}
redundant-trunk-group {
    group name {
        preempt-cutover-timer seconds;
        interface
            primary;
        }
        interface
    }
}
secure-access-port {
    dhcp-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    interface (all | interface-name) {
        allowed-mac {
            mac-address-list;
        }
        (dhcp-trusted | no-dhcp-trusted );
        fcoe-trusted;
        mac-limit limit action action;
        no-allowed-mac-log;
        static-ip  ip-address {
            vlan  vlan-name;
            mac mac-address;
        }
    }
    vlan (all | vlan-name) {
        (arp-inspection | no-arp-inspection) [
            forwarding-class class-name;
        }
        dhcp-option82 {
            circuit-id {
                prefix hostname;
                use-interface-description;
                use-vlan-id;
            }
            remote-id {
                prefix hostname | mac | none;
                use-interface-description;
                use-string string;
            }
            vendor-id [string];
        }
        (examine-dhcp | no-examine-dhcp) {
            forwarding-class class-name;
        }
```

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

Related Documentation

- Understanding Port Mirroring on EX Series Switches
- Port Security for EX Series Switches Overview on page 3
- Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches
- Understanding Redundant Trunk Links on EX Series Switches
- Understanding Storm Control on EX Series Switches
- Understanding 802.1X and VoIP on EX Series Switches
- Understanding Q-in-Q Tunneling on EX Series Switches

- Understanding Unknown Unicast Forwarding on EX Series Switches
- Understanding MAC Notification on EX Series Switches
- Understanding FIP Snooping
- Understanding Nonstop Bridging on EX Series Switches

[edit forwarding-options] Configuration Statement Hierarchy

```
helpers {
  bootp {
    dhcp-option82 {
      circuit-id {
        prefix hostname;
        use-interface-description;
        use-vlan-id;
      }
      remote-id {
        prefix hostname | mac | none;
        use-interface-description;
        use-string string;
      }
      vendor-id <string>;
    }
    interface interface-name {
      dhcp-option82 {
        circuit-id {
          prefix hostname;
          use-interface-description;
          use-vlan-id;
        }
        remote-id {
          prefix hostname | mac | none;
          use-interface-description;
          use-string string;
        }
        vendor-id <string>;
      }
      source-address-giaddr;
    }
    source-address-giaddr;
  }
}
```

Related Documentation

- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- Understanding DHCP Option 82 for Port Security on EX Series Switches on page 20
- DHCP/BOOTP Relay for EX Series Switches Overview

- For more information about the [edit forwarding-options] hierarchy and its options, see *Junos OS Policy Framework Configuration Guide*

allowed-mac

Syntax

```
allowed-mac {
  mac-address-list;
}
```

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

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

Description Specify particular MAC addresses to be added to the MAC address cache.

NOTE: Although this configuration restricts the addresses that can be added to the MAC address cache, it does not block the switch from receiving Layer 2 control packets—such as Link Layer Discovery Protocol (LLDP) packets—transmitted from MAC addresses that are not specified in the list of allowed MAC addresses. Control packets do not undergo the MAC address check and they are therefore included in the statistics of packets received. However, they are not forwarded to another destination. They are trapped within the switch.

Default Allowed MAC addresses take precedence over dynamic MAC values that have been applied with the **mac-limit** statement.

Options ***mac-address-list***—One or more MAC addresses configured as allowed MAC addresses for a specified interface or all interfaces.

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

Related Documentation

- mac-limit on page 152
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 48
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 34
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 41
- Configuring MAC Limiting (CLI Procedure) on page 100
- Configuring MAC Limiting (J-Web Procedure) on page 103

arp-inspection

Syntax

```
(arp-inspection | no-arp-inspection) {
  forwarding-class class-name;
}
```

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

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

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

- **arp-inspection**—Enable DAI.

  When ARP inspection is enabled, the switch logs invalid ARP packets that it receives on each interface, along with the sender's IP and MAC addresses.

- **no-arp-inspection**—Disable DAI.

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 Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44
- Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 81
- Enabling Dynamic ARP Inspection (CLI Procedure) on page 96
- Enabling Dynamic ARP Inspection (J-Web Procedure) on page 98

circuit-id

Syntax

```
circuit-id {
  prefix hostname;
  use-interface-description;
  use-vlan-id;
}
```

Hierarchy Level

[edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82]
[edit forwarding-options helpers bootp dhcp-option82]
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

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 (interface and/or VLAN) on which the DHCP request arrived.

The format of the **circuit-id** information for Gigabit Ethernet interfaces that use VLANs is ***interface-name*:*vlan-name***. On a Layer 3 interface, the format is just ***interface-name*.**

The remaining statements are explained separately.

Default

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

Required Privilege Level

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

Related Documentation

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- [edit forwarding-options] Configuration Statement Hierarchy on page 136
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

dhcp-option82

Syntax

```
dhcp-option82 {
  circuit-id {
    prefix hostname;
    use-interface-description;
    use-vlan-id;
  }
  remote-id {
    prefix hostname | mac | none;
    use-interface-description;
    use-string string;
  }
  vendor-id <string>;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

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

The remaining statements are explained separately.

Default

Insertion of DHCP option 82 information is not enabled.

Required Privilege Level

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

Related Documentation

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- [edit forwarding-options] Configuration Statement Hierarchy on page 136

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

dhcp-snooping-file

Syntax

```
dhcp-snooping-file {
  location local_pathname | remote_URL;
  timeout seconds;
  write-interval seconds;
}
```

Hierarchy Level [edit ethernet-switching-options secure-access-port]

Release Information Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description Specify a local pathname or remote URL for the DHCP snooping database file to maintain persistence of IP-MAC bindings.

The remaining statements are explained separately.

Default The IP-MAC bindings in the DHCP snooping database file are not persistent. If the switch is rebooted, the bindings are lost.

Required Privilege Level 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 EX Series Switches on page 8

dhcp-trusted

Syntax (dhcp-trusted | no-dhcp-trusted);

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

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

Description Allow DHCP responses from the specified interfaces (ports) or all interfaces.

- **dhcp-trusted**—Allow DHCP responses.
- **no-dhcp-trusted**—Deny DHCP responses.

Default Trusted for trunk ports, untrusted for access ports.

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 38
- Enabling a Trusted DHCP Server (CLI Procedure) on page 95
- Enabling a Trusted DHCP Server (J-Web Procedure) on page 96

disable-timeout

Syntax disable-timeout *timeout*;

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

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

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

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

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

Default The disable timeout is not enabled.

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

Range: 10 through 3600 seconds

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

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118

ethernet-switching-options

Syntax

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

```
interface (all | interface-name) {
  allowed-mac {
    mac-address-list;
  }
  (dhcp-trusted | no-dhcp-trusted);
  fcoe-trusted;
  mac-limit limit action action;
  no-allowed-mac-log;
  static-ip ip-address {
    vlan  vlan-name;
    mac mac-address;
  }
}
vlan (all | vlan-name) {
  (arp-inspection | no-arp-inspection) [
    forwarding-class class-name;
  }
  dhcp-option82 {
    circuit-id {
      prefix hostname;
      use-interface-description;
      use-vlan-id;
    }
    remote-id {
      prefix hostname | mac | none;
      use-interface-description;
      use-string string;
    }
    vendor-id [string];
  }
  (examine-dhcp | no-examine-dhcp) {
    forwarding-class class-name;
  }
  examine-fip {
    fc-map fc-map-value;
  }
  (ip-source-guard | no-ip-source-guard);
  mac-move-limit limit action action;
}
static {
  vlan name {
    mac mac-address {
      next-hop interface-name;
    }
  }
}
storm-control {
  action-shutdown;
  interface (all | interface-name) {
    bandwidth bandwidth;
    no-broadcast;
    no-multicast;
    no-registered-multicast;
    no-unknown-unicast;
    no-unregistered-multicast;
  }
```

```
    }
    traceoptions {
      file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
    unknown-unicast-forwarding {
      vlan (all | vlan-name) {
        interface interface-name;
      }
    }
    voip {
      interface (all | [interface-name | access-ports]) {
        vlan vlan-name ;
        forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
          network-control);
      }
    }
  }
```

Hierarchy Level [edit]

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

Description Configure Ethernet switching options.

The remaining statements are explained separately.

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

Related Documentation

- Understanding Port Mirroring on EX Series Switches
- Port Security for EX Series Switches Overview on page 3
- Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches
- Understanding Redundant Trunk Links on EX Series Switches
- Understanding Storm Control on EX Series Switches
- Understanding 802.1X and VoIP on EX Series Switches
- Understanding Q-in-Q Tunneling on EX Series Switches
- Understanding Unknown Unicast Forwarding on EX Series Switches
- Understanding MAC Notification on EX Series Switches
- Understanding FIP Snooping
- Understanding Nonstop Bridging on EX Series Switches

examine-dhcp

Syntax

```
(examine-dhcp | no-examine-dhcp) {
  forwarding-class class-name;
}
```

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

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

Description Enable DHCP snooping on all VLANs or on the specified VLAN.

NOTE: If you configure DHCP for all VLANs and you enable a different port security feature on a specific VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

- **examine-dhcp**—Enable DHCP snooping.
- **no-examine-dhcp**—Disable DHCP snooping.

When DHCP snooping is enabled, the switch logs DHCP packets (DHCPOFFER, DHCPDECLINE, DHCPACK, and DHCPNAK packets) that it receives on untrusted ports. You can monitor the log for these messages, which can signal the presence of a malicious DHCP server on the network.

TIP: For private VLANs (PVLANs), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from PVLAN trunk ports are not snooped.

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 Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 44
- Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 81

- Enabling DHCP Snooping (CLI Procedure) on page 92
- Enabling DHCP Snooping (J-Web Procedure) on page 94

forwarding-class

Syntax forwarding-class class *class-name*;

Hierarchy Level [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) (examine-dhcp |arp-inspection)]

Release Information Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description Assign a user-defined or a pre-defined forwarding class to the packets that have been checked for DHCP snooping or dynamic ARP inspection (DAI).

NOTE: To assign a user-defined class, you must first configure the user-defined class by using the forwarding-classes configuration statement at the [edit class-of-service] hierarchy level.

Default Disabled.

Options *class-name*—Name of the forwarding class. The forwarding class can be one of the pre-defined forwarding classes (best-effort, assured-forwarding, expedited-forwarding, network-control) or it can be a user-defined forwarding class.

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

Related Documentation

- Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 81
- Understanding Junos OS CoS Components for EX Series Switches
- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8
- Understanding DAI for Port Security on EX Series Switches on page 15

interface

Syntax

```
interface (all | interface-name) {
  allowed-mac {
    mac-address-list;
  }
  (dhcp-trusted | no-dhcp-trusted);
  fcoe-trusted;
  mac-limit limit action action;
  no-allowed-mac-log;
  static-ip  ip-address {
    vlan  vlan-name;
    mac mac-address;
  }
}
```

Hierarchy Level [edit ethernet-switching-options secure-access-port]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
static-ip introduced in Junos OS Release 9.2 for EX Series switches.
no-allowed-mac-log introduced in Junos OS Release 9.3 for EX Series switches.

Description Apply port security features to all interfaces or to the specified interface.

The statements are explained separately.

Options **all**—Apply port security features to all interfaces.

interface-name —Apply port security features to the specified interface.

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 48
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 34
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 41
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 38
- Configuring MAC Limiting (CLI Procedure) on page 100
- Enabling a Trusted DHCP Server (CLI Procedure) on page 95
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 111

ip-source-guard

Syntax (ip-source-guard | no-ip-source-guard);

Hierarchy Level [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.

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**—Disable IP source guard checking.

NOTE:

Before you configure IP source guard, be sure that you have:

Explicitly enabled DHCP snooping on the specific VLAN or specific VLANs on which you will configure IP source guard. See "Enabling DHCP Snooping (CLI Procedure)" on page 92. If you configure IP source guard on specific VLANs rather than on all VLANs, you must also enable DHCP snooping explicitly on those VLANs. Otherwise, the default value of no DHCP snooping applies to that VLAN.

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 on page 67
- Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 59
- Configuring IP Source Guard (CLI Procedure) on page 109

mac

Syntax mac *mac-address*;

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

Release Information Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Media access control (MAC) address, or hardware address, for the device connected to the specified interface.

Options ***mac-address*** —Value (in hexadecimal format) for 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) on page 111

mac-limit

Syntax mac-limit *limit* action *action*;

Hierarchy Level [edit ethernet-switching-options secure-access-port interface (all | *interface-name*)], [edit vlans *vlan-name*]

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

Description Specify the number of MAC addresses to dynamically add to the MAC address cache for this access interface (port) or VLAN and the action to be taken by the switch if the MAC address learning limit is exceeded on the interface (port) or VLAN. The MAC address learning limit varies depending on the switch model. Use the ? help with this command to determine the learning limit for a switch.

Default The default action is **drop**.

Options *limit*—Maximum number of MAC addresses (varies depending on switch model).

action *action*—(Optional) Action to take when the MAC address limit is exceeded:

- **drop**—Drop the packet and generate an alarm, an SNMP trap, or a system log entry. This is the default.
- **log**—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- **none**—No action.
- **shutdown**—Disable the interface or VLAN and generate an alarm. If you have configured the switch with the port-error-disable statement, the disabled interface or VLAN recovers automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces or VLAN by running the **clear ethernet-switching port-error** command.

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

Related Documentation

- allowed-mac on page 137
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 34
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 41
- Configuring MAC Limiting (CLI Procedure) on page 100
- Configuring MAC Limiting (J-Web Procedure) on page 103

- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118

mac-move-limit

Syntax mac-move-limit *limit* action *action*;

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
The default value for the **action** option was changed in Junos OS Release 9.5 for EX Series switches.
The **shutdown** option was modified in Junos OS Release 9.6 for EX Series switches.

Description Specify the number of times a MAC address can move to a new interface (port) in 1 second and the action to be taken by the switch if the MAC address move limit is exceeded.

Default The default move limit is unlimited. The default action is **drop**.

Options *limit*—Maximum number of moves to a new interface per second.

action *action*—(Optional) Action to take when the MAC address move limit is reached:

- **drop**—Drop the packet and generate an alarm, an SNMP trap, or a system log entry. This is the default.
- **log**—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- **none**—No action.
- **shutdown**—Disable the interface and generate an alarm. If you have configured the switch with the port-error-disable statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the **clear ethernet-switching port-error** command.

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

Related Documentation

- mac-limit on page 152
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Configuring MAC Move Limiting (CLI Procedure) on page 105
- Configuring MAC Move Limiting (J-Web Procedure) on page 107
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118

no-allowed-mac-log

Syntax no-allowed-mac-log;

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

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description Specify that the switch does not log messages when it receives packets from invalid MAC addresses on an interface that has been configured for particular (allowed) MAC addresses.

Default The switch logs messages when it receives packets from invalid MAC addresses on an interface that has been configured for particular (allowed) MAC addresses.

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

Related Documentation

- allowed-mac on page 137
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 48
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 41
- Configuring MAC Limiting (CLI Procedure) on page 100
- Configuring MAC Limiting (J-Web Procedure) on page 103

no-gratuitous-arp-request

Syntax no-gratuitous-arp-request;

Hierarchy Level [edit interfaces *interface-name*]

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

Description Configure the switch not to respond to gratuitous ARP requests. You can disable responses to gratuitous ARP requests on both Layer 2 Ethernet switching interfaces and routed VLAN interfaces (RVIs).

Default Gratuitous ARP responses are enabled on all Ethernet switching interfaces and RVIs.

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

Related Documentation

- Example: Configuring Proxy ARP on an EX Series Switch
- Configuring Proxy ARP (CLI Procedure)

port-error-disable

Syntax

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

Hierarchy Level [edit ethernet-switching-options]

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

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

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

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

Default Not enabled.

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

Related Documentation

- action-shutdown
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 118
- Configuring Port Security (CLI Procedure) on page 88

prefix

Syntax prefix hostname;

Hierarchy Level [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]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Configure an 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.

Default If **prefix** is not explicitly specified, no prefix is appended to the circuit ID. When **prefix** is specified, it is specified as **prefix hostname** (and the value is the hostname of the switch).

Options **hostname**—Name of the host system (the switch) that is forwarding or relaying the DHCP request from the DHCP client to the DHCP server.

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 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- [edit forwarding-options] Configuration Statement Hierarchy on page 136
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

prefix

Syntax prefix hostname | mac | none;

Hierarchy Level [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82 remote-id]
[edit forwarding-options helpers bootp dhcp-option82 remote-id]
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82 remote-id]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.

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

Default If **prefix** is not explicitly specified, no prefix is appended to the remote ID.

Options

hostname—Name of the host system (the switch) that is forwarding or relaying the DHCP request from the DHCP client to the DHCP server.

mac—MAC address of the host system (the switch) that is forwarding or relaying the DHCP request from the DHCP client to the DHCP server.

none—No prefix is applied to the remote ID.

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

Related Documentation

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- [edit forwarding-options] Configuration Statement Hierarchy on page 136
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

remote-id

Syntax

```
remote-id {
  prefix hostname | mac | none;
  use-interface-description;
  use-string string;
}
```

Hierarchy Level

[edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82]
[edit forwarding-options helpers bootp dhcp-option82]
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

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.

Default

If **remote-id** is not explicitly set, no remote ID value is inserted in the DHCP request packet header. If the **remote-id** option is specified but is not qualified by a keyword, the MAC address of the host device (the switch) is used as the remote ID.

Required Privilege Level

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

Related Documentation

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- [edit forwarding-options] Configuration Statement Hierarchy on page 136
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

secure-access-port

Syntax

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

Hierarchy Level [edit ethernet-switching-options]

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

Description Configure port security features, including MAC limiting, dynamic ARP inspection, whether interfaces can receive DHCP responses, DHCP snooping, IP source guard, DHCP option 82, MAC move limiting, and FIP snooping.

The remaining statements are explained separately.

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

Related Documentation

- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch on page 52
- Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 67
- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Configuring FIP Snooping and Priority-Based Flow Control on an FCoE Transit Switch

static-ip

Syntax

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

Hierarchy Level [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.

Description Static (fixed) IP address and static MAC address, with an associated VLAN, added to the DHCP snooping database.

Options ***ip-address***—IP 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) on page 111

timeout

Syntax timeout *seconds*;

Hierarchy Level [edit ethernet-switching-options secure-access-port dhcp-snooping-file]

Release Information Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description Specify a timeout value for remote read and write operations. This value determines the amount of time that the switch waits for a remote system to respond when the DHCP snooping database is stored on a remote FTP site.

Default None

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

Range: 10 through 3600

Required Privilege Level 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 EX Series Switches on page 8

traceoptions

Syntax

```
traceoptions {
  file filename <files number> <no-stamp> <replace> <size size> <world-readable |
    no-world-readable>;
  flag flag <disable>;
}
```

Hierarchy Level [edit ethernet-switching-options]

Release Information Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Define global tracing operations for access security features on Ethernet switches.

Default The **traceoptions** feature is disabled by default.

Options

disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

file *filename* —Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached (***x*k to specify KB, ***x*m to specify MB, or ***x*g to specify gigabytes), at which point the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- **access-security**—Trace access security events.
- **all**—All tracing operations.
- **config-internals**—Trace internal configuration operations.
- **forwarding-database**—Trace forwarding database and next-hop events.
- **general**—Trace general events.
- **interface**—Trace interface events.
- **ip-source-guard**—Trace IP source guard events.
- **krt**—Trace communications over routing sockets.
- **lib**—Trace library calls.
- **normal**—Trace normal events.

- **parse**—Trace reading of the configuration.
- **regex-parse**—Trace regular-expression parsing operations.
- **rtg**—Trace redundant trunk group events.
- **state**—Trace state transitions.
- **stp**—Trace spanning-tree events.
- **task**—Trace Ethernet-switching task processing.
- **timer**—Trace Ethernet-switching timer processing.
- **vlan**—Trace VLAN events.

no-stamp—(Optional) Do not timestamp the trace file.

Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Restrict file access to the user who created the file.

replace—(Optional) Replace an existing trace file if there is one rather than appending to it.

Default: If you do not include this option, tracing output is appended to an existing trace file.

size ***size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **files** option.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify gigabytes

Range: 10 KB through 1 gigabyte

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

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

Related Documentation

- Port Security for EX Series Switches Overview on page 3
- EX Series Switches Interfaces Overview
- Understanding IP Source Guard for Port Security on EX Series Switches on page 23
- Understanding Redundant Trunk Links on EX Series Switches
- Understanding STP for EX Series Switches
- Understanding Bridging and VLANs on EX Series Switches

use-interface-description

Syntax use-interface-description;

Hierarchy Level
[edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82 circuit-id]
[edit forwarding-options helpers bootp dhcp-option82 circuit-id]
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82 circuit-id]

[edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82 remote-id]
[edit forwarding-options helpers bootp dhcp-option82 remote-id]
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82 remote-id]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

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

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

Related Documentation

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- [edit forwarding-options] Configuration Statement Hierarchy on page 136
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

use-string

Syntax use-string *string*;

Hierarchy Level [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82 remote-id]
[edit forwarding-options helpers bootp dhcp-option82 remote-id]
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82 remote-id]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Use a string rather than the MAC address of the host system (the default) in the remote ID value in the DHCP option 82 information.

Options ***string***—Character string used as the remote ID value.

Range:1–255 characters

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

Related Documentation

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- [edit forwarding-options] Configuration Statement Hierarchy on page 136
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

use-vlan-id

Syntax use-vlan-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.

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

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- [edit forwarding-options] Configuration Statement Hierarchy on page 136
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

vendor-id

Syntax vendor-id <*string*>;

Hierarchy Level [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82]
[edit forwarding-options helpers bootp dhcp-option82]
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

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, 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, the default vendor ID **Juniper** is configured.

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

Related Documentation

- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Setting Up DHCP Option 82 with an EX Series Switch as Relay Agent Between Clients and a DHCP Server on page 74
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 115
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 112
- [edit forwarding-options] Configuration Statement Hierarchy on page 136

vlan

Syntax

```
vlan (all | vlan-name) {
  (arp-inspection | no-arp-inspection);
  dhcp-option82 {
    circuit-id {
      prefix hostname;
      use-interface-description;
      use-vlan-id;
    }
    remote-id {
      prefix hostname | mac | none;
      use-interface-description;
      use-string string;
    }
    vendor-id <string>;
  }
  (examine-dhcp | no-examine-dhcp);
  examine-fip {
    fc-map fc-map-value;
  }
  (ip-source-guard | no-ip-source-guard);
  mac-move-limit limit action action;
}
```

Hierarchy Level [edit ethernet-switching-options secure-access-port]

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

Description Apply any of the following security options to a VLAN:

- DHCP snooping
- DHCP option 82
- Dynamic ARP inspection (DAI)
- FIP snooping
- IP source guard
- MAC move limiting

The remaining statements are explained separately.

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

Options **all**—Apply the feature to all VLANs.

vlan-name—Apply the feature to the specified VLAN.

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

Related Documentation
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 59
- Example: Setting Up DHCP Option 82 on an EX Series Switch with No Relay Agent Between Clients and DHCP Server on page 77
- Example: Configuring FIP Snooping and Priority-Based Flow Control on an FCoE Transit Switch

vlan

Syntax vlan *vlan-name*;

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

Release Information Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Associate the static IP address with the specified VLAN associated with the specified interface.

Options ***vlan-name*** —Name of a specific VLAN associated with the specified interface.

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

Related Documentation
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 111

write-interval

Syntax write-interval *seconds*;

Hierarchy Level [edit ethernet-switching-options secure-access-port dhcp-snooping-file]

Release Information Statement introduced in Junos OS Release 9.4 for EX Series switches.

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

Default None

Options ***seconds***—Value in seconds.
Range: 60 through 86400

Required Privilege Level 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 EX Series Switches on page 8

CHAPTER 7

Operational Commands for Port Security

clear arp inspection statistics

Syntax clear arp inspection statistics
<interface *interface*>

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

Description Clear ARP inspection statistics.

Options none—Clears ARP statistics on all interfaces.

interface *interface-names*—(Optional) Clear ARP statistics on one or more interfaces.

Required Privilege Level clear

Related Documentation
- show arp inspection statistics on page 177
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Verifying That DAI Is Working Correctly on page 122

List of Sample Output clear arp inspection statistics on page 174

Output Fields This command produces no output.

Sample Output

clear arp inspection statistics

```
user@switch> clear arp inspection statistics
```

clear dhcp snooping binding

Syntax

clear dhcp snooping binding
<mac (all | *mac-address*)>
<vlan (all | *vlan-name*)>
<vlan (all | *vlan-name*) mac (all | *mac-address*)>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Clear the DHCP snooping database information.

Options

mac (all | ***mac-address***)—(Optional) Clear DHCP snooping information for the specified MAC address or all MAC addresses.

vlan (all | ***vlan-name***)—(Optional) Clear DHCP snooping information for the specified VLAN or all VLANs.

Required Privilege Level

clear

Related Documentation

- show dhcp snooping binding on page 178
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Verifying That DHCP Snooping Is Working Correctly on page 120

List of Sample Output

clear dhcp snooping binding on page 175

Output Fields

This command produces no output.

Sample Output

clear dhcp snooping binding

```
user@switch> clear dhcp snooping binding
```

clear dhcp snooping statistics

Syntax **clear dhcp snooping statistics**

Release Information Command introduced in Junos OS Release 9.4 for EX Series switches.

Description Clear all Dynamic Host Configuration Protocol (DHCP) snooping statistics.

Required Privilege Level view

Related Documentation
- show dhcp snooping statistics on page 179
- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8

List of Sample Output clear dhcp snooping statistics on page 176

Output Fields See show dhcp snooping statistics for an explanation of the output fields.

Sample Output

clear dhcp snooping statistics The following sample output displays the DHCP snooping statistics before and after the **clear dhcp snooping statistics** command is issued.

```
user@switch> show dhcp snooping statistics
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21

user@switch> clear dhcp snooping statistics

user@switch> show dhcp snooping statistics
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
```

show arp inspection statistics

Syntax show arp inspection statistics

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

Description Display ARP inspection statistics.

Required Privilege Level view

Related Documentation
- clear arp inspection statistics on page 174
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Verifying That DAI Is Working Correctly on page 122

List of Sample Output show arp inspection statistics on page 177

Output Fields Table 11 on page 177 lists the output fields for the **show arp inspection statistics** command. Output fields are listed in the approximate order in which they appear.

Table 11: show arp inspection statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which ARP inspection has been applied.	All levels
Packets received	Total number of packets total that underwent ARP inspection.	All levels
ARP inspection pass	Total number of packets that passed ARP inspection.	All levels
ARP inspection failed	Total number of packets that failed ARP inspection.	All levels

Sample Output

show arp inspection statistics

```
user@switch> show arp inspection statistics

Interface     Packets received     ARP inspection pass  ARP inspection failed
---------     ----------------     -------------------  --------------------
  ge-0/0/0                   0                       0                     0
  ge-0/0/1                   0                       0                     0
  ge-0/0/2                   0                       0                     0
  ge-0/0/3                   0                       0                     0
  ge-0/0/4                   0                       0                     0
  ge-0/0/5                   0                       0                     0
  ge-0/0/6                   0                       0                     0
  ge-0/0/7                 703                     701                     2
```

show dhcp snooping binding

Syntax show dhcp snooping binding

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

Description Display the DHCP snooping database information.

Required Privilege Level view

Related Documentation
- clear dhcp snooping binding on page 175
- Example: Configuring Basic Port Security Features on an EX Series Switch on page 27
- Verifying That DHCP Snooping Is Working Correctly on page 120

List of Sample Output show dhcp snooping binding on page 178

Output Fields Table 12 on page 178 lists the output fields for the **show dhcp snooping binding** command. Output fields are listed in the approximate order in which they appear.

Table 12: show dhcp snooping binding Output Fields

Field Name	Field Description	Level of Output
MAC Address	MAC address of the network device; bound to the IP address.	All levels
IP Address	IP address of the network device; bound to the MAC address.	All levels
Lease	Lease granted to the IP address.	All levels
Type	How the MAC address was acquired.	All levels
VLAN	VLAN name of the network device whose MAC address is shown.	All levels
Interface	Interface address (port).	All levels

Sample Output

show dhcp snooping binding

```
user@switch> show dhcp snooping binding

DHCP Snooping Information:
MAC Address             IP Address Lease   Type     VLAN    Interface
-----------------       ---------- -----   -------  ----    ---------
00:00:01:00:00:03       192.0.2.0  640     dynamic  guest    ge-0/0/12.0
00:00:01:00:00:04       192.0.2.1  720     dynamic  guest    ge-0/0/12.0
00:00:01:00:00:05       192.0.2.5  800     dynamic  guest    ge-0/0/13.0
```

show dhcp snooping statistics

Syntax **show dhcp snooping statistics**

Release Information Command introduced in Junos OS Release 9.4 for EX Series switches.

Description Display statistics for read and write operations to the DHCP snooping database.

Required Privilege Level view

Related Documentation
- clear dhcp snooping statistics on page 176
- Understanding DHCP Snooping for Port Security on EX Series Switches on page 8

List of Sample Output show dhcp snooping statistics on page 179

Output Fields Table 13 on page 179 lists the output fields for the **show dhcp snooping statistics** command. Output fields are listed in the approximate order in which they appear.

Table 13: show dhcp snooping statistics Output Fields

Field Name	Field Description
Successful Transfers	Number of entries successfully transferred from memory to the DHCP snooping database.
Successful Reads	Number of entries successfully read from memory to the DHCP snooping database.
Successful Writes	Number of entries successfully written from memory to the DHCP snooping database.
Failed Transfers	Number of entries that failed being transferred from memory to the DHCP snooping database.
Failed Reads	Number of entries that failed being read from memory to the DHCP snooping database.
Failed Writes	Number of entries that failed being written from memory to the DHCP snooping database.

Sample Output

show dhcp snooping statistics

```
user@switch> show dhcp snooping statistics
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
```

show ethernet-switching table

Syntax

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

Release Information

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

Description

Display the Ethernet switching table.

Options

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

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

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

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

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

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

Required Privilege Level

view

Related Documentation

- clear ethernet-switching table
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch
- Example: Setting Up Bridging with Multiple VLANs for EX Series Switches
- Example: Setting Up Q-in-Q Tunneling on EX Series Switches

List of Sample Output

show ethernet-switching table on page 181
show ethernet-switching table brief on page 182
show ethernet-switching table detail on page 182
show ethernet-switching table extensive on page 183
show ethernet-switching table interface ge-0/0/1 on page 183

Output Fields

Table 14 on page 181 lists the output fields for the **show ethernet-switching table** command. Output fields are listed in the approximate order in which they appear.

Table 14: show ethernet-switching table Output Fields

Field Name	Field Description	Level of Output
VLAN	The name of a VLAN.	All levels
Tag	The VLAN ID tag name or number.	**extensive**
MAC or **MAC address**	The MAC address associated with the VLAN.	All levels
Type	The type of MAC address. Values are: • **static**—The MAC address is manually created. • **learn**—The MAC address is learned dynamically from a packet's source MAC address. • **flood**—The MAC address is unknown and flooded to all members.	All levels
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.	All levels
Interfaces	Interface associated with learned MAC addresses or **All-members** (flood entry).	All levels
Learned	For learned entries, the time which the entry was added to the Ethernet switching table.	**detail**, **extensive**
Nexthop index	The next-hop index number.	**detail**, **extensive**

Sample Output

show ethernet-switching table

```
user@switch> show ethernet-switching table
Ethernet-switching table: 57 entries, 17 learned
  VLAN              MAC address       Type         Age Interfaces
  F2                *                 Flood          - All-members
  F2                00:00:05:00:00:03 Learn          0 ge-0/0/44.0
  F2                00:19:e2:50:7d:e0 Static         - Router
  Linux             *                 Flood          - All-members
  Linux             00:19:e2:50:7d:e0 Static         - Router
  Linux             00:30:48:90:54:89 Learn          0 ge-0/0/47.0
  T1                *                 Flood          - All-members
  T1                00:00:05:00:00:01 Learn          0 ge-0/0/46.0
  T1                00:00:5e:00:01:00 Static         - Router
  T1                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T1                00:19:e2:50:7d:e0 Static         - Router
  T10               *                 Flood          - All-members
  T10               00:00:5e:00:01:09 Static         - Router
  T10               00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T10               00:19:e2:50:7d:e0 Static         - Router
  T111              *                 Flood          - All-members
  T111              00:19:e2:50:63:e0 Learn          0 ge-0/0/15.0
  T111              00:19:e2:50:7d:e0 Static         - Router
  T111              00:19:e2:50:ac:00 Learn          0 ge-0/0/15.0
  T2                *                 Flood          - All-members
  T2                00:00:5e:00:01:01 Static         - Router
  T2                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T2                00:19:e2:50:7d:e0 Static         - Router
  T3                *                 Flood          - All-members
```

```
  T3                00:00:5e:00:01:02 Static         - Router
  T3                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T3                00:19:e2:50:7d:e0 Static         - Router
  T4                *                 Flood          - All-members
  T4                00:00:5e:00:01:03 Static         - Router
  T4                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
[output truncated]
```

show ethernet-switching table brief

```
user@switch> show ethernet-switching table brief
Ethernet-switching table: 57 entries, 17 learned
  VLAN              MAC address       Type          Age Interfaces
  F2                *                 Flood           - All-members
  F2                00:00:05:00:00:03 Learn           0 ge-0/0/44.0
  F2                00:19:e2:50:7d:e0 Static          - Router
  Linux             *                 Flood           - All-members
  Linux             00:19:e2:50:7d:e0 Static          - Router
  Linux             00:30:48:90:54:89 Learn           0 ge-0/0/47.0
  T1                *                 Flood           - All-members
  T1                00:00:05:00:00:01 Learn           0 ge-0/0/46.0
  T1                00:00:5e:00:01:00 Static          - Router
  T1                00:19:e2:50:63:e0 Learn           0 ge-0/0/46.0
  T1                00:19:e2:50:7d:e0 Static          - Router
  T10               *                 Flood           - All-members
  T10               00:00:5e:00:01:09 Static          - Router
  T10               00:19:e2:50:63:e0 Learn           0 ge-0/0/46.0
  T10               00:19:e2:50:7d:e0 Static          - Router
  T111              *                 Flood           - All-members
  T111              00:19:e2:50:63:e0 Learn           0 ge-0/0/15.0
  T111              00:19:e2:50:7d:e0 Static          - Router
  T111              00:19:e2:50:ac:00 Learn           0 ge-0/0/15.0
  T2                *                 Flood           - All-members
  T2                00:00:5e:00:01:01 Static          - Router
  T2                00:19:e2:50:63:e0 Learn           0 ge-0/0/46.0
  T2                00:19:e2:50:7d:e0 Static          - Router
  T3                *                 Flood           - All-members
  T3                00:00:5e:00:01:02 Static          - Router
  T3                00:19:e2:50:63:e0 Learn           0 ge-0/0/46.0
  T3                00:19:e2:50:7d:e0 Static          - Router
  T4                *                 Flood           - All-members
  T4                00:00:5e:00:01:03 Static          - Router
  T4                00:19:e2:50:63:e0 Learn           0 ge-0/0/46.0
[output truncated]
```

show ethernet-switching table detail

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

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

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

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

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

show ethernet-switching table extensive

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

    VLAN: v1, Tag: 10, MAC: *, Interface: All-members
    Interfaces:
                ge-0/0/14.0, ge-0/0/1.0, ge-0/0/2.0, ge-0/0/3.0, ge-0/0/4.0,
                ge-0/0/5.0, ge-0/0/6.0, ge-0/0/7.0, ge-0/0/8.0, ge-0/0/10.0,
                ge-0/0/0.0
    Type: Flood
    Nexthop index: 567

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

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

show ethernet-switching table interface ge-0/0/1

```
user@switch> show ethernet-switching table interface ge-0/0/1
Ethernet-switching table: 1 unicast entries
  VLAN              MAC address       Type         Age Interfaces
  V1                *                 Flood          - All-members
  V1                00:00:05:00:00:05 Learn          0 ge-0/0/1.0
```

show ip-source-guard

Syntax **show ip-source-guard**

Release Information Command introduced in Junos OS Release 9.2 for EX Series switches.

Description Display IP source guard database information.

Required Privilege Level view

Related Documentation

- Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 67
- Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 59
- Verifying That IP Source Guard Is Working Correctly on page 128

List of Sample Output show ip-source-guard on page 184

Output Fields Table 15 on page 184 lists the output fields for the **show ip-source-guard** command. Output fields are listed in the approximate order in which they appear.

Table 15: show ip-source-guard Output Fields

Field Name	Field Description
VLAN	VLAN on which IP source guard is enabled.
Interface	Access interface associated with the VLAN in column 1.
Tag	VLAN ID for the VLAN in column 1. Possible values are: • 0, indicating the VLAN is not tagged. • 1 – 4093
IP Address	Source IP address for a device connected to the interface in column 2. A value of * (star, or asterisk) indicates that IP source guard is not enabled on this VLAN but the interface is shared with a VLAN that is enabled for IP source guard.
MAC Address	Source MAC address for a device connected to the interface in column 2. A value of * (star, or asterisk) indicates that IP source guard is not enabled on this VLAN but the interface is shared with a VLAN that is enabled for IP source guard.

Sample Output

show ip-source-guard

```
user@switch> show ip-source-guard
IP source guard information:
Interface    Tag  IP Address   MAC Address        VLAN

ge-0/0/12.0  0    10.10.10.7   00:30:48:92:A5:9D  vlan100
```

```
ge-0/0/13.0  0    10.10.10.9   00:30:48:8D:01:3D  vlan100
ge-0/0/13.0  100  *            *                  voice
```