



---

# Junos<sup>®</sup> OS for EX Series Ethernet Switches

## Port Security on EX Series Switches

Release

14.1X53



---

Published: 2014-12-18

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

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

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

*Junos<sup>®</sup> OS for EX Series Ethernet Switches Port Security on EX Series Switches*  
Release 14.1X53  
Copyright © 2014, Juniper Networks, Inc.  
All rights reserved.

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

#### YEAR 2000 NOTICE

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

#### END USER LICENSE AGREEMENT

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

# Table of Contents

	About the Documentation . . . . .	xv
	Documentation and Release Notes . . . . .	xv
	Supported Platforms . . . . .	xv
	Using the Examples in This Manual . . . . .	xv
	Merging a Full Example . . . . .	xvi
	Merging a Snippet . . . . .	xvi
	Documentation Conventions . . . . .	xvii
	Documentation Feedback . . . . .	xix
	Requesting Technical Support . . . . .	xix
	Self-Help Online Tools and Resources . . . . .	xix
	Opening a Case with JTAC . . . . .	xx
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Security Features Overview . . . . .</b>	<b>3</b>
	Security Features for EX Series Switches Overview . . . . .	3
<b>Chapter 2</b>	<b>Port Security Overview . . . . .</b>	<b>7</b>
	Understanding Port Security . . . . .	7
	Understanding How to Protect Access Ports on EX Series Switches from	
	Common Attacks . . . . .	9
	Mitigation of Ethernet Switching Table Overflow Attacks . . . . .	10
	Mitigation of Rogue DHCP Server Attacks . . . . .	10
	Protection Against ARP Spoofing Attacks . . . . .	11
	Protection Against DHCP Snooping Database Alteration Attacks . . . . .	11
	Protection Against DHCP Starvation Attacks . . . . .	11
	Understanding DHCP Snooping for Port Security . . . . .	12
	DHCP Snooping Basics . . . . .	13
	DHCP Snooping Process . . . . .	14
	DHCPv6 Snooping . . . . .	14
	Rapid Commit for DHCPv6 . . . . .	15
	DHCP Server Access . . . . .	15
	Switching Device, DHCP Clients, and DHCP Server Are All on the Same	
	VLAN . . . . .	16
	Switching Device Acts as DHCP Server . . . . .	17
	Switching Device Acts as Relay Agent . . . . .	18
	Static IP Address Additions to the DHCP Snooping Database . . . . .	19
	Snooping DHCP Packets That Have Invalid IP Addresses . . . . .	19
	Prioritizing Snooped Packets . . . . .	20

Understanding DAI for Port Security . . . . .	20
Address Resolution Protocol . . . . .	20
ARP Spoofing . . . . .	21
Dynamic ARP Inspection . . . . .	21
Prioritizing Inspected Packets . . . . .	22
Understanding IPv6 Neighbor Discovery Inspection . . . . .	23
Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches . . . . .	24
MAC Limiting for Port Security by Limiting the Number of MAC Addresses That Can be Learned on Interfaces . . . . .	24
MAC Limiting for Port Security by Specifying MAC Addresses That Are Allowed to Access Interfaces . . . . .	25
MAC Move Limiting for Port Security by Monitoring MAC Address Moves within VLANs . . . . .	25
Understanding Media Access Control Security (MACsec) . . . . .	26
How MACsec Works . . . . .	26
Understanding Connectivity Associations and Secure Channels . . . . .	27
Understanding MACsec Security Modes . . . . .	27
Understanding Static Connectivity Association Key Security Mode (Recommended Security Mode for Switch-to-Switch Links) . . . . .	27
Understanding Dynamic Secure Association Key Security Mode (Switch-to-Host Links) . . . . .	28
Understanding Static Secure Association Key Security Mode (Supported for Switch-to-Switch Links) . . . . .	29
Understanding the Requirements to Enable MACsec on a Switch-to-Host Link . . . . .	29
Understanding MACsec Hardware Requirements for EX Series and QFX Series Switches . . . . .	30
Understanding MACsec Software Requirements for EX Series and QFX Series Switches . . . . .	30
Understanding the MACsec Feature License Requirement . . . . .	31
MACsec Limitations . . . . .	31
Understanding Trusted DHCP Servers for Port Security . . . . .	32
Understanding IP Source Guard for Port Security on EX Series Switches . . . . .	32
IP Address Spoofing . . . . .	32
How IP Source Guard Works . . . . .	32
IPv6 Source Guard . . . . .	33
The DHCP Snooping Table . . . . .	33
Typical Uses of Other Junos OS Features with IP Source Guard . . . . .	34
Understanding DHCP Option 82 for Port Security on Switching Devices . . . . .	35
DHCP Option 82 Processing . . . . .	35
Suboption Components of Option 82 . . . . .	36
Switching Device Configurations That Support Option 82 . . . . .	37
Switching Device, DHCP Clients, and the DHCP Server Are on the Same VLAN or Bridge Domain . . . . .	37
Switching Device Acts as a Relay Agent . . . . .	37
DHCPv6 Options . . . . .	38
Understanding Persistent MAC Learning (Sticky MAC) . . . . .	39

<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Configuration Examples</b>	<b>43</b>
	Example: Configuring Basic Port Security Features	43
	Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks	51
	Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks	54
	Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks	58
	Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks	61
	Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks	66
	Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch	69
	Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces	77
	Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN	87
	Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing	94
	Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server	98
	Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server	101
	Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic	104
<b>Chapter 4</b>	<b>Configuration Tasks</b>	<b>109</b>
	Configuring Port Security (CLI Procedure)	110
	Enabling DHCP Snooping	110
	Enabling Dynamic ARP Inspection (DAI)	111
	Enabling IPv6 Neighbor Discovery Inspection	111
	Limiting Dynamic MAC Addresses on an Interface	111
	Enabling Persistent MAC Learning on an Interface	112
	Limiting MAC Address Movement	112
	Configuring Trusted DHCP Servers on an Interface	112
	Configuring Port Security (J-Web Procedure)	112
	Configuring Media Access Control Security (MACsec)	116
	Acquiring and Downloading the Junos OS Software	117
	Acquiring and Downloading the MACsec Feature License	118
	Configuring the PIC Mode of the MACsec-capable Interfaces (EX4200 switches only)	119
	Configuring MACsec Using Static Connectivity Association Key Security Mode (Recommended for Enabling MACsec on Switch-to-Switch Links)	120
	Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link	124

Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link . . . . .	128
Enabling DHCP Snooping (CLI Procedure) . . . . .	132
Enabling DHCP Snooping . . . . .	133
Applying CoS Forwarding Classes to Prioritize Snooped Packets . . . . .	133
Enabling DHCP Snooping (J-Web Procedure) . . . . .	135
Enabling a Trusted DHCP Server (CLI Procedure) . . . . .	136
Enabling a Trusted DHCP Server (J-Web Procedure) . . . . .	136
Enabling Dynamic ARP Inspection (CLI Procedure) . . . . .	137
Enabling DAI . . . . .	138
Applying CoS Forwarding Classes to Prioritize Inspected Packets . . . . .	138
Enabling Dynamic ARP Inspection (J-Web Procedure) . . . . .	139
Configuring MAC Limiting (CLI Procedure) . . . . .	140
Configuring MAC Limiting for Port Security by Limiting the Number of MAC Addresses That Can be Learned on Interfaces . . . . .	140
Configuring MAC Limiting for Port Security by Specifying MAC Addresses That Are Allowed . . . . .	141
Configuring MAC Limiting for VLANs . . . . .	141
Configuring MAC Limiting (J-Web Procedure) . . . . .	143
Configuring MAC Move Limiting (CLI Procedure) . . . . .	145
Configuring MAC Move Limiting (J-Web Procedure) . . . . .	147
Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure) . . . . .	148
Configuring IP Source Guard (CLI Procedure) . . . . .	148
Configuring IP Source Guard . . . . .	149
Configuring IPv6 Source Guard . . . . .	150
Disabling IP Source Guard . . . . .	151
Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) . . . . .	152
Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) . . . . .	153
Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) . . . . .	156
Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) . . . . .	159
Configuring Persistent MAC Learning (CLI Procedure) . . . . .	159
Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) . . . . .	161

<b>Chapter 5</b>	<b>Configuration Statements</b>	<b>163</b>
	[edit ethernet-switching-options] Configuration Statement Hierarchy on EX Series Switches	165
	Supported Statements in the [edit ethernet-switching-options] Hierarchy Level	165
	Unsupported Statements in the [edit ethernet-switching-options] Hierarchy Level	168
	[edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches	168
	Supported Statements in the [edit forwarding-options] Hierarchy Level	168
	Unsupported Statements in the [edit forwarding-options] Hierarchy Level	170
	[edit security] Configuration Statement Hierarchy on EX Series Switches	172
	Supported Statements in the [edit security] Hierarchy Level	172
	Unsupported Statements in the [edit security] Hierarchy Level	175
	allowed-mac	176
	arp-inspection	177
	cak	178
	circuit-id	179
	ckn	180
	connectivity-association	181
	connectivity-association (MACsec Interfaces)	182
	direction	183
	dhcp-option82	184
	dhcp-snooping-file	185
	dhcp-trusted	186
	disable-timeout	187
	encryption	188
	ethernet-switching-options	189
	examine-dhcp	193
	examine-dhcpv6	195
	exclude-protocol	196
	forwarding-class (for DHCP Snooping or DAI Packets)	197
	id	198
	include-sci	199
	interface (Access Port Security)	200
	interfaces (MACsec)	201
	ip-source-guard	202
	ipv6-source-guard-sessions	203
	key	204
	key-server-priority	205
	location (DHCP Snooping Database)	206
	mac	207
	mac-address (MACsec)	208
	mac-limit (Access Port Security)	209
	mac-move-limit	211
	macsec	213
	mka	214
	must-secure	215

no-allowed-mac-log	216
no-encryption	217
no-examine-dhcpv6	218
no-gratuitous-arp-request	219
no-option-37	219
offset	220
persistent-learning	221
port-error-disable	222
port-id	223
pre-shared-key	224
prefix (Circuit ID for Option 82)	225
prefix (Remote ID for Option 82)	227
remote-id	228
replay-protect	229
replay-window-size	230
secure-access-port	231
secure-channel	233
security-association	234
security-mode	235
static-ip	236
timeout	237
traceoptions (Access Port Security)	238
transmit-interval (MACsec)	240
use-interface-description	241
use-string	243
use-vlan-id	244
vendor-id	245
vlan (Access Port Security)	247
vlan (DHCP Bindings on Access Ports)	249
write-interval	250

## Part 3

### Chapter 6

## Administration

<b>Routine Monitoring</b>	<b>253</b>
Monitoring Port Security	253
Verifying That DHCP Snooping Is Working Correctly	255
Verifying That a Trusted DHCP Server Is Working Correctly	256
Verifying That DAI Is Working Correctly	256
Verifying That MAC Limiting Is Working Correctly	257
Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly	258
Verifying That MAC Limiting for a Specific Interface Within a Specific VLAN Is Working Correctly	258
Verifying That Allowed MAC Addresses Are Working Correctly	259
Verifying Results of Various Action Settings When the MAC Limit Is Exceeded	259
Customizing the Ethernet Switching Table Display to View Information for a Specific Interface	261
Verifying That MAC Move Limiting Is Working Correctly	262



	Verifying That IP Source Guard Is Working Correctly . . . . .	263
	Verifying That the Port Error Disable Setting Is Working Correctly . . . . .	263
	Verifying That Persistent MAC Learning Is Working Correctly . . . . .	264
<b>Chapter 7</b>	<b>Operational Commands . . . . .</b>	<b>267</b>
	clear arp inspection statistics . . . . .	268
	clear dhcp snooping binding . . . . .	269
	clear dhcp snooping statistics . . . . .	270
	clear dhcpv6 snooping binding . . . . .	271
	clear dhcpv6 snooping statistics . . . . .	272
	clear dot1x . . . . .	273
	clear neighbor-discovery-inspection statistics . . . . .	275
	clear security mka statistics . . . . .	276
	show arp inspection statistics . . . . .	277
	show dhcp snooping binding . . . . .	278
	show dhcp snooping statistics . . . . .	280
	show dhcpv6 snooping binding . . . . .	281
	show dhcpv6 snooping statistics . . . . .	283
	show ethernet-switching table . . . . .	284
	show ip-source-guard . . . . .	289
	show ipv6-source-guard . . . . .	291
	show neighbor-discovery-inspection statistics . . . . .	293
	show security macsec connections . . . . .	294
	show security macsec statistics . . . . .	296
	show security mka sessions . . . . .	300
	show security mka statistics . . . . .	302
	show system statistics arp . . . . .	304
<b>Part 4</b>	<b>Troubleshooting</b>	
<b>Chapter 8</b>	<b>Troubleshooting Procedures . . . . .</b>	<b>307</b>
	Troubleshooting Port Security . . . . .	307
	MAC Addresses That Exceed the MAC Limit or MAC Move Limit Are Not Listed in the Ethernet Switching Table . . . . .	307
	Multiple DHCP Server Packets Have Been Received on Untrusted Interfaces . . . . .	307



# List of Figures

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 2</b>	<b>Port Security Overview</b>	<b>7</b>
	Figure 1: DHCP Server Connected Directly to a Switching Device	16
	Figure 2: DHCP Server Connected Directly to Switching Device 2, with Switching Device 2 Connected to Switching Device 1 Through a Trusted Trunk Port	17
	Figure 3: Switching Device Is the DHCP Server	18
	Figure 4: Switching Device Acting as Relay Agent Through Router to DHCP Server	19
	Figure 5: DHCP Clients, Switching Device, and the DHCP Server Are All on the Same VLAN or Bridge Domain	37
	Figure 6: Switching Device Acting as an Extended Relay Server	38
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Configuration Examples</b>	<b>43</b>
	Figure 7: Network Topology for Basic Port Security	45
	Figure 8: Network Topology for Basic Port Security	52
	Figure 9: Network Topology for Basic Port Security	56
	Figure 10: Network Topology for Basic Port Security	59
	Figure 11: Network Topology for Basic Port Security	63
	Figure 12: Network Topology for Basic Port Security	67
	Figure 13: Network Topology for Port Security Setup with Two Switches on the Same VLAN	71
	Figure 14: Network Topology for Basic Port Security	95
	Figure 15: Network Topology for Configuring DHCP Option 82 on a Switch That Is on the Same VLAN as the DHCP Clients and the DHCP Server	102
	Figure 16: Network Topology for Using CoS Forwarding Classes to Prioritize Snooped and Inspected Packets	106



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>xv</b>
	Table 1: Notice Icons . . . . .	xvii
	Table 2: Text and Syntax Conventions . . . . .	xvii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 2</b>	<b>Port Security Overview</b> . . . . .	<b>7</b>
	Table 3: DHCPv6 Messages and Equivalent DHCPv4 Messages . . . . .	15
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Configuration Examples</b> . . . . .	<b>43</b>
	Table 4: Components of the Port Security Topology . . . . .	45
	Table 5: Components of the Port Security Topology . . . . .	52
	Table 6: Components of the Port Security Topology . . . . .	56
	Table 7: Components of the Port Security Topology . . . . .	59
	Table 8: Components of the Port Security Topology . . . . .	63
	Table 9: Components of the Port Security Topology . . . . .	67
	Table 10: Components of Port Security Setup on Switch 1 with a DHCP Server Connected to Switch 2 . . . . .	71
	Table 11: Components of the Port Security Topology . . . . .	95
	Table 12: Components of the Topology for Using CoS Forwarding Classes to Prioritize Snooped and Inspected Packets . . . . .	106
<b>Chapter 4</b>	<b>Configuration Tasks</b> . . . . .	<b>109</b>
	Table 13: Port Security Settings on VLANs . . . . .	113
	Table 14: Port Security on Interfaces . . . . .	115
<b>Chapter 5</b>	<b>Configuration Statements</b> . . . . .	<b>163</b>
	Table 15: Unsupported [edit forwarding-options] Configuration Statements on EX Series Switches . . . . .	170
	Table 16: Unsupported [edit security] Configuration Statements on EX Series Switches . . . . .	175
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 7</b>	<b>Operational Commands</b> . . . . .	<b>267</b>
	Table 17: show arp inspection statistics Output Fields . . . . .	277
	Table 18: show dhcp snooping binding Output Fields . . . . .	278
	Table 19: show dhcp snooping statistics Output Fields . . . . .	280
	Table 20: show dhcp snooping binding Output Fields . . . . .	281
	Table 21: show dhcpv6 snooping statistics Output Fields . . . . .	283

Table 22: show ethernet-switching table Output Fields . . . . .	285
Table 23: show ip-source-guard Output Fields . . . . .	289
Table 24: show ipv6-source-guard Output Fields . . . . .	291
Table 25: show neighbor-discovery-inspection statistics Output Fields . . . . .	293
Table 26: show security macsec connections Output Fields . . . . .	294
Table 27: show security macsec statistics Output Fields . . . . .	296
Table 28: show security mka sessions Output Fields . . . . .	300
Table 29: show security mka statistics Output Fields . . . . .	302

# About the Documentation

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

## Documentation and Release Notes

---

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

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

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

## Supported Platforms

---

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

- EX Series

## Using the Examples in This Manual

---

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

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

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

## Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

## Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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



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

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

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

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

## Documentation Conventions

Table 1 on page xvii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xvii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

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

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

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

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

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

## Requesting Technical Support

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

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

## Self-Help Online Tools and Resources

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

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

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

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

## Opening a Case with JTAC

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

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

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

## PART 1

# Overview

- [Security Features Overview on page 3](#)
- [Port Security Overview on page 7](#)



## CHAPTER 1

# Security Features Overview

- [Security Features for EX Series Switches Overview on page 3](#)

## Security Features for EX Series Switches Overview

---

Juniper Networks Junos operating system (Junos OS) is a network operating system that has been hardened through the separation of control forwarding and services planes, with each function running in protected memory. The control-plane CPU is protected by rate limiting, routing policy, and firewall filters to ensure switch uptime even under severe attack. Access port security features such as dynamic Address Resolution Protocol (ARP) inspection, DHCP snooping, and MAC limiting are controlled through a single Junos OS CLI command.

Juniper Networks EX Series Ethernet Switches provide the following hardware and software security features:

**Console Port**—Allows use of the console port to connect to the Routing Engine through an RJ-45 cable. You then use the command-line interface (CLI) to configure the switch.

**Out-of-Band Management**—A dedicated management Ethernet port on the rear panel allows out-of-band management.

**Software Images**—All Junos OS images are signed by Juniper Networks certificate authority (CA) with public key infrastructure (PKI).

**User Authentication, Authorization, and Accounting (AAA)**—Features include:

- User and group accounts with password encryption and authentication.
- Access privilege levels configurable for login classes and user templates.
- RADIUS authentication, TACACS+ authentication, or both, for authenticating users who attempt to access the switch.
- Auditing of configuration changes through system logging or RADIUS/TACACS+.

**802.1X Authentication**—Provides network access control. Supplicants (hosts) are authenticated when they initially connect to a LAN. Authenticating supplicants before they receive an IP address from a DHCP server prevents unauthorized supplicants from gaining access to the LAN. EX Series switches support Extensible Authentication Protocol (EAP) methods, including EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP.

**Port Security**—Access port security features include:

- 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).
- 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.
- MAC limiting—Protects against flooding of the Ethernet switching table.
- MAC move limiting—Detects MAC movement and MAC spoofing on access ports.
- Trusted DHCP server—With a DHCP server on a trusted port, protects against rogue DHCP servers sending leases.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. 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 (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.
- Unrestricted proxy ARP—The switch responds to all ARP messages with its own MAC address. Hosts that are connected to the switch's interfaces cannot communicate directly with other hosts. Instead, all communications between hosts go through the switch.
- Restricted proxy ARP—The switch does not respond to an ARP request if the physical networks of the source and target of the ARP request are the same. It does not matter whether the destination host has the same IP address as the incoming interface or a different (remote) IP address. An ARP request for a broadcast address elicits no reply.

**Device Security**—Storm control permits the switch to monitor unknown unicast and broadcast traffic and drop packets, or shut down, or temporarily disable the interface when a specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. You can enable storm control on access interfaces or trunk interfaces.

**Firewall Filters**—Allow auditing of various types of security violations, including attempts to access the switch from unauthorized locations. Firewall filters can detect such attempts and create audit log entries when they occur. The filters can also restrict access by limiting traffic to source and destination MAC addresses, specific protocols, or, in combination with policers, to specified data rates to prevent denial of service (DoS) attacks.

**Policers**—Provide rate-limiting capability to control the amount of traffic that enters an interface, which acts to counter DoS attacks.



**Encryption Standards**—Supported standards include:

- 128-, 192-, and 256-bit Advanced Encryption Standard (AES)
- 56-bit Data Encryption Standard (DES) and 168-bit 3DES

**Related  
Documentation**

- *802.1X for EX Series Switches Overview*
- *Firewall Filters for EX Series Switches Overview*
- [Understanding Port Security on page 7](#)
- *Understanding Proxy ARP on EX Series Switches*
- *Understanding Storm Control on EX Series Switches*
- *Understanding the Use of Policers in Firewall Filters*
- *Understanding Centralized Network Access Control and EX Series Switches*



## CHAPTER 2

# Port Security Overview

- [Understanding Port Security on page 7](#)
- [Understanding How to Protect Access Ports on EX Series Switches from Common Attacks on page 9](#)
- [Understanding DHCP Snooping for Port Security on page 12](#)
- [Understanding DAI for Port Security on page 20](#)
- [Understanding IPv6 Neighbor Discovery Inspection on page 23](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 24](#)
- [Understanding Media Access Control Security \(MACsec\) on page 26](#)
- [Understanding Trusted DHCP Servers for Port Security on page 32](#)
- [Understanding IP Source Guard for Port Security on EX Series Switches on page 32](#)
- [Understanding DHCP Option 82 for Port Security on Switching Devices on page 35](#)
- [Understanding Persistent MAC Learning \(Sticky MAC\) on page 39](#)

## Understanding Port Security

---

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

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

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

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

Port security features supported on switching devices are:

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



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

- DHCPv6 snooping—DHCP snooping for IPv6.
- DHCP option 82—Also known as the DHCP Relay Agent Information option. This DHCPv4 feature helps protect the switching device against attacks such as spoofing of IP addresses and MAC addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.
- DHCPv6 option 37—Option 37 is the remote ID option for DHCPv6 and is used to insert information about the network location of the remote host into DHCPv6 packets. You enable option 37 on a VLAN.



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

- DHCPv6 option 18—Option 18 is the circuit ID option for DHCPv6 and is used to insert information about the client port into DHCPv6 packets. This option includes other details that can be optionally configured, such as the prefix and the interface description.
- DHCPv6 option 16—Option 16 is the vendor ID option for DHCPv6 and is used to insert information about the vendor of the client hardware into DHCPv6 packets.
- Dynamic ARP inspection (DAI)—Prevents Address Resolution Protocol (ARP) spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable DAI on a VLAN.
- IPv6 neighbor discovery inspection—Prevents IPv6 address spoofing attacks. Neighbor discovery requests and replies are compared against entries in the DHCPv6 snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable neighbor discovery inspection on a VLAN.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. With IP source guard enabled, the source IP address in the packet sent from an untrusted access interface is validated against the DHCP snooping database. If the packet cannot be validated, it is discarded. You enable IP source guard on a VLAN or bridge domain.



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

- IPv6 source guard—IP source guard for IPv6.



**NOTE:** IPv6 source guard is not supported on the QFX Series.

- MAC limiting—Protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You can enable MAC limiting on an interface.
- MAC move limiting—(Not supported on EX9200) Tracks MAC movement and detects MAC spoofing on access ports. You enable this feature on a VLAN or bridge domain.
- Persistent MAC learning—Also known as sticky MAC. Persistent MAC learning enables interfaces to retain dynamically learned MAC addresses across switch reboots. You enable this feature on an interface.
- Trusted DHCP server—Configuring the DHCP server on a trusted port protects against rogue DHCP servers sending leases. You enable this feature on an interface (port). By default, access ports are untrusted, and trunk ports are trusted. (Access ports are the switch ports that connect to Ethernet endpoints such as user PCs and laptops, servers, and printers. Trunk ports are the switch ports that connect an Ethernet switch to other switches or to routers.)

#### Related Documentation

- [Security Features for EX Series Switches Overview on page 3](#)
- [Understanding DHCP Snooping for Port Security on page 12](#)
- [\*Understanding DHCP Snooping for Port Security\*](#)
- [Understanding IPv6 Neighbor Discovery Inspection on page 23](#)
- [Understanding DAI for Port Security on page 20](#)
- [Understanding IP Source Guard for Port Security on EX Series Switches on page 32](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 24](#)
- [Understanding DHCP Option 82 for Port Security on Switching Devices on page 35](#)

## 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 10](#)
- [Mitigation of Rogue DHCP Server Attacks on page 10](#)
- [Protection Against ARP Spoofing Attacks on page 11](#)
- [Protection Against DHCP Snooping Database Alteration Attacks on page 11](#)
- [Protection Against DHCP Starvation Attacks on page 11](#)

## 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 limiting 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 51.



**NOTE:** You can also configure learned MAC addresses to persist on each interface. Used in combination with a configured MAC limit, this persistent MAC learning helps prevent traffic loss after a restart or an interface-down event and also increases port security by limiting the MAC addresses allowed on the interface.

## 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 54.



**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 61.

## 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 66.

## 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 58.](#)



**NOTE:** For additional protection, you can configure learned MAC addresses on each interface to persist across restarts of the switch by enabling persistent MAC learning. This persistent MAC learning both helps to prevent traffic loss after a restart and ensures that even after a restart or an interface-down event, the persistent MAC addresses are re-entered into the forwarding database rather than the switch learning new MAC addresses.

#### Related Documentation

- [Understanding DHCP Snooping for Port Security on page 12](#)
- [Understanding DAI for Port Security on page 20](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 24](#)
- [Understanding Trusted DHCP Servers for Port Security on page 32](#)
- [Configuring Port Security \(CLI Procedure\) on page 110](#)
- [Configuring Port Security \(J-Web Procedure\) on page 112](#)

---

## Understanding DHCP Snooping for Port Security

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

- [DHCP Snooping Basics on page 13](#)
- [DHCP Snooping Process on page 14](#)
- [DHCPv6 Snooping on page 14](#)
- [Rapid Commit for DHCPv6 on page 15](#)
- [DHCP Server Access on page 15](#)
- [Static IP Address Additions to the DHCP Snooping Database on page 19](#)



- [Snooping DHCP Packets That Have Invalid IP Addresses on page 19](#)
- [Prioritizing Snooped Packets on page 20](#)

## DHCP Snooping Basics

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

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

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

When DHCP snooping is enabled, the lease information from the switching device is used to create the DHCP snooping table, also known as the binding table. The table shows current IP-MAC bindings, as well as lease time, type of binding, names of associated VLANs, and associated interfaces.



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

Entries in the DHCP snooping database are updated in these events:

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



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

You can configure the switching device to snoop DHCP server responses from particular VLANs only. This prevents spoofing of DHCP server messages.

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

## DHCP Snooping Process

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



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

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



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

For general information about the messages that the DHCP client and DHCP server exchange during the assignment of an IP address for the client, see the *Junos OS Administration Library for Routing Devices*.

## DHCPv6 Snooping

DHCPv6 snooping is the equivalent of DHCP snooping for IPv6. The process for DHCPv6 snooping is similar to that for DHCP snooping, but uses different names for the messages exchanged between the client and server to assign IPv6 addresses. [Table 3 on page 15](#) shows DHCPv6 messages and their DHCP equivalents.

Table 3: DHCPv6 Messages and Equivalent DHCPv4 Messages

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

## Rapid Commit for DHCPv6

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

In the rapid commit process:

1. The DHCPv6 client sends out a SOLICIT message that contains a request that rapid assignment of address, prefix, and other configuration parameters be preferred.
2. If the DHCPv6 server supports rapid assignment, it responds with a REPLY message, which contains the assigned IPv6 address and prefix and other configuration parameters.

## DHCP Server Access

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

- [Switching Device, DHCP Clients, and DHCP Server Are All on the Same VLAN on page 16](#)
- [Switching Device Acts as DHCP Server on page 17](#)
- [Switching Device Acts as Relay Agent on page 18](#)

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

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

- The server is directly connected to the same switching device as the one connected to the DHCP clients (the hosts, or network devices, that are requesting IP addresses from the server). The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. See [Figure 1 on page 16](#).
- The server is connected to an intermediary switching device (Switching Device 2). The DHCP clients are connected to Switching Device 1, which is connected through a trunk port to Switching Device 2. Switching Device 2 is being used as a transit device. The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. As shown in [Figure 2 on page 17](#), ge-0/0/11 is a trusted trunk port.

Figure 1: DHCP Server Connected Directly to a Switching Device

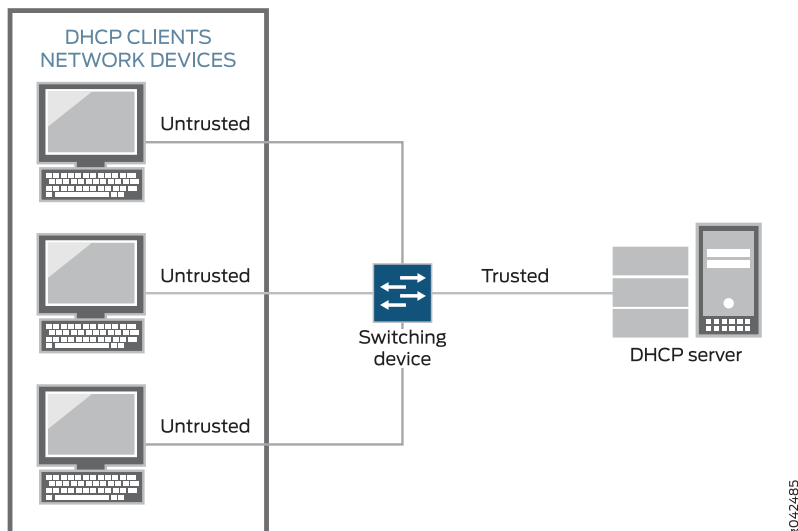
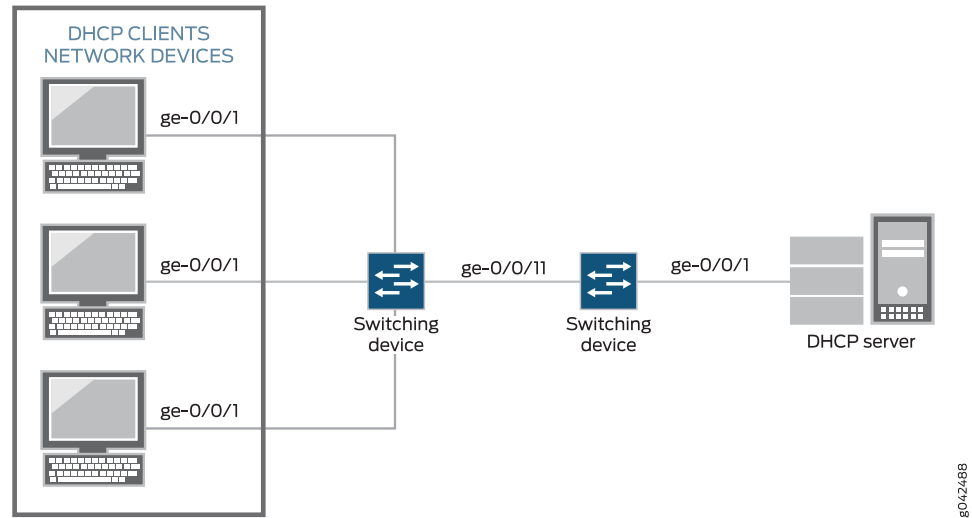


Figure 2: DHCP Server Connected Directly to Switching Device 2, with Switching Device 2 Connected to Switching Device 1 Through a Trusted Trunk Port



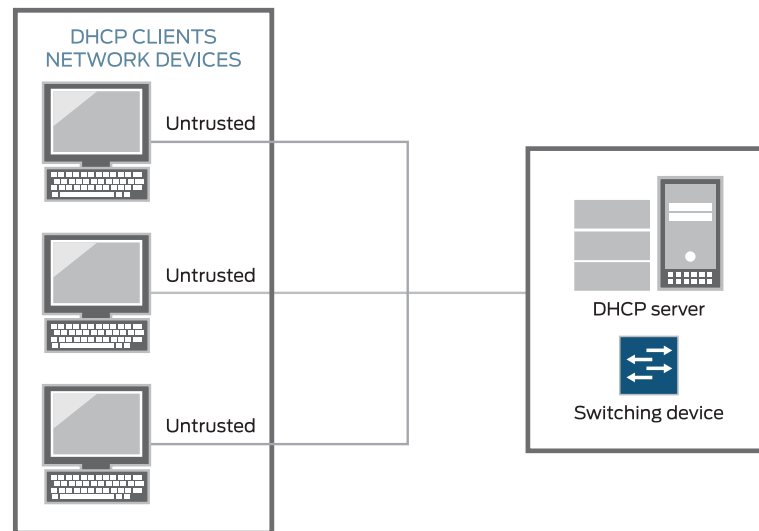
### Switching Device Acts as DHCP Server



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

The switching device itself is configured as a DHCP server; this is known as a *local configuration*. See [Figure 3 on page 18](#).

Figure 3: Switching Device Is the DHCP Server



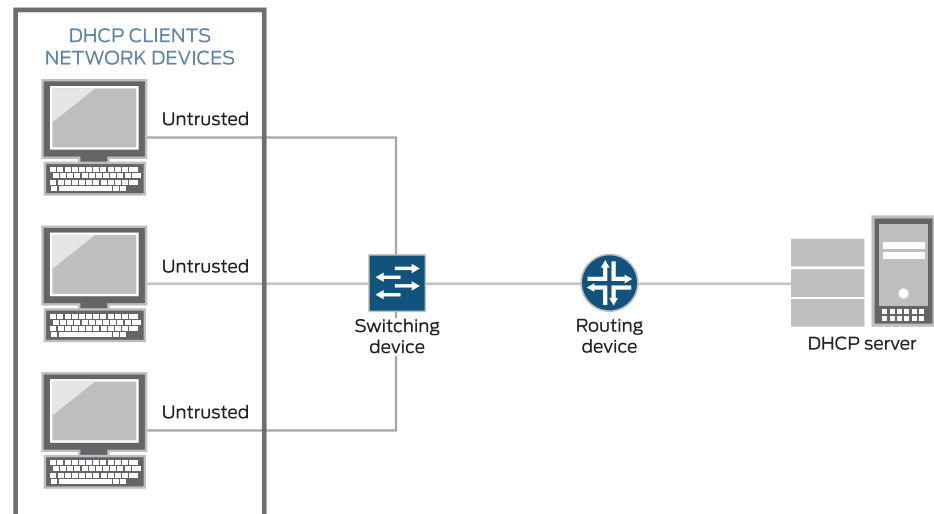
### Switching Device Acts as Relay Agent

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

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

- The DHCP server and clients are in different VLANs.
- The switching device is connected to a router that is in turn connected to the DHCP server. See [Figure 4 on page 19](#).

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



8042487

## Static IP Address Additions to the DHCP Snooping Database

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

## Snooping DHCP Packets That Have Invalid IP Addresses

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

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

## Prioritizing Snooped Packets



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

You can use class-of-service (CoS) forwarding classes and queues to prioritize DHCP snooped packets for a specified VLAN. This type of configuration places the DHCP snooped packets for that VLAN in a specified egress queue, so that the security procedure does not interfere with the transmission of high-priority traffic. For additional information, see [“Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic”](#) on page 104.

### Related Documentation

- [Understanding Port Security on page 7](#)
- [Understanding Trusted DHCP Servers for Port Security on page 32](#)
- [Enabling a Trusted DHCP Server on an MX Series Router \(CLI Procedure\)](#)
- [Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers \(CLI Procedure\)](#)

## Understanding DAI for Port Security

---

Dynamic ARP inspection (DAI) protects switching devices against ARP spoofing.

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

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

- [Address Resolution Protocol on page 20](#)
- [ARP Spoofing on page 21](#)
- [Dynamic ARP Inspection on page 21](#)
- [Prioritizing Inspected Packets on page 22](#)

## Address Resolution Protocol

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

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



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

## ARP Spoofing

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

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

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

## Dynamic ARP Inspection

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

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

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

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

**NOTE:**

- If your switching device is an EX Series switch and uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, see *Enabling a Trusted DHCP Server (CLI Procedure)* for information about configuring an access interface to be a DHCP trusted port.
- If your switching device is an EX Series switch and is *not* using Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, see “[Enabling a Trusted DHCP Server \(CLI Procedure\)](#)” on [page 136](#) for information about configuring an access interface to be a DHCP trusted port.

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

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

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

## Prioritizing Inspected Packets



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

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

**Related Documentation**

- [Understanding Port Security on page 7](#)
- [Understanding DHCP Snooping for Port Security on page 12](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61](#)
- [Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing](#)
- [Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 104](#)
- [Enabling Dynamic ARP Inspection \(CLI Procedure\) on page 137](#)

- *Enabling Dynamic ARP Inspection (CLI Procedure)*
- [Enabling Dynamic ARP Inspection \(J-Web Procedure\) on page 139](#)

## Understanding IPv6 Neighbor Discovery Inspection

IPv6 nodes (hosts and routers) use Neighbor Discovery Protocol (NDP) to discover the presence and link-layer addresses of other nodes residing on the same link. Hosts use NDP to find neighboring routers that are willing to forward packets on their behalf, while routers use it to advertise their presence. Nodes also use NDP to maintain reachability information about the paths to active neighbors. When a router or the path to a router fails, a host can search for alternate paths.

IPv6 nodes use NDP exchange neighbor solicitation and advertisement messages to learn the link-layer addresses of their neighbors. This process makes NDP susceptible to attacks that involve the spoofing (or forging) of link-layer addresses. An attacking node can cause packets for legitimate nodes to be sent to some other link-layer address by either sending a neighbor solicitation message with a spoofed source MAC address, or by sending a neighbor advertisement address with a spoofed target MAC address. The spoofed MAC address is then associated with a legitimate network IPv6 address by the other nodes.

IPv6 neighbor discovery inspection prevents NDP security vulnerabilities by inspecting neighbor discovery messages and verifying them against the DHCPv6 binding table. The DHCPv6 binding table is a database of valid matches, or bindings, of IP addresses to MAC addresses, also known as the DHCPv6 snooping table. With neighbor discovery inspection, the source IP address and source MAC address of the ICMPv6 packet carrying the neighbor discovery message are compared against the entries in the binding table. If no match is found, the packet is dropped.

The neighbor discovery process uses five types of ICMPv6 packets for the purposes of advertisement, solicitation, or redirection: Neighbor Solicit, Neighbor Advertise, Router Solicit, Router Advertise, and Router Redirect. Neighbor discovery inspection checks all Neighbor or Router Solicit messages and Neighbor or Router Advertise messages for their source IPv6 address and MAC address, and also checks that Router Redirect messages are sent only by trusted routers. These checks can prevent the following types of attacks:

Cache poisoning attacks—Neighbor Discovery cache poisoning is the IPv6 equivalent of ARP spoofing, in which an attacker sends an unsolicited advertisement to other hosts on the network with a forged address, to associate its own MAC address with a legitimate network IP address. These bindings between IPv6 addresses and MAC addresses are stored by each node in its neighbor cache. When the caches are updated with the malicious binding, the attacker can initiate a man-in-the-middle attack, intercepting traffic that was intended for a legitimate host.

Routing denial-of-service (DoS) attacks—An attacker could cause a host to disable its first-hop router by spoofing the address of a router and sending a neighbor advertisement message with the *router* flag cleared. The victim host assumes that the device that used to be its first-hop router is no longer a router.

Redirect attacks—Routers use ICMPv6 redirect requests to inform a host of a more efficient route to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a Router Redirect message that the destination is in fact a neighbor. An attacker using this provision can achieve an effect similar to cache poisoning and intercept all traffic from the victim host.

**Related  
Documentation**

- [IPv6 Neighbor Discovery Protocol Overview](#)
- [Enabling IPv6 Neighbor Discovery Inspection](#)
- [Understanding Port Security on page 7](#)
- [Configuring Port Security \(CLI Procedure\) on page 110](#)
- [Understanding DHCP Snooping for Port Security](#)

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

---

MAC limiting for port security 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.

This topic describes the various method of MAC limiting and MAC move limiting for port security:

- [MAC Limiting for Port Security by Limiting the Number of MAC Addresses That Can be Learned on Interfaces on page 24](#)
- [MAC Limiting for Port Security by Specifying MAC Addresses That Are Allowed to Access Interfaces on page 25](#)
- [MAC Move Limiting for Port Security by Monitoring MAC Address Moves within VLANs on page 25](#)

### MAC Limiting for Port Security by Limiting the Number of MAC Addresses That Can be Learned on Interfaces

One method to enhance port security is to set the maximum number of MAC addresses that can be learned (added to the Ethernet switching table) on any of the following:

- A specific access interface (port)
- All access interfaces
- A specific access interface on the basis of its membership within a specific virtual LAN (VLAN membership MAC limit)



**NOTE:** Static MAC addresses do not count toward the limit you specify for dynamic MAC addresses.

---

When you are configuring the maximum MAC limit for an interface, you can choose the action that occurs on incoming packets when the MAC limit is exceeded. For additional information about configuring MAC limit for an interface, see [“Configuring MAC Limiting \(CLI Procedure\)” on page 140](#) or *Configuring MAC Limiting (CLI Procedure)*.

## MAC Limiting for Port Security by Specifying MAC Addresses That Are Allowed to Access Interfaces

Another method to enhance port security is to configure specific MAC addresses as *allowed MAC addresses* for specific access interfaces. Any MAC address that is not in the list of the configured addresses is not learned and the switch logs a 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.

## MAC Move Limiting for Port Security by Monitoring MAC Address Moves within VLANs

MAC move limiting causes the switch to limit and track the frequency with which a MAC address can move to a new interface (port). It can help prevent MAC spoofing, and it can also detect and prevent loops.



**NOTE:** MAC move limiting is not supported on EX9200.

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.

### Related Documentation

- [Understanding Port Security on page 7](#)
- [Configuring MAC Limiting \(J-Web Procedure\) on page 143](#)
- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 159](#)
- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\)](#)
- [Adding a Static MAC Address Entry to the Ethernet Switching Table \(CLI Procedure\)](#)
- [Adding a Static MAC Address Entry to the Ethernet Switching Table \(CLI Procedure\)](#)

## Understanding Media Access Control Security (MACsec)

---

Media Access Control Security (MACsec) is an industry-standard security technology that provides secure communication for all traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec is standardized in IEEE 802.1AE.

MACsec allows you to secure an Ethernet link for almost all traffic, including frames from the Link Layer Discovery Protocol (LLDP), Link Aggregation Control Protocol (LACP), Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), and other protocols that are not typically secured on an Ethernet link because of limitations with other security solutions. MACsec can be used in combination with other security protocols such as IP Security (IPsec) and Secure Sockets Layer (SSL) to provide end-to-end network security.

This topic contains the following sections:

- [How MACsec Works on page 26](#)
- [Understanding Connectivity Associations and Secure Channels on page 27](#)
- [Understanding MACsec Security Modes on page 27](#)
- [Understanding the Requirements to Enable MACsec on a Switch-to-Host Link on page 29](#)
- [Understanding MACsec Hardware Requirements for EX Series and QFX Series Switches on page 30](#)
- [Understanding MACsec Software Requirements for EX Series and QFX Series Switches on page 30](#)
- [Understanding the MACsec Feature License Requirement on page 31](#)
- [MACsec Limitations on page 31](#)

### How MACsec Works

MACsec provides industry-standard security through the use of secured point-to-point Ethernet links. The point-to-point links are secured after matching security keys—a user-configured pre-shared key when you enable MACsec using static connectivity association key (CAK) security mode, a user-configured static secure association key when you enable MACsec using static secure association key (SAK) security mode, or a dynamic key included as part of the AAA handshake with the RADIUS server when you enable MACsec using dynamic security mode—are exchanged and verified between the interfaces at each end of the point-to-point Ethernet link. Other user-configurable parameters, such as MAC address or port, must also match on the interfaces on each side of the link to enable MACsec. See [“Configuring Media Access Control Security \(MACsec\)” on page 116](#).

Once MACsec is enabled on a point-to-point Ethernet link, all traffic traversing the link is MACsec-secured through the use of data integrity checks and, if configured, encryption.

The data integrity checks verify the integrity of the data. MACsec appends an 8-byte header and a 16-byte tail to all Ethernet frames traversing the MACsec-secured point-to-point Ethernet link, and the header and tail are checked by the receiving interface to ensure that the data was not compromised while traversing the link. If the data integrity check detects anything irregular about the traffic, the traffic is dropped.

MACsec can also be used to encrypt all traffic on the Ethernet link. The encryption used by MACsec ensures that the data in the Ethernet frame cannot be viewed by anybody monitoring traffic on the link. MACsec encryption is optional and user-configurable; you can enable MACsec to ensure the data integrity checks are performed while still sending unencrypted data “in the clear” over the MACsec-secured link, if desired.

MACsec is configured on point-to-point Ethernet links between MACsec-capable interfaces. If you want to enable MACsec on multiple Ethernet links, you must configure MACsec individually on each point-to-point Ethernet link.

## Understanding Connectivity Associations and Secure Channels

MACsec is configured in connectivity associations. MACsec is enabled when a connectivity association is assigned to an interface.

When you are configuring MACsec using static secure association key (SAK) security mode, you must configure secure channels within a connectivity association. The secure channels are responsible for transmitting and receiving data on the MACsec-enabled link, and also responsible for transmitting SAKs across the link to enable and maintain MACsec. A single secure channel is uni-directional—it can only be used to apply MACsec to inbound or outbound traffic. A typical connectivity association when MACsec is enabled using SAK security mode contains two secure channels—one secure channel for inbound traffic and another secure channel for outbound traffic.

When you enable MACsec using static CAK or dynamic security mode, you have to create and configure a connectivity association. Two secure channels—one secure channel for inbound traffic and another secure channel for outbound traffic—are automatically created. The automatically-created secure channels do not have any user-configurable parameters; all configuration is done in the connectivity association outside of the secure channels.

## Understanding MACsec Security Modes

### Understanding Static Connectivity Association Key Security Mode (Recommended Security Mode for Switch-to-Switch Links)

When you enable MACsec using static connectivity association key (CAK) security mode, two security keys—a connectivity association key (CAK) that secures control plane traffic and a randomly-generated secure association key (SAK) that secures data plane traffic—are used to secure the point-to-point Ethernet link. Both keys are regularly exchanged between both devices on each end of the point-to-point Ethernet link to ensure link security.

You initially establish a MACsec-secured link using a pre-shared key when you are using static CAK security mode to enable MACsec. A pre-shared key includes a connectivity association name (CKN) and its own connectivity association key (CAK). The CKN and

CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

Once matching pre-shared keys are successfully exchanged, the MACsec Key Agreement (MKA) protocol is enabled. The MKA protocol is responsible for maintaining MACsec on the link, and decides which switch on the point-to-point link becomes the key server. The key server then creates an SAK that is shared with the switch at the other end of the point-to-point link only, and that SAK is used to secure all data traffic traversing the link. The key server will continue to periodically create and share a randomly-created SAK over the point-to-point link for as long as MACsec is enabled.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels—one for inbound traffic and one for outbound traffic—are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

We recommend enabling MACsec on switch-to-switch links using static CAK security mode. Static CAK security mode ensures security by frequently refreshing to a new random security key and by only sharing the security key between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available when you enable MACsec using static CAK security mode.

See [“Configuring Media Access Control Security \(MACsec\)” on page 116](#) for step-by-step instructions on enabling MACsec using static CAK security mode.

### **Understanding Dynamic Secure Association Key Security Mode (Switch-to-Host Links)**

---

Dynamic secure association key security mode is used to enable MACsec on a switch-to-host link.

To enable MACsec on a link connecting an endpoint device—such as a server, phone, or personal computer—to a switch, the endpoint device must support MACsec and must be running software that allows it to enable a MACsec-secured connection. When configuring MACsec on a switch-to-host link, the MACsec Key Agreement (MKA) keys, which are included as part of 802.1X authentication, are retrieved from a RADIUS server as part of the AAA handshake. A master key is passed from the RADIUS server to the switch and from the RADIUS server to the host in independent authentication transactions. The master key is then passed between the switch and the host to create a MACsec-secured connection.

A secure association using dynamic secure association security mode must be configured on the switch's Ethernet interface that connects to the host in order for the switch to create a MACsec-secured connection after receiving the MKA keys from the RADIUS server.

The RADIUS server must be using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) in order to support MACsec. The RADIUS servers that support other



widely-used authentication frameworks, such as password-only or md5, cannot be used to support MACsec. In order to enable MACsec on a switch to secure a connection to a host, you must be using 802.1X authentication on the RADIUS server. MACsec must be configured into dynamic mode. MACsec is still enabled using connectivity associations when enabled on a switch-to-host link, as it is on a switch-to-switch link.

### Understanding Static Secure Association Key Security Mode (Supported for Switch-to-Switch Links)

When you enable MACsec using static secure association key (SAK) security mode, one of up to two manually configured SAKs is used to secure data traffic on the point-to-point Ethernet link. All SAK names and values are configured by the user; there is no key server or other tool that creates SAKs. Security is maintained on the point-to-point Ethernet link by periodically rotating between the two security keys. Each security key name and value must have a corresponding matching value on the interface at the other end of the point-to-point Ethernet link to maintain MACsec on the link.

You configure SAKs within secure channels when you enable MACsec using static SAK security mode. You configure secure channels within connectivity associations. A typical connectivity association for MACsec using static SAK security mode contains two secure channels—one for inbound traffic and one for outbound traffic—that have each been configured with two manually-configured SAKs. You must attach the connectivity association with the secure channel configurations to an interface to enable MACsec using static SAK security mode.

We recommend enabling MACsec using static CAK security mode. You should only use static SAK security mode if you have a compelling reason to use it instead of static CAK security mode.

See [“Configuring Media Access Control Security \(MACsec\)” on page 116](#) for step-by-step instructions on enabling MACsec using SAKs.

### Understanding the Requirements to Enable MACsec on a Switch-to-Host Link

When configuring MACsec on a switch-to-host link, the MACsec Key Agreement (MKA) keys, which are included as part of 802.1X authentication, are retrieved from a RADIUS server as part of the AAA handshake. A master key is passed from the RADIUS server to the switch and from the RADIUS server to the host in independent authentication transactions. The master key is then passed between the switch and the host to create a MACsec-secured connection.

The following requirements must be met in order to enable MACsec on a link connecting a host device to a switch.

The host device:

- must support MACsec and must be running software that allows it to enable a MACsec-secured connection with the switch.

The switch:

- must be an EX4200, EX4300, or EX4550 switch running Junos OS Release 14.1X51-D10 or later, or an EX4600 or QFX5100-24Q switch running Junos OS Release 14.1X51-D15 or later.
- must be configured into dynamic secure association key security mode.
- must be using 802.1X authentication to communicate with the RADIUS server.

The RADIUS server:

- must be using the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework.



**NOTE:** RADIUS servers that support other widely-used authentication frameworks, such as password-only or md5, cannot be used to support MACsec.

- must be using 802.1X authentication.
- can be multiple hops from the switch and the host device.

## Understanding MACsec Hardware Requirements for EX Series and QFX Series Switches

MACsec is currently supported on the following EX Series and QFX Series switch interfaces:

- The uplink port connections on the SFP+ MACsec uplink module that can be installed on EX4200 series switches.
- All access and uplink ports on EX4300 switches.
- All EX4550 optical interfaces that use the LC connection type. See *Pluggable Transceivers Supported on EX4550 Switches*.
- All twenty-four fixed SFP+ interfaces on an EX4600 switch.
- All eight SFP+ interfaces on the EX4600-EM-8F expansion module, when installed in an EX4600 or QFX5100-24Q switch.

MACsec can be configured on supported switch interfaces when those switches are configured in a Virtual Chassis or Virtual Chassis Fabric (VCF), including when MACsec-supported interfaces are on member switches in a mixed Virtual Chassis or VCF that includes switch interfaces that do not support MACsec. MACsec, however, cannot be enabled on Virtual Chassis ports (VCPs) to secure traffic travelling between member switches in a Virtual Chassis or VCF.

## Understanding MACsec Software Requirements for EX Series and QFX Series Switches

MACsec was initially released on EX4200, EX4300, and EX4550 switches in Junos OS Release 13.2X50-D15.

MACsec support for dynamic security mode, which allows MACsec to be configured on switch-to-host links, for EX4200, EX4300, and EX4550 switches was introduced in Junos OS Release 14.1X51-D10.

MACsec support for EX4600 switches and QFX5100-24Q switches was introduced in Junos OS Release 14.1X51-D15. The EX4600 switch and the QFX5100-24Q switch supported all MACsec security modes, including dynamic security mode to enable MACsec on switch-to-host links, upon introduction in Junos OS Release 14.1X51-D15.

The switches on each end of a MACsec-secured switch-to-switch link must either both be using Junos OS Release 14.1X51-D10 or later, or must both be using an earlier version of Junos, in order to establish a MACsec-secured connection when using static CAK security mode.

You must download the controlled version of your Junos OS software to enable MACsec. MACsec software support is not available in the domestic version of your Junos OS software. The controlled version of Junos OS software includes all features and functionality available in the domestic version of Junos OS, while also supporting MACsec. The domestic version of Junos OS software is shipped on all switches that support MACsec, so you must download and install a controlled version of Junos OS software for your switch before you can enable MACsec.

The controlled version of Junos OS software contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS software is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring the controlled version of your Junos OS software, contact Juniper Networks Trade Compliance group at [compliance\\_helpdesk@juniper.net](mailto:compliance_helpdesk@juniper.net).

The process for installing a controlled version of Junos OS software on your switch is identical to installing the domestic version. See *Downloading Software Packages from Juniper Networks*.

## Understanding the MACsec Feature License Requirement

A feature license is required to configure MACsec on a switch.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key. You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on your switches cannot be purchased to enable MACsec.

## MACsec Limitations

All types of Spanning Tree Protocol frames cannot currently be encrypted using MACsec.

### Related Documentation

- [Configuring Media Access Control Security \(MACsec\) on page 116](#)

## Understanding Trusted DHCP Servers for Port Security

---

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

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

### Related Documentation

- [Understanding DHCP Snooping for Port Security on page 12](#)
- [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 54](#)
- [Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing](#)
- [Enabling a Trusted DHCP Server \(CLI Procedure\) on page 136](#)
- [Enabling a Trusted DHCP Server \(CLI Procedure\)](#)

## Understanding IP Source Guard for Port Security on EX Series Switches

---

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

- [IP Address Spoofing on page 32](#)
- [How IP Source Guard Works on page 32](#)
- [IPv6 Source Guard on page 33](#)
- [The DHCP Snooping Table on page 33](#)
- [Typical Uses of Other Junos OS Features with IP Source Guard on page 34](#)

### IP Address Spoofing

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

### How IP Source Guard Works

IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the switch against entries stored in the DHCP snooping database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the switch does not forward the packet—that is, the packet is discarded.

**NOTE:**

- If your switch uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, DHCP snooping is enabled automatically when you enable IP source guard on a VLAN. See *Configuring IP Source Guard (CLI Procedure)*.
- If your switch is *not* using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style and you enable IP source guard on a VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to the VLAN. See [“Configuring IP Source Guard \(CLI Procedure\)” on page 148](#).

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



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

## IPv6 Source Guard

IPv6 source guard is available on switches that support DHCPv6 snooping. To determine whether your switch supports DHCPv6 snooping, see the *EX Series Switch Software Features Overview*.

## The DHCP Snooping Table

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

To display the DHCP snooping table, issue the operational mode command that appears in the switch CLI.

For DHCP snooping:

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

For DHCPv6 snooping:

- (For non-ELS switches) [show dhcpv6 snooping binding](#)
- (EX4300 switches only) [show dhcp-security ipv6 binding](#)

## Typical Uses of Other Junos OS Features with IP Source Guard

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

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



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

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

### Related Documentation

- [Understanding DHCP Snooping for Port Security on page 12](#)
- [Configuring IP Source Guard \(CLI Procedure\)](#)
- [Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 87](#)
- [Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 77](#)
- [Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing](#)

## Understanding DHCP Option 82 for Port Security on Switching Devices

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

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

This topic covers:

- [DHCP Option 82 Processing on page 35](#)
- [Suboption Components of Option 82 on page 36](#)
- [Switching Device Configurations That Support Option 82 on page 37](#)
- [DHCPv6 Options on page 38](#)

### DHCP Option 82 Processing

If DHCP option 82 is enabled on a VLAN or bridge domain, then when a network device—a DHCP client—that is connected to the VLAN or bridge domain on an untrusted interface sends a DHCP request, the switching device inserts information about the client's network location into the packet header of that request. The switching device then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or another parameter for the client. See “[Suboption Components of Option 82](#)” on page 36 for more information about option 82.



#### NOTE:

- If your switching device is an EX Series switch and uses Junos OS with Enhanced Layer 2 Software (ELS) configuration style, you can enable DHCP option 82 only for a specific VLAN. See *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*.
- If your switching device is an EX Series switch and does *not* use Junos OS with Enhanced Layer 2 Software (ELS) configuration style, you can enable DHCP option 82 either for a specific VLAN or for all VLANs. See “[Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server \(CLI Procedure\)](#)” on page 156.

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

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



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

---

## Suboption Components of Option 82

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

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

Use the `prefix` option to add an optional prefix to the circuit ID. If you enable the `prefix` option, the hostname for the switching device is used as the prefix; for example, `device1:ge-0/0/10:vlan1`, where `device1` is the hostname.

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

- **remote ID**—Identifies the remote host. See [remote-id](#) for details.
- **vendor ID**—Identifies the vendor of the host. If you specify the `vendor-id` option but do not enter a value, the default value Juniper is used. To specify a value, you type a character string.



## Switching Device Configurations That Support Option 82

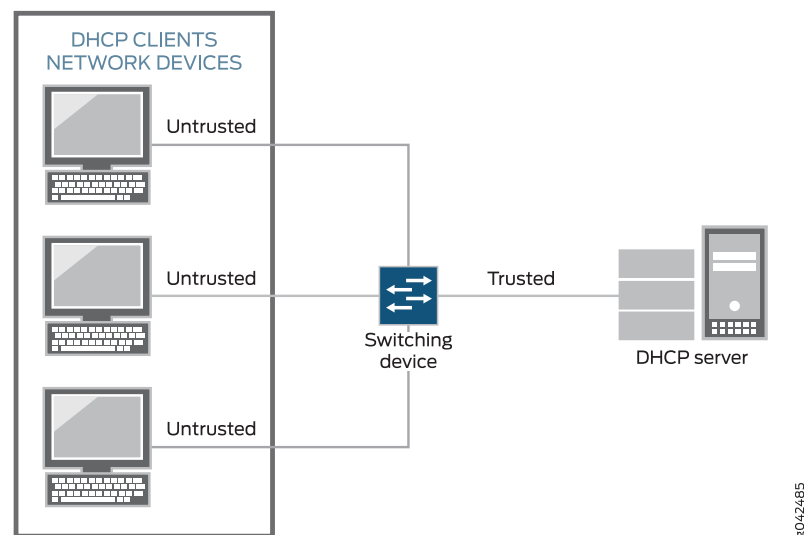
Switching device configurations that support option 82 are:

- [Switching Device, DHCP Clients, and the DHCP Server Are on the Same VLAN or Bridge Domain on page 37](#)
- [Switching Device Acts as a Relay Agent on page 37](#)

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

If the switching device, the DHCP clients, and the DHCP server are all on the same VLAN or bridge domain, the switching device forwards the requests from the clients on untrusted access interfaces to the server on a trusted interface. See [Figure 5 on page 37](#).

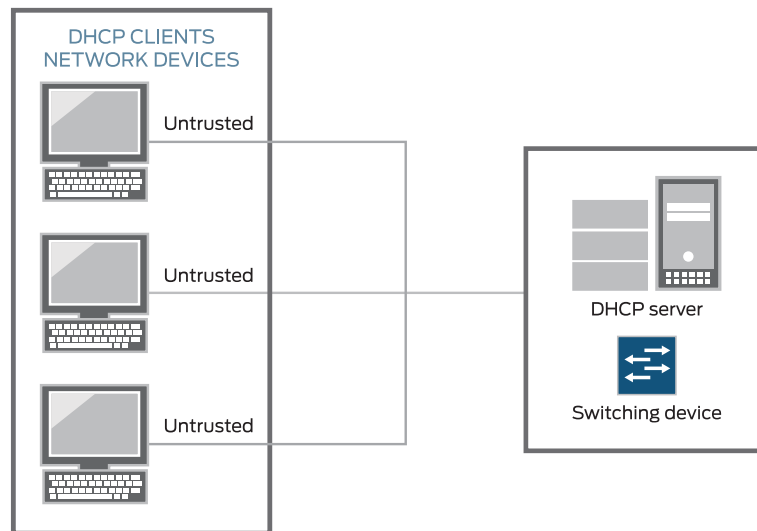
**Figure 5: DHCP Clients, Switching Device, and the DHCP Server Are All on the Same VLAN or Bridge Domain**



### Switching Device Acts as a Relay Agent

The switching device functions as a relay agent (extended relay server) when the DHCP clients or the DHCP server is connected to the switching device through a Layer 3 interface. On the switching device, these interfaces are configured as routed VLAN interfaces (RVIs). [Figure 6 on page 38](#) illustrates a scenario for the switching device acting as an extended relay server; in this instance, the switching device relays requests to the server.

Figure 6: Switching Device Acting as an Extended Relay Server



## DHCPv6 Options



**NOTE:** MX Series routers do not support DHCPv6.

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

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

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

### Related Documentation

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

## Understanding Persistent MAC Learning (Sticky MAC)

Persistent MAC learning, also known as sticky MAC, is a port security feature that enables an interface to retain dynamically learned MAC addresses when the switch is restarted or if the interface goes down and is brought back online.

Persistent MAC address learning is disabled by default. You can enable persistent MAC address learning in conjunction with MAC limiting to restrict the number of persistent MAC addresses. You enable this feature on interfaces.

Configure persistent MAC learning on an interface to:

- Prevent traffic losses for trusted workstations and servers because the interface does not have to relearn the addresses from ingress traffic after a restart.
- Protect the switch against security attacks. Use persistent MAC learning in combination with MAC limiting to protect against attacks, such as Layer 2 denial-of-service (DoS) attacks, overflow attacks on the Ethernet switching table, and DHCP starvation attacks, by limiting the MAC addresses allowed while still allowing the interface to dynamically learn a specified number of MAC addresses. The interface is secured because after the limit has been reached, additional devices cannot connect to the port.

By configuring persistent MAC learning along with MAC limiting, you enable interfaces to learn MAC addresses of trusted workstations and servers from the time when you connect the interface to your network until the limit for MAC addresses is reached, and ensure that after this limit is reached, new devices will not be allowed to connect to the interface even if the switch restarts. As an alternative to using persistent MAC learning with MAC limiting, you can statically configure each MAC address on each port or allow the port to continuously learn new MAC addresses after restarts or interface-down events. Allowing the port to continuously learn MAC addresses represents a security risk.



**NOTE:** While a switch is restarting or an interface is coming back up, there might be a short delay before the interface can learn more MAC addresses. This delay occurs while the system re-enters previously learned persistent MAC addresses into the forwarding database for the interface.



**TIP:** If you move a device within your network that has a persistent MAC address entry on the switch, use the `clear ethernet-switching table persistent-mac` command to clear the persistent MAC address entry from the interface. If you move the device and do not clear the persistent MAC address from the original port it was learned on, then the new port will not learn the MAC address of the device and the device will not be able to connect.

If the original port is down when you move the device, then the new port will learn the MAC address and the device can connect. However, if you do not clear the persistent MAC address on the original port, then when the port restarts, the system reinstalls the persistent MAC address in the forwarding

table for that port. If this occurs, the persistent MAC address is removed from the new port and the device loses connectivity.

.....  
Consider the following configuration guidelines when configuring persistent MAC learning:

- Interfaces must be configured in access mode (use the **port-mode** configuration statement or, for switches operating on the Enhanced Layer 2 Software (ELS) configuration style, the **interface-mode** configuration statement).
- You cannot enable persistent MAC learning on an interface on which 802.1x authentication is configured.
- You cannot enable persistent MAC learning on an interface that is part of a redundant trunk group.
- You cannot enable persistent MAC learning on an interface on which **no-mac-learning** is enabled.

**Related  
Documentation**

- [Understanding Port Security on page 7](#)
- [Configuring Persistent MAC Learning \(CLI Procedure\) on page 159](#)
- [Configuring Persistent MAC Learning \(CLI Procedure\) \(ELS\)](#)

## PART 2

# Configuration

- [Configuration Examples on page 43](#)
- [Configuration Tasks on page 109](#)
- [Configuration Statements on page 163](#)



## CHAPTER 3

# Configuration Examples

- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 51](#)
- [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 54](#)
- [Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 58](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61](#)
- [Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 66](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
- [Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 77](#)
- [Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 87](#)
- [Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 94](#)
- [Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98](#)
- [Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101](#)
- [Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 104](#)

### Example: Configuring Basic Port Security Features

---

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

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

- [Requirements on page 44](#)
- [Overview and Topology on page 44](#)
- [Configuration on page 46](#)
- [Verification on page 47](#)

## Requirements

This example uses the following hardware and software components:

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

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

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



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

---

## Overview and Topology

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

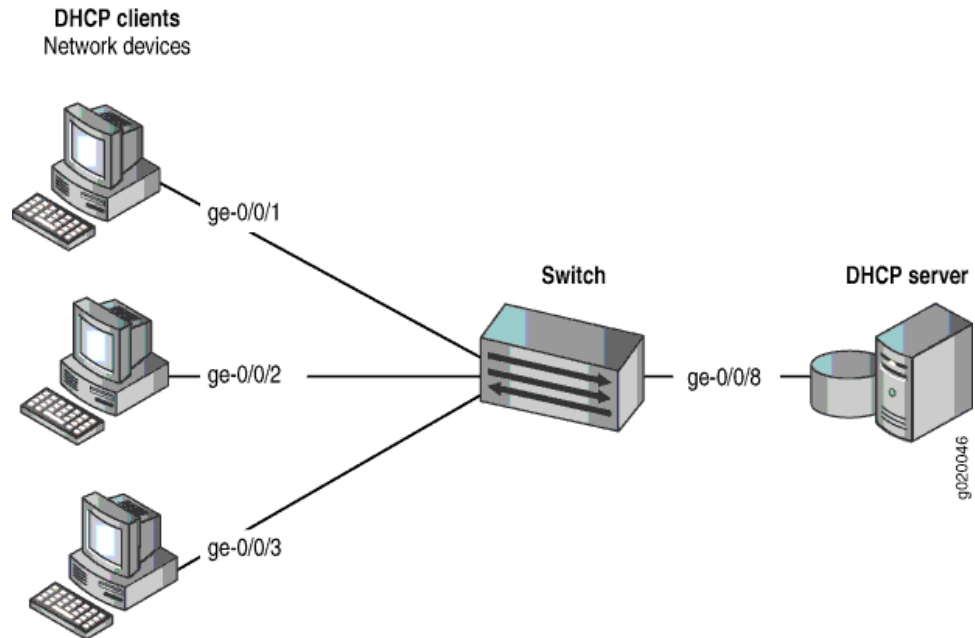
- DHCP snooping to validate DHCP server messages
- DAI to protect against MAC spoofing
- MAC limiting to constrain the number of MAC addresses the switch adds to its MAC address cache
- MAC move limiting to help prevent MAC spoofing
- Persistent MAC learning (sticky MAC) to constrain the MAC addresses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

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



The setup for this example includes the VLAN **employee-vlan** on the switch. [Figure 7 on page 45](#) 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 4 on page 45](#).

**Table 4: Components of the Port Security Topology**

Properties	Settings
Switch hardware	One EX Series or QFX series switch
VLAN name and ID	<b>employee-vlan</b> , 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 <b>employee-vlan</b>	<b>ge-0/0/1</b> , <b>ge-0/0/2</b> , <b>ge-0/0/3</b> , <b>ge-0/0/8</b>
Interface for DHCP server	<b>ge-0/0/8</b>

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

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

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

## Configuration

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

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

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

**Step-by-Step Procedure** Configure basic port security on the switch:

1. Enable DHCP snooping on the VLAN:  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan examine-dhcp
```
2. Specify the interface (port) from which DHCP responses are allowed:  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/8 dhcp-trusted
```
3. Enable dynamic ARP inspection (DAI) on the VLAN:  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan arp-inspection
```
4. Configure a MAC limit of **4** and use the default action, **drop**. (Packets are dropped, and the MAC address is not added to the Ethernet switching table if the MAC limit is exceeded on the interfaces):  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 mac-limit 4
user@switch# set interface ge-0/0/2 mac-limit 4
```
5. Allow learned MAC addresses for a particular interface to persist across restarts of the switch and interface-down events by enabling persistent MAC learning:  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 persistent-learning
```
6. Configure a MAC move limit of **5** and use the default action, **drop**. (Packets are dropped, and the MAC address is not added to the Ethernet switching table if a MAC address has exceeded the MAC move limit):  

```
[edit ethernet-switching-options secure-access-port]
```

```

user@switch# set vlan employee-vlan mac-move-limit 5
7. Configure allowed MAC addresses:

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

```

## Results

Check the results of the configuration:

```

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

```

## Verification

To confirm that the configuration is working properly:

- [Verifying That DHCP Snooping Is Working Correctly on the Switch on page 47](#)
- [Verifying That DAI Is Working Correctly on the Switch on page 48](#)
- [Verifying That MAC Limiting, MAC Move Limiting, and Persistent MAC Learning Are Working Correctly on the Switch on page 49](#)
- [Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 50](#)

### Verifying That DHCP Snooping Is Working Correctly on the Switch

**Purpose** Verify that DHCP snooping is working on the switch.

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

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

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

DHCP Snooping Information:

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

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

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

### Verifying That DAI Is Working Correctly on the Switch

**Purpose** Verify that DAI is working on the switch.

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

Display the DAI information:

```
user@switch> show arp inspection statistics
```

ARP inspection statistics:

Interface	Packets received	ARP inspection pass	ARP inspection failed
ge-0/0/1.0	7	5	2
ge-0/0/2.0	10	10	0
ge-0/0/3.0	12	12	0

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

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

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

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

Display the MAC addresses learned:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 7 entries, 4 learned, 2 persistent entries
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	-	All-members
employee-vlan	00:05:85:3A:82:77	Persistent	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:79	Persistent	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0

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

Display the MAC addresses in the table:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 7 entries, 2 learned, 2 persistent entries
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	-	All-members
employee-vlan	00:05:85:3A:82:77	Persistent	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:79	Persistent	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

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

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

### Verifying That Allowed MAC Addresses Are Working Correctly on the Switch

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

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

```
user@switch> show ethernet-switching table
Ethernet-switching table: 5 entries, 4 learned
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

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

- Related Documentation**
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
  - [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 54](#)
  - [Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 66](#)
  - [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61](#)
  - [Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 51](#)
  - [Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 58](#)
  - [Configuring Port Security \(CLI Procedure\) on page 110](#)
  - [Configuring Port Security \(J-Web Procedure\) on page 112](#)
  - [secure-access-port on page 231](#)
  - [secure-access-port](#)
  - [show arp inspection statistics on page 277](#)
  - [show dhcp snooping binding on page 278](#)
  - [show ethernet-switching table on page 284](#)
  - [show ethernet-switching table](#)

## 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 51](#)
- [Overview and Topology on page 51](#)
- [Configuration on page 53](#)
- [Verification on page 53](#)

### Requirements

This example uses the following hardware and software components:

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

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

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

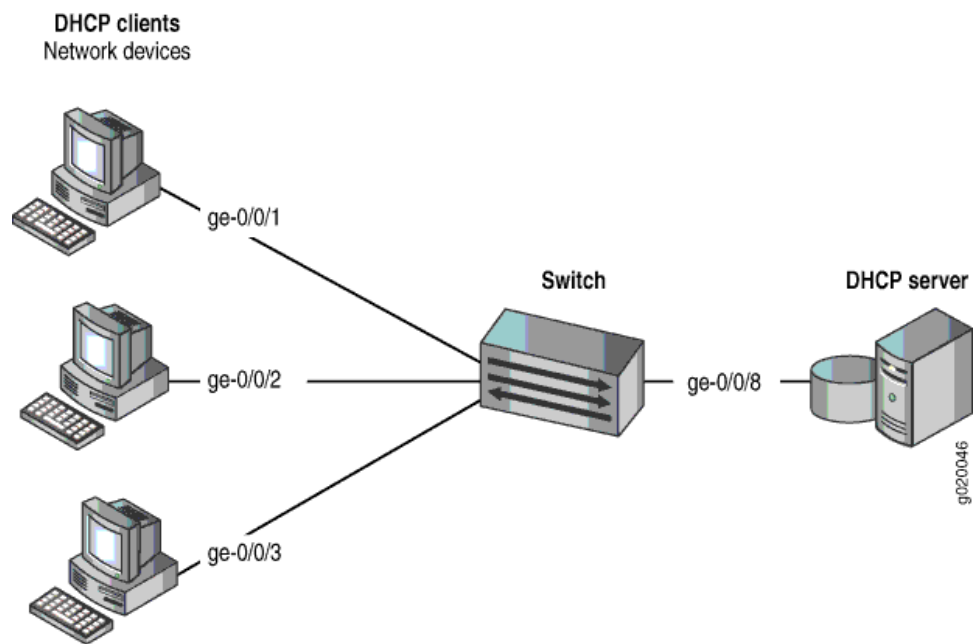
### Overview and Topology

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

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

The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches* and *Example: Setting Up Bridging with Multiple VLANs for the QFX Series*. That procedure is not repeated here. [Figure 8 on page 52](#) 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 5 on page 52](#).

Table 5: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX Series switch or one QFX3500 switch
VLAN name and ID	<b>employee-vlan</b> , 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 <b>employee-vlan</b>	<b>ge-0/0/1</b> , <b>ge-0/0/2</b> , <b>ge-0/0/3</b> , <b>ge-0/0/8</b>
Interface for DHCP server	<b>ge-0/0/8</b>

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

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

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



## Configuration

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

### CLI Quick Configuration

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

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

### Step-by-Step Procedure

Configure MAC limiting and some allowed MAC addresses:

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

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 mac-limit (Access Port Security) 4 action drop
```
2. Clear the current entries for interface **ge-0/0/1** from the MAC address forwarding table :  
  

```
user@switch# clear ethernet-switching-table interface ge-0/0/1
```
3. Configure the allowed MAC addresses on **ge-0/0/2**:  
  

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

### Results

Check the results of the configuration:

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

## Verification

To confirm that the configuration is working properly:

- [Verifying That MAC Limiting Is Working Correctly on the Switch on page 54](#)

### Verifying That MAC Limiting Is Working Correctly on the Switch

**Purpose** Verify that MAC limiting is working on the switch.

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

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

```
Ethernet-switching table: 5 entries, 4 learned
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	00:05:85:3A:82:71	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:74	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:77	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:79	Learn	0	ge-0/0/1.0
employee-vlan	*	Flood	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

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

- Related Documentation**
- [Example: Configuring Basic Port Security Features on page 43](#)
  - [Configuring MAC Limiting \(CLI Procedure\) on page 140](#)
  - [Configuring MAC Limiting](#)
  - [Configuring MAC Move Limiting \(CLI Procedure\) on page 145](#)
  - [Configuring MAC Limiting \(J-Web Procedure\) on page 143](#)

### 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 55](#)
- [Overview and Topology on page 55](#)

- [Configuration on page 56](#)
- [Verification on page 57](#)

## Requirements

This example uses the following hardware and software components:

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

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

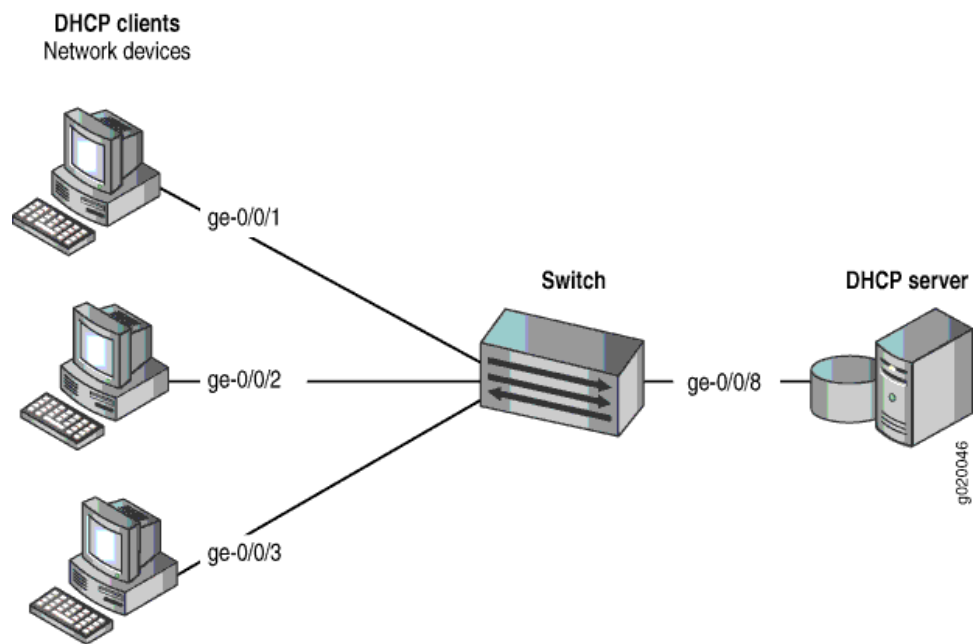
- Connected the DHCP server to the switch.
- Enabled DHCP snooping on the VLAN.
- Configured a VLAN on the switch. See the task for your platform:
  - *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
  - *Example: Setting Up Bridging with Multiple VLANs for the QFX Series*

## Overview and Topology

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

This example shows how to explicitly configure an untrusted interface on an EX3200-24P switch and a QFX3500 switch. [Figure 9 on page 56](#) 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 6 on page 56](#).

Table 6: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	<b>employee-vlan</b> , 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 <b>employee-vlan</b>	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:

<b>CLI Quick Configuration</b>	<p>To quickly set the rogue DHCP server interface as untrusted, copy the following command and paste it into the switch terminal window:</p> <pre>[edit ethernet-switching-options secure-access-port] set interface ge-0/0/8 no-dhcp-trusted</pre>
<b>Step-by-Step Procedure</b>	<p>To set the DHCP server interface as untrusted:</p> <ul style="list-style-type: none"> <li>Specify the interface (port) from which DHCP responses are not allowed:</li> </ul> <pre>[edit ethernet-switching-options secure-access-port] user@switch# set interface ge-0/0/8 no-dhcp-trusted</pre>
<b>Results</b>	<p>Check the results of the configuration:</p> <pre>[edit ethernet-switching-options secure-access-port] user@switch# show interface ge-0/0/8.0 {   no-dhcp-trusted; }</pre>

## Verification

Confirm that the configuration is working properly.

### Verifying That the DHCP Server Interface Is Untrusted

<b>Purpose</b>	Verify that the DHCP server is untrusted.
<b>Action</b>	<ol style="list-style-type: none"> <li>Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.</li> <li>Display the DHCP snooping information when the port on which the DHCP server connects to the switch is not trusted.</li> </ol>
<b>Meaning</b>	There is no output from the command because no entries are added to the DHCP snooping database.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Example: Configuring Basic Port Security Features on page 43</a></li> <li><a href="#">Enabling a Trusted DHCP Server (CLI Procedure) on page 136</a></li> <li><a href="#">Enabling a Trusted DHCP Server (J-Web Procedure) on page 136</a></li> <li><a href="#">secure-access-port on page 231</a></li> <li><a href="#">secure-access-port</a></li> <li><a href="#">show dhcp snooping binding on page 278</a></li> </ul>

## 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 on page 58](#)
- [Overview and Topology on page 58](#)
- [Configuration on page 59](#)
- [Verification on page 60](#)

### 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*.

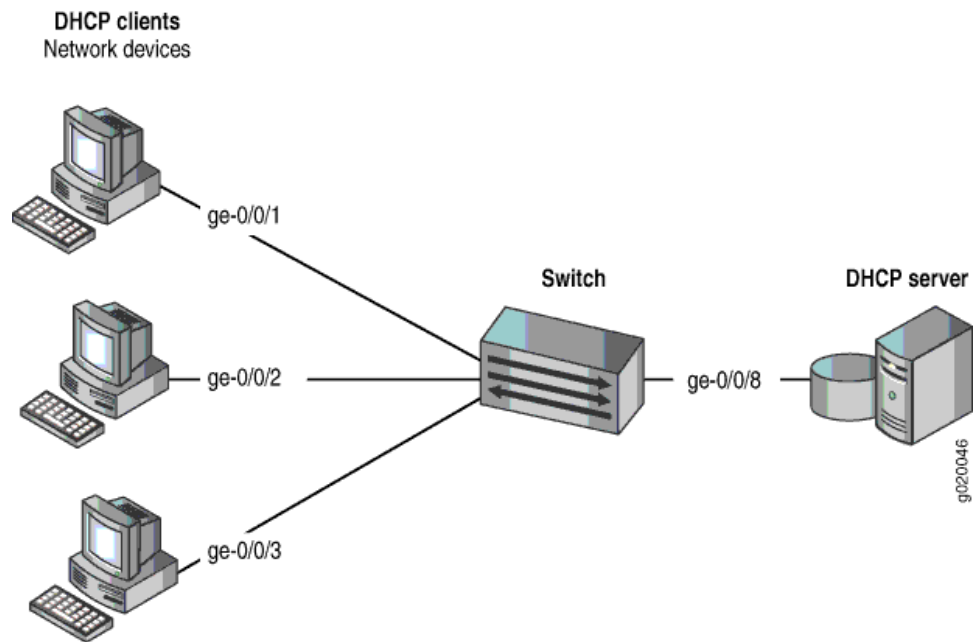
### Overview and Topology

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 59](#) 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 7 on page 59](#).

Table 7: Components of the Port Security Topology

Properties	Settings
Switch hardware	
VLAN name and ID	default
Interfaces in <b>employee-vlan</b>	<code>ge-0/0/1</code> , <code>ge-0/0/2</code> , <code>ge-0/0/3</code> , <code>ge-0/0/8</code>
Interface for DHCP server	<code>ge-0/0/8</code>

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:

<b>CLI Quick Configuration</b>	<p>To quickly configure MAC limiting, copy the following commands and paste them into the switch terminal window:</p> <pre>[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</pre>
<b>Step-by-Step Procedure</b>	<p>Configure MAC limiting:</p> <ol style="list-style-type: none"><li>1. Configure a MAC limit of <b>3</b> on <b>ge-0/0/1</b> and specify that packets with new addresses be dropped if the limit has been exceeded on the interface: <pre>[edit ethernet-switching-options secure-access-port] user@switch# set interface ge-0/0/1 mac-limit (Access Port Security) 3 action drop</pre></li><li>2. Configure a MAC limit of <b>3</b> on <b>ge-0/0/2</b> and specify that packets with new addresses be dropped if the limit has been exceeded on the interface: <pre>[edit ethernet-switching-options secure-access-port] user@switch# set interface ge-0/0/2 mac-limit 3 action drop</pre></li></ol>
<b>Results</b>	<p>Check the results of the configuration:</p> <pre>[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; }</pre>

## Verification

To confirm that the configuration is working properly:

- [Verifying That MAC Limiting Is Working Correctly on the Switch on page 60](#)

### 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 page 43](#)
  - [Configuring MAC Limiting \(CLI Procedure\) on page 140](#)
  - [Configuring MAC Limiting](#)
  - [Configuring MAC Limiting \(J-Web Procedure\) on page 143](#)

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

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



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

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

- [Requirements on page 62](#)
- [Overview and Topology on page 62](#)
- [Configuration on page 63](#)
- [Verification on page 64](#)

## Requirements

This example uses the following hardware and software components:

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

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

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

## Overview and Topology

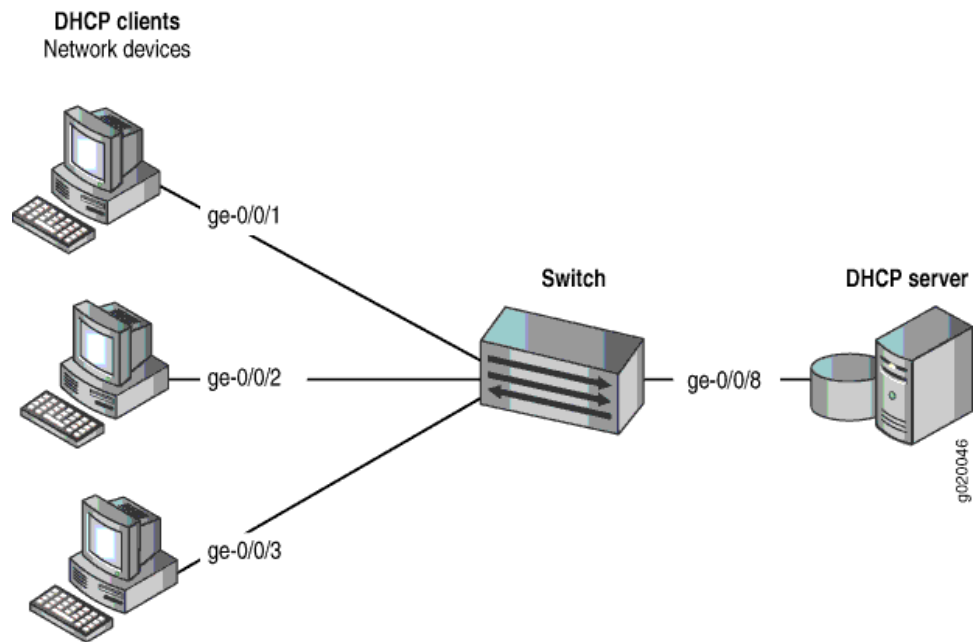
Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch against one common type of attack, an ARP spoofing attack.

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

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

[Figure 11 on page 63](#) 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 8 on page 63](#).

Table 8: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	<b>employee-vlan</b> , 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 <b>employee-vlan</b>	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface for DHCP server	ge-0/0/8

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

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

## Configuration

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

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

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

**Step-by-Step Procedure** Configure DHCP snooping and dynamic ARP inspection (DAI) on the VLAN:

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

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/8 dhcp-trusted
```
2. Enable DHCP snooping on the VLAN:  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan examine-dhcp
```
3. Enable DAI on the VLAN:  

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

**Results** Check the results of the configuration:

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

## Verification

Confirm that the configuration is working properly.

- [Verifying That DHCP Snooping Is Working Correctly on the Switch on page 64](#)
- [Verifying That DAI Is Working Correctly on the Switch on page 65](#)

---

### Verifying That DHCP Snooping Is Working Correctly on the Switch

**Purpose** Verify that DHCP snooping is working on the switch.

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

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

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

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

### Verifying That DAI Is Working Correctly on the Switch

**Purpose** Verify that DAI is working on the switch.

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

Display the DAI information:

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

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

**Related Documentation**

- [Example: Configuring Basic Port Security Features on page 43](#)
- [Enabling DHCP Snooping \(CLI Procedure\) on page 132](#)
- [Enabling DHCP Snooping \(J-Web Procedure\) on page 135](#)
- [Enabling Dynamic ARP Inspection \(CLI Procedure\) on page 137](#)

- [Enabling Dynamic ARP Inspection \(J-Web Procedure\) on page 139](#)
- [secure-access-port on page 231](#)
- [secure-access-port](#)
- [show arp inspection statistics on page 277](#)
- [show dhcp snooping binding on page 278](#)

## 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 on page 66](#)
- [Overview and Topology on page 67](#)
- [Configuration on page 68](#)
- [Verification on page 68](#)

### Requirements

This example uses the following hardware and software components:

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

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

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

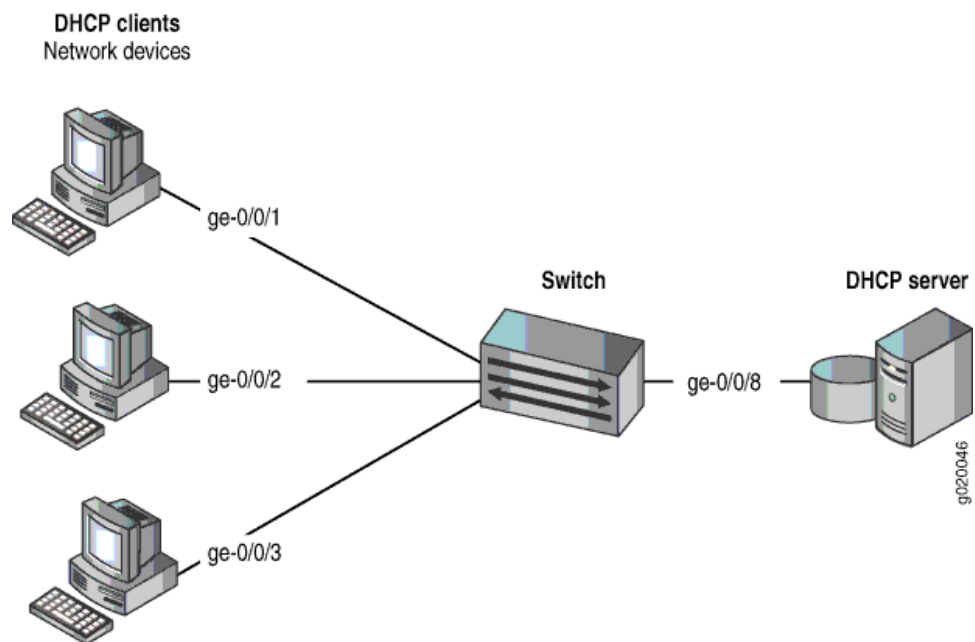
## Overview and Topology

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

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

The setup for this example includes the VLAN **employee-vlan** on the switch. [Figure 12 on page 67](#) 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 9 on page 67](#).

**Table 9: Components of the Port Security Topology**

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	<b>employee-vlan</b> , 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 <b>employee-vlan</b>	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface for DHCP server	ge-0/0/8

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

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

## Configuration

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

### CLI Quick Configuration

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

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

### Step-by-Step Procedure

To configure some allowed MAC addresses on an interface:

Configure the five allowed MAC addresses on an interface:

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

### Results

Check the results of the configuration:

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

## Verification

Confirm that the configuration is working properly.

- [Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 68](#)

### Verifying That Allowed MAC Addresses Are Working Correctly on the Switch

#### Purpose

Verify that allowed MAC addresses are working on the switch.



**Action** Display the MAC cache information:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 6 entries, 5 learned
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:88	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

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

- Related Documentation**
- [Example: Configuring Basic Port Security Features on page 43](#)
  - [Configuring MAC Limiting \(CLI Procedure\) on page 140](#)
  - [Configuring MAC Limiting \(J-Web Procedure\) on page 143](#)
  - [secure-access-port on page 231](#)
  - *secure-access-port*
  - [show ethernet-switching table on page 284](#)
  - *show ethernet-switching table*

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

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

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

- [Requirements on page 70](#)
- [Overview and Topology on page 70](#)
- [Configuring a VLAN, Interfaces, and Port Security Features on Switch 1 on page 72](#)
- [Configuring a VLAN and Interfaces on Switch 2 on page 74](#)
- [Verification on page 75](#)

## Requirements

This example uses the following hardware and software components:

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

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

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

## Overview and Topology

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

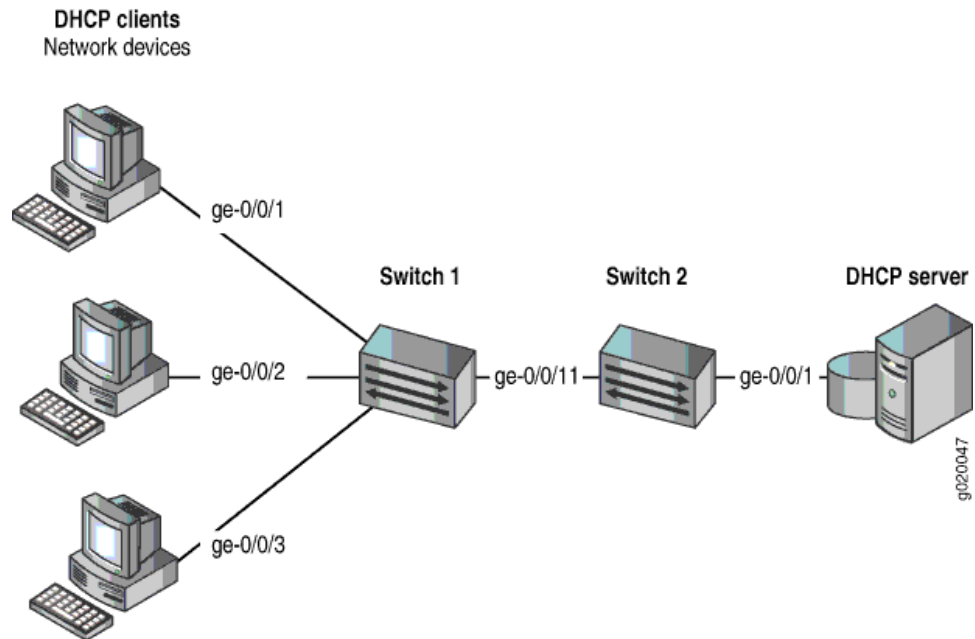
- DHCP snooping to validate DHCP server messages
- DAI to protect against ARP spoofing
- MAC limiting to constrain the number of MAC addresses the switch adds to its MAC address cache

This example shows how to configure these port security features on Switch 1. Switch 1 is connected to another switch (Switch 2), which is not configured with port security features. Switch 2 is connected to a DHCP server (see [Figure 13 on page 71](#).) Network devices (hosts) that are connected to Switch 1 send requests for IP addresses (these network devices are DHCP clients). Those requests are transmitted from Switch 1 to Switch 2 and then to the DHCP server connected to Switch 2. Responses to the requests are transmitted along the reverse path of the one followed by the requests.

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

[Figure 13 on page 71](#) 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 10 on page 71](#).

**Table 10: Components of Port Security Setup on Switch 1 with a DHCP Server Connected to Switch 2**

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

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

- Secure port access is activated on the switch.
- The switch does not drop any packets, which is the default setting.

- DHCP snooping and DAI are disabled on all VLANs.
- All access interfaces are untrusted and trunk interfaces are trusted; these are the default settings.

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

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

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

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

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

```
[edit]
set vlans employee-vlan vlan-id 20
set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members 20
set ethernet-switching-options secure-access-port interface ge-0/0/1 mac-limit 5 action drop
set ethernet-switching-options secure-access-port vlan employee-vlan arp-inspection
set ethernet-switching-options secure-access-port vlan employee-vlan examine-dhcp
clear ethernet-switching table interface ge-0/0/1
```

**Step-by-Step Procedure** To configure MAC limiting, a VLAN, and interfaces on Switch 1 and enable DAI and DHCP on the VLAN:

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

```
[edit vlans]
user@switch1# set employee-vlan vlan-id 20
```
2. Configure an interface on Switch 1 as a trunk interface:  

```
[edit interfaces]
user@switch1# set ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
```
3. Associate the VLAN with interfaces ge-0/0/1, ge-0/0/2, ge-0/0/3, and ge-0/0/11:  

```
[edit interfaces]
user@switch1# set ge-0/0/1 unit 0 family ethernet-switching vlan members 20
user@switch1# set ge-0/0/2 unit 0 family ethernet-switching vlan members 20
user@switch1# set ge-0/0/3 unit 0 family ethernet-switching vlan members 20
user@switch1# set ge-0/0/11 unit 0 family ethernet-switching vlan members 20
```
4. Enable DHCP snooping on the VLAN:  

```
[edit ethernet-switching-options secure-access-port]
user@switch1# set vlan employee-vlan examine-dhcp
```
5. Enable DAI on the VLAN:  

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

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

```
[edit ethernet-switching-options secure-access-port]
```

```
user@switch1# set interface ge-0/0/1 mac-limit 5 drop
```

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

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

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

```
[edit]
user@switch1# show
ethernet-switching-options {
  secure-access-port {
    interface ge-0/0/1.0 {
      mac-limit 5 action drop;
    }
    vlan employee-vlan {
      arp-inspection;
      examine-dhcp;
    }
  }
}
interfaces {
  ge-0/0/1 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members 20;
        }
      }
    }
  }
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members 20;
        }
      }
    }
  }
  ge-0/0/3 {
    unit 0 {
      family ethernet-switching {
        vlan {
          port-mode trunk;
          members 20;
        }
      }
    }
  }
  ge-0/0/11 {
    unit 0 {
      family ethernet-switching {
```

```
        port-mode trunk;
        vlan {
            members 20;
        }
    }
}
}
}
vlangs {
    employee-vlan {
        vlan-id 20;
    }
}
```

## Configuring a VLAN and Interfaces on Switch 2

To configure the VLAN and interfaces on Switch 2:

### CLI Quick Configuration

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

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

### Step-by-Step Procedure

To configure the VLAN and interfaces on Switch 2:

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

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

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

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

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

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

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

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

```

unit 0 {
    family ethernet-switching {
        port-mode trunk;
        vlan {
            members 20;
        }
    }
}
}
}
}
vllans {
    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 75](#)
- [Verifying That DAI Is Working Correctly on Switch 1 on page 76](#)
- [Verifying That MAC Limiting Is Working Correctly on Switch 1 on page 76](#)

### Verifying That DHCP Snooping Is Working Correctly on Switch 1

**Purpose** Verify that DHCP snooping is working on Switch 1.

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

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

```
user@switch1> show dhcp snooping binding
```

DHCP Snooping Information:

MAC Address	IP Address	Lease	Type	VLAN	Interface
-----	-----	-----	----	----	-----
00:05:85:3A:82:77	192.0.2.17	600	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:79	192.0.2.18	653	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:80	192.0.2.19	720	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:81	192.0.2.20	932	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:83	192.0.2.21	1230	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:90	192.0.2.20	932	dynamic	employee-vlan	ge-0/0/2.0
00:05:85:3A:82:91	192.0.2.21	1230	dynamic	employee-vlan	ge-0/0/3.0

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

### Verifying That DAI Is Working Correctly on Switch 1

**Purpose** Verify that DAI is working on Switch 1.

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

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

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

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

### Verifying That MAC Limiting Is Working Correctly on Switch 1

**Purpose** Verify that MAC limiting is working on Switch 1.

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

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

Ethernet-switching table: 6 entries, 5 learned
VLAN          MAC address      Type      Age      Interfaces
-----
employee-vlan  00:05:85:3A:82:77 Learn      0      ge-0/0/1.0
employee-vlan  00:05:85:3A:82:79 Learn      0      ge-0/0/1.0
employee-vlan  00:05:85:3A:82:80 Learn      0      ge-0/0/1.0
employee-vlan  00:05:85:3A:82:81 Learn      0      ge-0/0/1.0
employee-vlan  00:05:85:3A:82:83 Learn      0      ge-0/0/1.0
employee-vlan  *                Flood     -      ge-0/0/1.0
```

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

**Related Documentation**

- [Example: Configuring Basic Port Security Features on page 43](#)
- [Configuring Port Security \(CLI Procedure\) on page 110](#)
- [Configuring Port Security \(J-Web Procedure\) on page 112](#)
- [secure-access-port on page 231](#)



- *secure-access-port*
- [show arp inspection statistics on page 277](#)
- [show dhcp snooping binding on page 278](#)
- [show ethernet-switching table on page 284](#)
- *show ethernet-switching table*

## 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 on page 77](#)
- [Overview and Topology on page 78](#)
- [Configuring IP Source Guard with 802.1X Authentication, DHCP Snooping, and Dynamic ARP Inspection on page 79](#)
- [Configuring IP Source Guard on a Guest VLAN on page 82](#)
- [Verification on page 85](#)

### Requirements

This example uses the following hardware and software components:

- An 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 scenarios related in this example, be sure you have:

- Connected the DHCP server to the switch.
- Connected the RADIUS server to the switch and configured user authentication on the RADIUS server. See *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*.

- Configured VLANs on the switch. In this example, we have two VLANs, which are named **DATA** and **GUEST**. The **DATA** VLAN is configured with **vlan-id 300**. The **GUEST** VLAN (which functions as the guest VLAN) is configured with **vlan-id 100**. 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 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**. A DHCP server can be connected to a **dhcp-trusted** interface to provide dynamic IP addresses.

IP source guard obtains information about IP-addresses, MAC-addresses, or VLAN bindings from the DHCP snooping database, which enables the switch to validate incoming IP packets against the entries in that database.

The topology for this example includes an EX Series switch, which is connected to both a DHCP server and to a RADIUS server.



**NOTE:** The 802.1X user authentication applied in this example is for single-supplicant mode.

You can 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 configuration example, 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 configuration example, 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.



**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 other access interfaces (untrusted) 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-0/0/0.0;
  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;
    }
}
}

```

## 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 GUEST
set ethernet-switching-options secure-access-port vlan GUEST examine-dhcp
set ethernet-switching-options secure-access-port vlan GUEST 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 GUEST
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 GUEST
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 GUEST
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 GUEST
set protocols dot1x authenticator interface ge-0/0/1 supplicant-timeout 2

```

**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 **GUEST** 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 GUEST

```

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 **GUEST** VLAN:

```

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

```

4. Configure a static IP address on each of two (untrusted) interfaces on the **GUEST** 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 GUEST
[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 GUEST

```

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
```

**Results** Check the results of the configuration:

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

[edit vlans]
GUEST {
  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 GUEST;
      }
    }
  }
}

[edit ethernet-switching-options]
secure-access-port {
  interface ge-0/0/0.0 {
    static-ip 11.1.1.1 vlan GUEST mac 00:11:11:11:11:11;
  }
}
```



```

    }
    interface ge-0/0/1.0 {
        static-ip 11.1.1.2 vlan GUEST mac 00:22:22:22:22:22;
    }
    interface ge-0/0/24.0 {
        dhcp-trusted;
    }
    vlan GUEST {
        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 85](#)
- [Verifying the VLAN Association with the Interface on page 86](#)
- [Verifying That DHCP Snooping Is Working on the VLAN on page 86](#)
- [Verifying That IP Source Guard Is Working on the VLAN on page 86](#)

### Verifying That 802.1X User Authentication Is Working on the Interface

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

**Action** user@switch> show dot1x interface ge-0/0/0.0 detail  
ge-0/0/0.0  
Role: Authenticator  
Administrative state: Auto  
Supplicant mode: Single  
Number of retries: 2  
Quiet period: 30 seconds  
Transmit period: 15 seconds  
Mac Radius: Disabled  
Mac Radius Restrict: Disabled  
Reauthentication: Enabled  
Configured Reauthentication interval: 3600 seconds  
Supplicant timeout: 2 seconds  
Server timeout: 30 seconds  
Maximum EAPOL requests: 1  
Guest VLAN member: GUEST  
Number of connected supplicants: 1  
Supplicant: md5user01, 00:30:48:90:53:B7  
Operational state: Authenticated  
Backend Authentication state: Idle  
Authentication method: Radius  
Authenticated VLAN: DATA  
Session Reauth interval: 3600 seconds  
Reauthentication due in 3581 seconds

**Meaning** The **Supplicant mode** field displays the configured administrative mode for each interface.  
The **Guest VLAN member** field displays the VLAN to which a supplicant is connected

when the supplicant is authenticated using a guest VLAN. The **Authenticated VLAN** field displays the VLAN to which the supplicant is connected.

### Verifying the VLAN Association with the Interface

**Purpose** Verify interface states and VLAN memberships.

**Action** user@switch> **show ethernet-switching interfaces**

Interface	State	VLAN members	Tag	Tagging	Blocking
ge-0/0/0.0	up	DATA	101	untagged	unblocked
ge-0/0/1.0	up	DATA	101	untagged	unblocked
ge-0/0/24	up	DATA	101	untagged	unblocked

**Meaning** The **VLAN members** field 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 Is Working on the VLAN

**Purpose** Verify that DHCP snooping is enabled and working on the VLAN. Send some DHCP requests from network devices (DHCP clients) connected to the switch.

**Action** user@switch> **show dhcp snooping binding**

DHCP Snooping Information:

MAC address	IP address	Lease (seconds)	Type	VLAN	Interface
00:30:48:90:53:B7	212.2.1.241	86392	dynamic	DATA	ge-0/0/24.0

**Meaning** When the interface on which the DHCP server connects to the switch has been set to **dhcp-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.

### Verifying That IP Source Guard Is Working on the VLAN

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

**Action** user@switch> **show ip-source-guard**

IP source guard information:

Interface	Tag	IP Address	MAC Address	VLAN
ge-0/0/0.0	0	212.2.1.242	00:30:48:90:63:B7	DATA
ge-0/0/1.0	0	212.2.1.243	00:30:48:90:73:B7	DATA

**Meaning** The IP source guard database table contains the VLANs for which IP source guard is enabled, 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 have IP source guard enabled (or configured) while others do not have IP source guard enabled,

the VLANs that do not have IP source guard enabled have a star (\*) in the **IP Address** and **MAC Address** fields.

**Related  
Documentation**

- [Example: Configuring Basic Port Security Features on page 43](#)
- [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 87](#)
- [Configuring IP Source Guard \(CLI Procedure\) on page 148](#)

## 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 on page 87](#)
- [Overview and Topology on page 88](#)
- [Configuration on page 89](#)
- [Verification on page 91](#)

## 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 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 \(Access Port Security\)](#) 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 {
        suplicant 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 91](#)
- [Verifying the VLAN Association with the Interface on page 92](#)
- [Verifying That DHCP Snooping and IP Source Guard Are Working on the Data VLAN on page 92](#)

### 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 77](#)
  - [Example: Configuring Basic Port Security Features on page 43](#)
  - [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
  - [Configuring IP Source Guard \(CLI Procedure\) on page 148](#)

## Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing

---

This example describes how to enable IPv6 source guard and neighbor discovery inspection on a specified VLAN to protect an EX Series switch against IPv6 address spoofing attacks.

- [Requirements on page 94](#)
- [Overview and Topology on page 94](#)
- [Configuration on page 96](#)
- [Verification on page 96](#)

### Requirements

This example uses the following hardware and software components:

- One EX2200 or EX3300 switch
- Junos OS Release 14.1X53-D10 or later for EX Series switches
- A DHCPv6 server to provide IPv6 addresses to network devices on the switch

Before you configure IPv6 source guard and neighbor discovery inspection to prevent IPv6 address spoofing attacks, be sure you have:

- Connected the DHCPv6 server to the switch.
- Configured the VLAN to which you are adding DHCPv6 security features. See *Configuring VLANs for EX Series Switches (CLI Procedure)*.

### Overview and Topology

Ethernet LAN switches are vulnerable to attacks on security that involve spoofing (forging) of source MAC addresses or source IPv6 addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. For more information on IPv6 address spoofing attacks, see [“Understanding IPv6 Neighbor Discovery Inspection” on page 23](#).

IPv6 source guard and neighbor discovery inspection mitigate the risk of IPv6 spoofing attacks by using the DHCPv6 snooping table. Also known as the binding table, the DHCPv6 snooping table contains the valid bindings of IPv6 addresses to MAC addresses. When a packet is sent from a host attached to an untrusted access interface on the switch, IPv6 source guard verifies the source IPv6 address and MAC address of the packet against

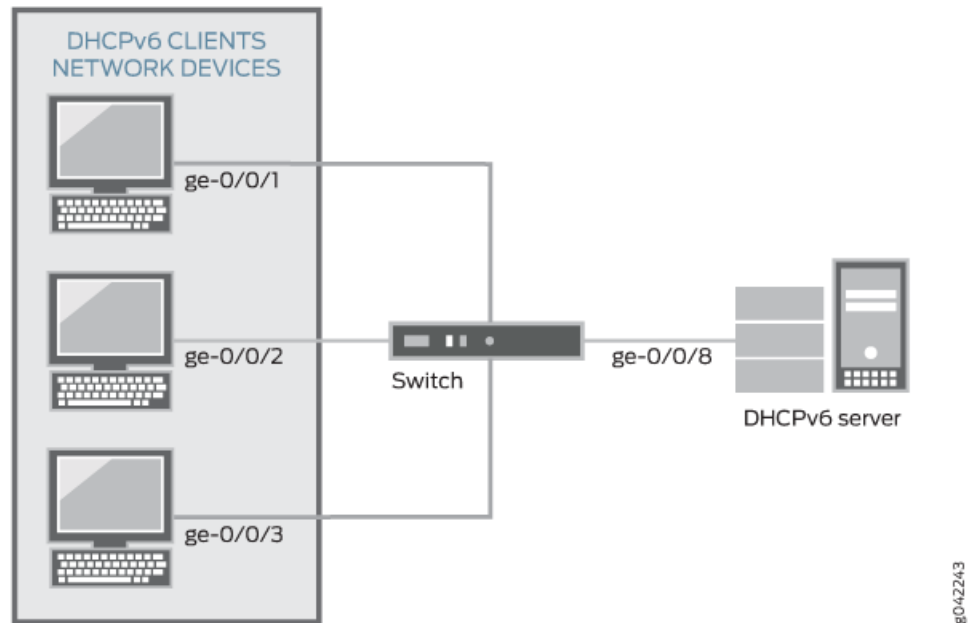
the DHCPv6 snooping table. If there is no match in the table, the switch does not forward the packet—that is, the packet is discarded. Neighbor discovery inspection verifies neighbor discovery messages sent between IPv6 nodes on the same network link against the DHCPv6 snooping table, and also discards the packet if no match is found.

This example shows how to configure these important port security features on a switch that is connected to a DHCPv6 server. The setup for this example includes the VLAN **sales** on the switch. [Figure 11 on page 63](#) illustrates the topology for this example.



**NOTE:** The trunk interface connecting to the DHCPv6 server interface is a trusted port by default.

Figure 14: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 8 on page 63](#).

Table 11: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX2200 or EX3300 switch
VLAN name and ID	sales, tag
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 <b>sales</b>	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8

Table 11: Components of the Port Security Topology (*continued*)

Properties	Settings
Interface connecting to DHCPv6 server	ge-0/0/8

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

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

## Configuration

**CLI Quick Configuration** To quickly configure IPv6 source guard and neighbor discovery inspection, copy the following commands and paste them into the switch terminal window:

```
[edit]
set ethernet-switching-options secure-access-port vlan sales examine-dhcpv6
set ethernet-switching-options secure-access-port vlan sales ipv6-source-guard
set ethernet-switching-options secure-access-port vlan sales neighbor-discovery-inspection
```

**Step-by-Step Procedure** Configure IPv6 source guard and neighbor discovery inspection (and thereby, also automatically configure DHCPv6 snooping) on the VLAN:

1. Enable DHCPv6 snooping on the VLAN:

```
[edit ethernet-switching-options secure-access-port vlan sales]
user@switch# set examine-dhcpv6
```
2. Configure IPv6 source guard on the VLAN:

```
[edit ethernet-switching-options secure-access-port vlan sales]
user@switch# set ipv6-source-guard
```
3. Configure neighbor discovery inspection on the VLAN:

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

**Results** Check the results of the configuration:

```
user@switch> show ethernet-switching-options secure-access-port
vlan sales {
  examine-dhcpv6;
  ipv6-source-guard;
  neighbor-discovery-inspection;
}
```

## Verification

Confirm that the configuration is working properly.

- [Verifying That DHCPv6 Snooping Is Working Correctly on the Switch on page 97](#)
- [Verifying That Neighbor Discovery Inspection Is Working Correctly on the Switch on page 97](#)

### Verifying That DHCPv6 Snooping Is Working Correctly on the Switch

**Purpose** Verify that DHCPv6 snooping is working on the switch.

**Action** Send DHCPv6 requests from network devices (in this example, these are DHCPv6 clients) connected to the switch.

Display the DHCPv6 snooping information when the port on which the DHCPv6 server connects to the switch is trusted. The following is the output when requests are sent from the MAC addresses and the server has provided the IPv6 addresses and leases:

```
user@switch> show dhcpv6 snooping binding
```

DHCP Snooping Information:

MAC address	IP address	Lease (seconds)	Type	VLAN	Interface
00:10:94:00:00:01	3000::10:10:0:3	3599992	dynamic	sales	ge-0/0/1.0
00:10:94:00:00:01	fe80::210:94ff:fe00:1	3599992	dynamic	sales	ge-0/0/1.0
00:10:94:00:00:02	3000::10:10:0:4	3599992	dynamic	sales	ge-0/0/2.0
00:10:94:00:00:02	fe80::210:94ff:fe00:2	3599992	dynamic	sales	ge-0/0/2.0
00:10:94:00:00:03	3000::10:10:0:5	3599992	dynamic	sales	ge-0/0/3.0
00:10:94:00:00:03	fe80::210:94ff:fe00:3	3599992	dynamic	sales	ge-0/0/3.0

**Meaning** The output shows the assigned IP address, the MAC address, the VLAN name, and the time, in seconds, leased to the IP address. Because IPv6 hosts usually have more than one IP address assigned to each of their IPv6-enabled network interfaces, there are two entries added for each client: one with the link-local IP address, which is used by the client for DHCP transactions, and another with the IP address assigned by the server. The link-local address always has the prefix **fe80::/10**.

### Verifying That Neighbor Discovery Inspection Is Working Correctly on the Switch

**Purpose** Verify that neighbor discovery inspection is working on the switch.

**Action** Send neighbor discovery packets from network devices connected to the switch.

Display the neighbor discovery information:

```
user@switch> show neighbor-discovery-inspection statistics
```

ND inspection statistics:

Interface	Packets received	ND inspection pass	ND 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 neighbor discovery packets received and inspected per interface, and lists the number of packets passed and the number that failed the inspection on each interface. The switch compares the neighbor discovery requests and replies against the entries in the DHCPv6 snooping database. If a MAC address or IPv6 address in the neighbor discovery packet does not match a valid entry in the database, the packet is dropped.

- Related Documentation**
- [Configuring IP Source Guard \(CLI Procedure\) on page 148](#)
  - [Enabling DHCP Snooping \(CLI Procedure\) on page 132](#)
  - [Configuring Port Security \(CLI Procedure\) on page 110](#)

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

---

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

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

- [Requirements on page 98](#)
- [Overview and Topology on page 99](#)
- [Configuration on page 99](#)

### Requirements

This example uses the following hardware and software components:

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

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

- Connected and configured the DHCP server.



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

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

- Configured the switch as a BOOTP relay agent. See *DHCP/BOOTP Relay for Switches Overview*.
- Configured the routed VLAN interface (RVI) to allow the switch to relay packets to the server and receive packets from the server. See *Configuring Routed VLAN Interfaces (CLI Procedure)* or *Configuring IRB Interfaces* for the QFX Series.

## Overview and Topology

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

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

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

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

## Configuration

To configure DHCP option 82:

### CLI Quick Configuration

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

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

**Step-by-Step  
Procedure**

To configure DHCP option 82:

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

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82
```
2. Configure a prefix for the circuit ID suboption (the prefix is always the hostname of the switch):  

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 circuit-id prefix hostname
```
3. Specify that the circuit ID suboption value contains the VLAN ID rather than the VLAN name (the default):  

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 circuit-id use-vlan-id
```
4. Specify that the remote ID suboption be included in the DHCP option 82 information:  

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id
```
5. Configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):  

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id prefix mac
```
6. Specify that the remote ID suboption value contains a character string (here, the string is **employee-switch1**):  

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id use-string employee-switch1
```
7. Configure a vendor ID suboption value, and use the default value. To use the default value, do not type a character string after the **vendor-id** option keyword:  

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

**Results** Check the results of the configuration:

```
[edit forwarding-options helpers bootp]
user@switch# show
dhcp-option82 {
  circuit-id {
    prefix hostname;
    use-vlan-id;
  }
  remote-id {
    prefix mac;
    use-string employee-switch1;
  }
  vendor-id;
}
```

**Related  
Documentation**

- [Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101](#)
- [Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 153](#)



- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.
- *forwarding-options*

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

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

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

- [Requirements on page 101](#)
- [Overview and Topology on page 102](#)
- [Configuration on page 103](#)

### Requirements

This example uses the following hardware and software components:

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

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

- Connected and configured the DHCP server.



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

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

## Overview and Topology

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

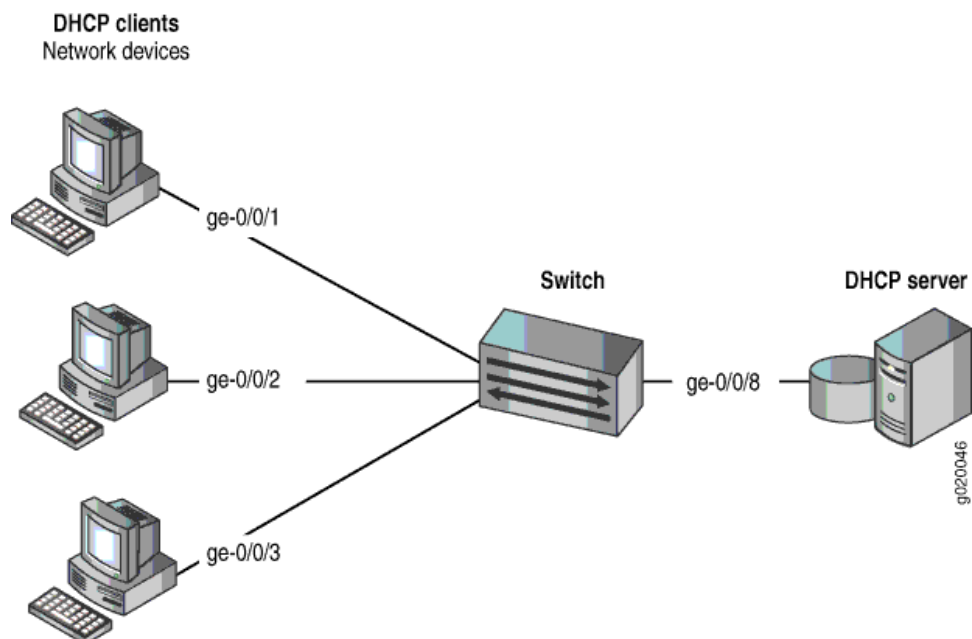
DHCP option 82 is enabled on an individual VLAN or on all VLANs on the switch.

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

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

Figure 15 on page 102 illustrates the topology for this example.

**Figure 15: Network Topology for Configuring DHCP Option 82 on a Switch That Is on the Same VLAN as the DHCP Clients and the DHCP Server**



In this example, you configure DHCP option 82 on the switch. The switch connects to the DHCP server on interface `ge-0/0/8`. The DHCP clients connect to the switch on interfaces

**ge-0/0/1**, **ge-0/0/2**, and **ge-0/0/3**. The switch, server, and clients are all members of the **employee** VLAN.

## Configuration

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

```

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

```

**Step-by-Step Procedure** To configure DHCP option 82:

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

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82
```
2. Configure a prefix for the circuit ID suboption (the prefix is always the hostname of the switch):  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 circuit-id prefix hostname
```
3. Specify that the circuit ID suboption value contains the VLAN ID rather than the VLAN name (the default):  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 circuit-id use-vlan-id
```
4. Specify that the remote ID suboption be included in the DHCP option 82 information:  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id
```
5. Configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id prefix mac
```
6. Specify that the remote ID suboption value contain a character string (here, the string is **employee-switch1**):  

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id use-string employee-switch1
```
7. Configure a vendor ID suboption value, and use the default value. To use the default value, do not type a character string after the **vendor-id** option keyword:  

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

**Results** Check the results of the configuration:

```

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

```

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

**Related  
Documentation**

- [Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 156](#)
- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.
- [secure-access-port on page 231](#)
- *secure-access-port*

---

## 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 on page 105](#)
- [Overview and Topology on page 105](#)
- [Configuration on page 106](#)
- [Verification on page 107](#)

## 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.

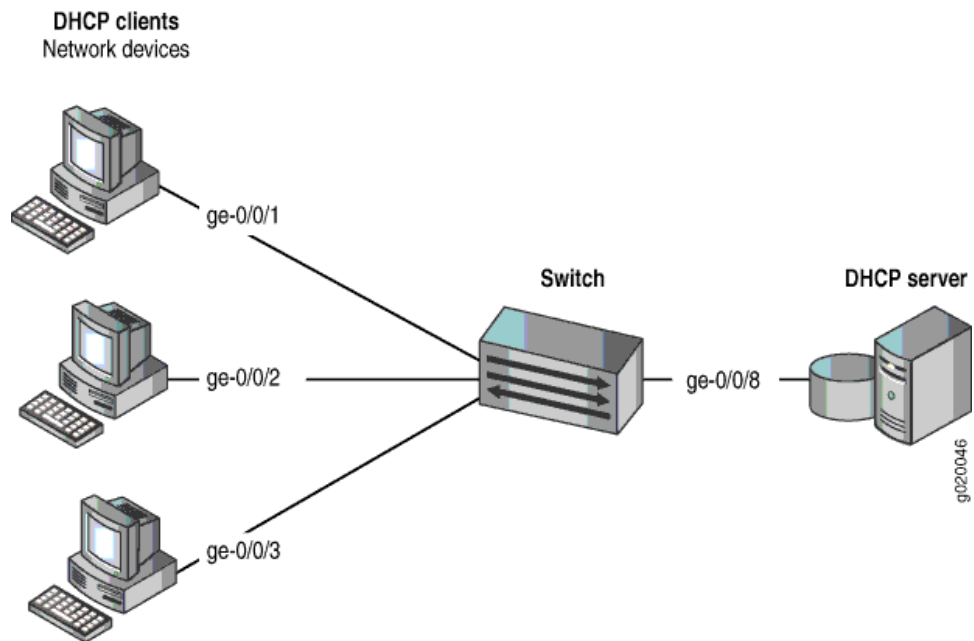
In the default switch configuration:

- 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 16 on page 106](#) illustrates the topology for this example.

Figure 16: 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 12 on page 106](#).

Table 12: 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 107](#)
- [Verifying That Prioritized Forwarding Is Working Correctly on the DAI Inspected Packets on page 108](#)

### 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 61](#)



## CHAPTER 4

# Configuration Tasks

- [Configuring Port Security \(CLI Procedure\) on page 110](#)
- [Configuring Port Security \(J-Web Procedure\) on page 112](#)
- [Configuring Media Access Control Security \(MACsec\) on page 116](#)
- [Enabling DHCP Snooping \(CLI Procedure\) on page 132](#)
- [Enabling DHCP Snooping \(J-Web Procedure\) on page 135](#)
- [Enabling a Trusted DHCP Server \(CLI Procedure\) on page 136](#)
- [Enabling a Trusted DHCP Server \(J-Web Procedure\) on page 136](#)
- [Enabling Dynamic ARP Inspection \(CLI Procedure\) on page 137](#)
- [Enabling Dynamic ARP Inspection \(J-Web Procedure\) on page 139](#)
- [Configuring MAC Limiting \(CLI Procedure\) on page 140](#)
- [Configuring MAC Limiting \(J-Web Procedure\) on page 143](#)
- [Configuring MAC Move Limiting \(CLI Procedure\) on page 145](#)
- [Configuring MAC Move Limiting \(J-Web Procedure\) on page 147](#)
- [Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces \(CLI Procedure\) on page 148](#)
- [Configuring IP Source Guard \(CLI Procedure\) on page 148](#)
- [Configuring Static IP Addresses for DHCP Bindings on Access Ports \(CLI Procedure\) on page 152](#)
- [Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 153](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 156](#)
- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 159](#)
- [Configuring Persistent MAC Learning \(CLI Procedure\) on page 159](#)
- [Making IP-MAC Bindings in the DHCP Snooping Database Persistent \(CLI Procedure\) on page 161](#)

## Configuring Port Security (CLI Procedure)

---

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

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

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



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

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

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

---

To configure port security features by using the CLI:

- [Enabling DHCP Snooping on page 110](#)
- [Enabling Dynamic ARP Inspection \(DAI\) on page 111](#)
- [Enabling IPv6 Neighbor Discovery Inspection on page 111](#)
- [Limiting Dynamic MAC Addresses on an Interface on page 111](#)
- [Enabling Persistent MAC Learning on an Interface on page 112](#)
- [Limiting MAC Address Movement on page 112](#)
- [Configuring Trusted DHCP Servers on an Interface on page 112](#)

### Enabling DHCP Snooping

You can configure DHCP snooping to enable the device to monitor DHCP messages received, ensure that hosts use only the IP addresses that are assigned to them, and allow access only to authorized DHCP servers.

To enable DHCP snooping:

- 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
```

To enable DHCPv6 snooping:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name examine-dhcpv6
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all examine-dhcpv6
```

## Enabling Dynamic ARP Inspection (DAI)

You can enable DAI to protect against ARP snooping. To enable DAI:

- On a single VLAN:

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

- On all VLANs:

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

## Enabling IPv6 Neighbor Discovery Inspection

You can enable neighbor discovery inspection to protect against IPv6 address spoofing.

- To enable neighbor discovery on a single VLAN:

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

- To enable neighbor discovery on all VLANs:

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

## Limiting Dynamic MAC Addresses on an Interface

Limit the number of dynamic MAC addresses allowed on an interface and specify the action to take if the limit is exceeded:

- On a single interface:

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

- On all interfaces:

```
[edit ethernet-switching-options secure-access-port]
```

```
user@switch# set interface all mac-limit limit action action
```

## Enabling Persistent MAC Learning on an Interface

You can configure learned MAC addresses to persist on an interface across restarts of the switch:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name persistent-learning
```

## Limiting MAC Address Movement

You can limit the number of times a MAC address can move from its original interface in 1 second:

- On a single VLAN:

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

- On all VLANs:

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

## Configuring Trusted DHCP Servers on an Interface

Configure a trusted DHCP server on an interface:

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

### Related Documentation

- [Configuring Port Security \(J-Web Procedure\) on page 112](#)
- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 159](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
- [Monitoring Port Security on page 253](#)
- [Understanding Port Security on page 7](#)
- [secure-access-port on page 231](#)
- [secure-access-port](#)

---

## Configuring Port Security (J-Web Procedure)



NOTE: This topic applies only to the J-Web Application package.

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 on 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 of the following options:

- **Edit**—Click this option to modify the security features for the selected port or VLAN.  
Enter information as specified in [Table 13 on page 113](#) to modify port security settings on VLANs.  
Enter information as specified in [Table 14 on page 115](#) to modify port security settings on interfaces.
- **Activate/Deactivate**—Click this option to enable or disable security on the switch.



**NOTE:** This option is not supported on EX4300 switches.

- **Delete**—Click this option to delete the security features of the selected port or VLAN.



**NOTE:** This option is supported only on EX4300 switches.

**Table 13: Port Security Settings on VLANs**

Field	Function	Your Action
General tab		
Enable DHCP Snooping on VLAN  <b>NOTE:</b> On EX4300 switches, DHCP snooping is enabled implicitly for all VLANs if you configure <b>dhcp-security</b> on one or more VLANs.	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.  <b>TIP:</b> For private VLANs (P-VLANs), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from P-VLAN 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 13: Port Security Settings on VLANs (*continued*)

Field	Function	Your Action
MAC movement	Number of MAC movements allowed on the given VLAN.	Enter a number. The default is unlimited.
MAC movement action	Specifies the action to be taken if the MAC movement limit is exceeded.	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>log</b>—Generate a system log entry, an SNMP trap, or an alarm.</li> <li>• <b>drop</b>—Drop the packets and generate a system log entry, an SNMP trap, or an alarm (default).</li> <li>• <b>shutdown</b>—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 <b>disable timeout</b> value. See <a href="#">“Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)”</a> on page 159.</li> <li>• <b>none</b>—Take no action.</li> </ul> <p>EX4300 switches have an additional option:</p> <ul style="list-style-type: none"> <li>• <b>drop-and-log</b>—Drop the packet and generate an alarm, an SNMP trap, or a system log entry.</li> </ul>
DHCP Groups		
Group Name <b>NOTE:</b> This option is supported only on EX4300 switches.	Specifies the DHCP name of the group.	Enter a name.
Trusted <b>NOTE:</b> This option is supported only on EX4300 switches.	Specifies trusting DHCP packets on the selected interface. By default, trunk ports are <b>dhcp-trusted</b> .	To enable this option, select the check box.
No Option-82 <b>NOTE:</b> This option is supported only on EX4300 switches.	Enable or disable the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.	To enable this option, select the check box.
Interfaces <b>NOTE:</b> This option is supported only on EX4300 switches.	Specifies the DHCP interface.	Select the required interface.
Ports		
Interface <b>NOTE:</b> This option is supported only on EX4300 switches.	Name of the interface.	Click the <b>Edit</b> button of the selected interface, to configure the MAC limit and the MAC limit action.

Table 13: Port Security Settings on VLANs (*continued*)

MAC Limit  <b>NOTE:</b> This option is supported only on EX4300 switches.	Maximum number of MAC addresses learned on the interface.	Enter a number. The default is unlimited.
MAC Limit Action  <b>NOTE:</b> This option is supported only on EX4300 switches.	Specifies the action to be taken if the MAC move limit is exceeded.	<p>Action to be taken when MAC limit is reached. The options are:</p> <ul style="list-style-type: none"> <li>• <b>drop</b>—Drop the packet and do not learn. Default is forward.</li> <li>• <b>drop-and-log</b>—Drop the packet and generate an alarm, an SNMP trap, or a system log entry.</li> <li>• <b>log</b>—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.</li> <li>• <b>none</b>—Forward the packet.</li> <li>• <b>shutdown</b>—Disable the interface and generate an alarm, an SNMP trap, or a system log entry.</li> </ul>

Table 14: Port Security on Interfaces

Field	Function	Your Action
Trust DHCP  <b>NOTE:</b> This option is not supported on EX4300 switches.	Specifies trusting DHCP packets on the selected interface. By default, trunk ports are <b>dhcp-trusted</b> .	Select to enable DHCP trust.
MAC Limit	<p>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.</p> <p><b>NOTE:</b> Trunk ports are supported only on EX4300 switches.</p>	Enter a number.

Table 14: Port Security on Interfaces (*continued*)

Field	Function	Your Action
MAC Limit Action	Specifies the action to be taken if the MAC limit is exceeded. This option is not valid for trunk ports.	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>log</b>—Generate a system log entry, an SNMP trap, or an alarm.</li> <li>• <b>drop</b>—Drop the packets and generate a system log entry, an SNMP trap, or an alarm. (Default)</li> <li>• <b>shutdown</b>—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 <b>disable timeout</b> value. See <a href="#">“Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)” on page 159</a></li> <li>• <b>none</b>—Take no action.</li> </ul> <p>EX4300 switches have an additional option:</p> <ul style="list-style-type: none"> <li>• <b>drop-and-log</b>—Drop the packet and generate an alarm, an SNMP trap, or a system log entry.</li> </ul>
Allowed MAC List	Specifies the MAC addresses that are allowed for the interface.	<p>To add a MAC address:</p> <ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. Enter the MAC address.</li> <li>3. Click <b>OK</b>.</li> </ol>

- Related Documentation**
- [Configuring Port Security \(CLI Procedure\) on page 110](#)
  - [Example: Configuring Basic Port Security Features on page 43](#)
  - [Monitoring Port Security on page 253](#)
  - [Understanding Port Security on page 7](#)

## Configuring Media Access Control Security (MACsec)

Media Access Control Security (MACsec) is an industry-standard security technology that provides secure communication for almost all types of traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly-connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec is standardized in IEEE 802.1AE.

You can configure MACsec to secure point-to-point Ethernet links connecting EX Series or QFX Series switches, or on Ethernet links connecting a switch to a host device such as a PC, phone, or server. Each point-to-point Ethernet link that you want to secure using MACsec must be configured independently. You can enable MACsec on switch-to-switch links using static secure association key (SAK) security mode or static connectivity association key (CAK) security mode. Both processes are provided in this document.





**BEST PRACTICE:** We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

The configuration steps for both processes are provided in this document.

- [Acquiring and Downloading the Junos OS Software on page 117](#)
- [Acquiring and Downloading the MACsec Feature License on page 118](#)
- [Configuring the PIC Mode of the MACsec-capable Interfaces \(EX4200 switches only\) on page 119](#)
- [Configuring MACsec Using Static Connectivity Association Key Security Mode \(Recommended for Enabling MACsec on Switch-to-Switch Links\) on page 120](#)
- [Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link on page 124](#)
- [Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link on page 128](#)

## Acquiring and Downloading the Junos OS Software

MACsec was initially released on EX Series switches in Junos OS Release 13.2X50-D15. MACsec was released on EX4600 and QFX5100-24Q switches in Junos OS Release 14.1X53-D15. The switches on each end of a MACsec-secured switch-to-switch link must either both be using Junos OS Release 14.1X51-D10 or later, or must both be using an earlier version of Junos, in order to establish a MACsec-secured connection when using static CAK security mode.

You must download the controlled version of your Junos OS software to enable MACsec. MACsec software support is not available in the domestic version of your Junos OS software. The controlled version of Junos OS software includes all features and functionality available in the domestic version of Junos OS, while also supporting MACsec. The domestic version of Junos OS software is shipped on all EX Series and QFX Series switches, so you must download and install a controlled version of Junos OS software on your switch before you can enable MACsec.

You can identify whether a software package is the controlled or domestic version of Junos OS by viewing the package name. A software package for a controlled version of Junos OS is named using the following format:

***package-name-m.nZx.y-controlled-signed.tgz***

A software package for a domestic version of Junos OS is named using the following format:

***package-name-m.nZx.y-domestic-signed.tgz***

If you are unsure which version of Junos OS is running on your switch, enter the **show version** command. If the “JUNOS Crypto Software Suite” description appears in the output, you are running the controlled version of Junos OS.

The controlled version of Junos OS software contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS software is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring the controlled version of your Junos OS software, contact Juniper Networks Trade Compliance group at [compliance\\_helpdesk@juniper.net](mailto:compliance_helpdesk@juniper.net).

The process for installing the controlled version of Junos OS software on your switch is identical to installing the domestic version of Junos OS software. You must enter the **request system software add** statement to download the Junos OS image, and the **request system reboot** statement to reboot the switch to complete the upgrade procedure. See *Downloading Software Packages from Juniper Networks, Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)*, and *Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)* for detailed information about acquiring and installing Junos OS software images for your switches.

## Acquiring and Downloading the MACsec Feature License

A feature license is required to configure MACsec on an EX Series or a QFX Series switch.

The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series or QFX Series switches cannot be purchased to enable MACsec.

To purchase a software license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key. You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

For a Virtual Chassis deployment, two MACsec license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role

To add one or more new MACsec license keys on the switch, follow this procedure:

1. Add the license key or keys:
  - To add one or more license keys from a file or URL, specify the filename of the file or the URL where the key is located:  

```
user@switch> request system license add filename |url
```
  - To add a license key from the terminal:  

```
user@switch> request system license add terminal
```
2. When prompted, enter the license key, separating multiple license keys with a blank line.

If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit the license entry mode.

A MACsec feature license is installed and maintained like any other switch license. See *Managing Licenses for the EX Series Switch (CLI Procedure)* or *Adding New Licenses (CLI Procedure)* for more detailed information on configuring and managing your MACsec software license.

## Configuring the PIC Mode of the MACsec-capable Interfaces (EX4200 switches only)

To configure MACsec on an EX4200 switch, you must install the SFP+ MACsec uplink module. The interfaces on the SFP+ MACsec uplink module are the only MACsec-capable interfaces available for EX4200 switches. All four ports on the uplink module are MACsec-capable.

The SFP+ MACsec uplink module provides two ports for 10-gigabit small form-factor pluggable (SFP+) transceivers when configured to operate in 10-gigabit mode or four ports for 1-gigabit small form-factor pluggable (SFP) transceivers when configured to operate in 1-gigabit mode.

The PIC mode is set to **10g**, by default. You only need to perform this procedure if you want to operate your uplink in 1-gigabit mode, or if you previously set the uplink module to 1-gigabit mode and would like to return it to 10-gigabit mode.

To configure the PIC mode:

```
[edit chassis]
user@switch# set fpc fpc-slot-number pic 1 sfpplus pic-mode (1g | 10g)
```

where *fpc-slot-number* is the FPC slot number, *pic-slot-number* is the PIC slot number, and the **[1g | 10g]** option configures the MACsec capability of the four SFP+ ports on the MACsec uplink module.

The *fpc-slot-number* is always 0 on standalone EX4200 switches, and is the member ID of the member switch in an EX4200 Virtual Chassis.

The PIC slot number is always 1 for the uplink module port slot on an EX4200 switch, so **pic 1** is always the specified PIC slot number.

The PIC mode is set to **10g** by default. When the PIC mode is set to **10g**, uplink ports 0 and 2 on the MACsec uplink module support MACsec at 10-Gbps speeds. Ports 1 and 3 cannot be used to send any traffic.

When the PIC mode is set to **1g**, all four SFP+ ports on the MACsec uplink module support MACsec at 1-Gbps speeds.

## Configuring MACsec Using Static Connectivity Association Key Security Mode (Recommended for Enabling MACsec on Switch-to-Switch Links)

You can enable MACsec using static connectivity association key (CAK) security mode or static secure association keys (SAK) security mode on a point-to-point Ethernet link connecting switches. This procedure shows you how to configure MACsec using static CAK security mode.



**BEST PRACTICE:** We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

When you enable MACsec using static CAK security mode, a pre-shared key is exchanged between the switches on each end of the point-to-point Ethernet link. The pre-shared key includes a connectivity association name (CKN) and a connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

After the pre-shared keys are exchanged and verified, the MACsec Key Agreement (MKA) protocol, which enables and maintains MACsec on the link, is enabled. The MKA is responsible for selecting one of the two switches on the point-to-point link as the key server. The key server then creates a randomized security key that is shared only with the other device over the MACsec-secured link. The randomized security key enables and maintains MACsec on the point-to-point link. The key server will continue to periodically create and share a randomly-created security key over the point-to-point link for as long as MACsec is enabled.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels—one for inbound traffic and one for outbound traffic—are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

To configure MACsec using static CAK security mode to secure a switch-to-switch Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1
```

2. Configure the MACsec security mode as **static-cak** for the connectivity association:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name security-mode
static-cak
```

For instance, to configure the MACsec security mode to **static-cak** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 security-mode static-cak
```

3. Create the pre-shared key by configuring the connectivity association key name (CKN) and connectivity association key (CAK):

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name pre-shared-key
ckn hexadecimal-number
user@switch# set connectivity-association connectivity-association-name pre-shared-key
cak hexadecimal-number
```

A pre-shared key is exchanged between directly-connected links to establish a MACsec-secure link. The pre-shared-key includes the CKN and the CAK. The CKN is a 64-digit hexadecimal number and the CAK is a 32-digit hexadecimal number. The CKN and the CAK must match on both ends of a link to create a MACsec-secured link.



**NOTE:** To maximize security, we recommend configuring all 64 digits of a CKN and all 32 digits of a CAK.

If you do not configure all 64 digits of a CKN or all 32 digits of a CAK, however, all remaining digits will be auto-configured to 0.

After the pre-shared keys are successfully exchanged and verified by both ends of the link, the MACsec Key Agreement (MKA) protocol is enabled and manages the secure link. The MKA protocol then elects one of the two directly-connected switches as the key server. The key server then shares a random security with the other device over the MACsec-secure point-to-point link. The key server will continue to periodically create and share a random security key with the other device over the MACsec-secured point-to-point link as long as MACsec is enabled.

To configure a CKN of **37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311** and CAK of **228ef255aa23ff6729ee664acb66e91f** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@switch# set connectivity-association ca1 pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```



**NOTE:** MACsec is not enabled until a connectivity association is attached to an interface. See the final step of this procedure to attach a connectivity association to an interface.

4. (Required on switches when connecting to EX4300 switches only) Enable SCI tagging:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set include-sci
```

You must enable SCI tagging on a switch that is enabling MACsec on an Ethernet link connecting to an EX4300 switch.

SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. This option is, therefore, not available on EX4300 switches.

You should only use this option when enabling MACsec on a link to an EX4300 switch. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16.

If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower *interval* increases bandwidth overhead on the link; a higher *interval* optimizes MKA protocol communication.

The default *interval* is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link when MACsec using static CAK security mode is enabled.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association *ca1* is attached to an interface:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using static CAK security mode, by default.

When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named *ca1*:

```
[edit security macsec connectivity-association ca1]
user@switch# set offset 30
```

The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an **offset** is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link.

When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance,

if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association **ca1** to interface **xe-0/0/1**:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca1
```

MACsec using static CAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and contains pre-shared keys that match on both ends of the link.

## Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link

Before you begin to enable MACsec on a switch-to-host link:

- Configure a RADIUS server. The RADIUS server:
  - must be configured as the user database for 802.1X authentication.
  - must be using the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework.



- must have connectivity to the switch and to the host. The RADIUS server can be multiple hops from the switch or the host.

See *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*.

- Enable MACsec on the host device.

The procedures for enabling MACsec on the host device varies by host device, and is beyond the scope of this document.

To configure MACsec using dynamic security mode to secure a switch-to-host Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named `ca-dynamic1`, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca-dynamic1
```

2. Configure the MACsec security mode as dynamic for the connectivity association:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name security-mode
dynamic
```

For instance, to configure the MACsec security mode to dynamic on connectivity association `ca-dynamic1`:

```
[edit security macsec]
user@switch# set connectivity-association ca-dynamic1 security-mode dynamic
```

3. (Optional) Configure the **must-secure** option:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name mka must-secure
```

When the **must-secure** option is enabled, all traffic that is not MACsec-secured that is received on the interface is dropped.

When the **must-secure** option is disabled, all traffic from devices that support MACsec is MACsec-secured while traffic received from devices that do not support MACsec is forwarded through the network.

The **must-secure** option is particularly useful in scenarios where multiple devices, such as a phone and a PC, are accessing the network through the same Ethernet interface. If one of the devices supports MACsec while the other device does not support MACsec, the device that doesn't support MACsec can continue to send and receive traffic over the network—provided the **must-secure** option is disabled—while traffic to and from the device that supports MACsec is MACsec-secured. In this scenario, traffic to the device that is not MACsec-secured must be VLAN-tagged.

The **must-secure** option is disabled, by default.

4. (Required only if the host device requires SCI tagging) Enable SCI tagging:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set include-sci
```

You should only use this option when connecting a switch to a host that requires SCI tags. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16. If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association ca1:

```
[edit security macsec connectivity-association ca-dynamic1]  
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]  
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower interval increases bandwidth overhead on the link; a higher interval optimizes MKA protocol communication.

The default interval is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association ca-dynamic1 is attached to an interface:

```
[edit security macsec connectivity-association ca-dynamic1]  
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using dynamic security mode, by default. When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are

run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set offset 30
```

The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an offset is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link. When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
```

```
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface. For instance, to assign connectivity association `ca-dynamic1` to interface `xe-0/0/1`:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca-dynamic1
```

## Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link

When you enable MACsec using static secure association key (SAK) security mode, one of up to two manually configured security keys is used to secure the point-to-point Ethernet link between the switches. All security key names and values are configured by the user; there is no key server or other tool that creates security keys. Security is maintained on the point-to-point Ethernet link by periodically rotating the security keys. Each security key name and value must have a corresponding matching value on the interface at the other end of the point-to-point Ethernet link to maintain MACsec on the link.

You configure static SAKs within secure channels when you are enabling MACsec using static SAK security mode. You configure secure channels within connectivity associations. A typical connectivity association for MACsec using static SAK security mode contains two secure channels—one for inbound traffic and one for outbound traffic—that have each been configured with two static SAKs. You must attach the connectivity association with the secure channel configurations to an interface to enable MACsec using static SAK security mode.

To configure MACsec on a switch-to-switch Ethernet link using static SAK security mode:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named `ca1`, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1
```

2. Configure the MACsec security mode as **static-sak** for the connectivity association:

```
[edit security macsec]
```

```
user@switch# set connectivity-association connectivity-association-name security-mode
static-sak
```

For instance, to configure the MACsec security mode to **static-sak** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 security-mode static-sak
```

3. Create a secure channel within the connectivity association. You can skip this step if you are configuring an existing secure channel.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name
```

For instance, to create secure channel **sc1** in connectivity association **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1
```

4. Define the security associations and the static SAKs for the secure channel:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name security-association number key key-string
```

where the **security-association number** is a number between 0 and 3, and the **key-string** is a 32-digit key defined statically by the network administrator.

The key string is a 32-digit hexadecimal number. The key string and the security association must match on both sides of an Ethernet connection to secure traffic using MACsec.

A secure channel must have at least two security associations with unique key strings. MACsec uses a security associations to establish a secure communications link, and periodically rotates to a new security association to keep the link secure. MACsec, therefore, must have at least one backup security association and key at all times.

To create one secure channel with two security associations and keys, for example:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 security-association 0 key
d183c4002fa6fe3d2d9a852c20ab8412
user@switch# set connectivity-association ca1 secure-channel sc1 security-association 1 key
b976c7494ab6fe2f2d4c432a90fd90a8
```

5. Specify whether the secure channel should be applied to traffic entering or leaving the switch:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name direction [inbound | outbound]
```

where **inbound** applies the secure channel to traffic entering the switch, and **outbound** applies the secure channel to traffic leaving the switch.



**NOTE:** A secure channel can only be applied to traffic entering (inbound) or leaving (outbound) an interface on the switch.

If you need to configure MACsec using SAKs on inbound and outbound traffic on the same interface, you must configure a connectivity association with one secure channel for inbound traffic and a second secure channel for outbound traffic. The connectivity association is assigned to an interface later in this process.

For instance, to configure secure channel **sc1** to apply MACsec to incoming traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 direction inbound
```

To configure secure channel **sc2** to apply MACsec to outgoing traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc2 direction outbound
```

6. Specify a MAC address:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id mac-address mac-address
```

If you are configuring a MAC address on a secure channel in the outbound direction, you should specify the MAC address of the interface as the **mac-address**.

If you are configuring a MAC address on a secure channel in the inbound direction, you should specify the MAC address of the interface at the other end of the link as the **mac-address**.

The **mac-address** variables must match on the sending and receiving secure channel on each side of a link to enable MACsec using static SAK security mode.



**NOTE:** You can see the MAC address of an interface in the **show interfaces** output.

To configure MACsec to accept frames from MAC address **12:34:56:ab:cd:ef** on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id mac-address
12:34:56:ab:cd:ef
```

7. Specify a port:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id port-id port-id-number
```

The **port-id-number** variables must match on a sending and receiving secure channel on each side of a link to enable MACsec.



**NOTE:** The only requirement for port numbers in this implementation of MACsec is that they match on the sending and receiving ends of an Ethernet link. When the port numbers match, MACsec is enabled for all traffic on the connection.

To specify port ID 4 on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id port-id 4
```

8. (Optional) Enable encryption:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name encryption
```

You can enable MACsec without enabling encryption. If a secure channel is configured on an interface without encryption, traffic is forwarded across the Ethernet link in clear text, and you will be able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic on the link does not represent a security threat.

Encryption is disabled by default when you are enabling MACsec using static SAK security mode. To ensure all traffic traversing secure-channel **sc1** is encrypted:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 encryption
```

9. (Optional) Set an offset to send the first 30 or 50 octets in unencrypted plain text when encryption is enabled.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name offset [0 | 30 | 50]
```

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

The default offset is 0, so all traffic on the link is encrypted when the **encryption** option is enabled and an **offset** is not set.

To change the offset to 30 for secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 offset 30
```

10. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association ca1 to interface xe-0/0/1:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca1
```

MACsec using static SAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and the configuration match on both ends of the link.

**Related  
Documentation**

- [Understanding Media Access Control Security \(MACsec\) on page 26](#)

---

## Enabling DHCP Snooping (CLI Procedure)

---

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. The switch builds and maintains a database of valid bindings between IP address and MAC addresses (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 133](#)
- [Applying CoS Forwarding Classes to Prioritize Snooped Packets on page 133](#)



## 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 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
```

To enable DHCPv6 snooping:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan vlan-name examine-dhcpv6
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all examine-dhcpv6
```



**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 might also need to configure the port security features of DHCP snooping on the ports through which those packets enter or leave.



**NOTE:** Prioritizing snooped packets by using CoS forwarding classes is not supported on the QFX Series switch.

To apply CoS forwarding classes and queues to snooped packets:

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

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

2. Enable DHCP snooping on a specific VLAN or on all VLANs and apply the required 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
```



**NOTE:** Replace `examine-dhcp` with `examine-dhcpv6` to enable DHCPv6 snooping.

---

#### Related Documentation

- [Enabling DHCP Snooping \(J-Web Procedure\) on page 135](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61](#)
- [Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 104](#)
- [Verifying That DHCP Snooping Is Working Correctly on page 255](#)
- [Monitoring Port Security on page 253](#)
- [Understanding DHCP Snooping for Port Security on page 12](#)
- [class-of-service](#)
- [secure-access-port on page 231](#)
- [secure-access-port](#)

## 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 132](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61](#)
- [Verifying That DHCP Snooping Is Working Correctly on page 255](#)
- [Monitoring Port Security on page 253](#)
- [Understanding DHCP Snooping for Port Security on page 12](#)

## Enabling a Trusted DHCP Server (CLI Procedure)

---

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

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

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

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

### Related Documentation

- [Enabling a Trusted DHCP Server \(J-Web Procedure\) on page 136](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 54](#)
- [Verifying That a Trusted DHCP Server Is Working Correctly on page 256](#)
- [Monitoring Port Security on page 253](#)
- [Understanding Trusted DHCP Servers for Port Security on page 32](#)
- [secure-access-port on page 231](#)
- [secure-access-port](#)

## 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 136](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 54](#)
- [Verifying That a Trusted DHCP Server Is Working Correctly on page 256](#)
- [Monitoring Port Security on page 253](#)
- [Understanding Trusted DHCP Servers for Port Security on page 32](#)

## Enabling Dynamic ARP Inspection (CLI Procedure)

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

This topic describes:

- [Enabling DAI on page 138](#)
- [Applying CoS Forwarding Classes to Prioritize Inspected Packets on page 138](#)

## Enabling DAI

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

To enable DAI on a VLAN or all VLANs:

- On a single VLAN:

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

- On all VLANs:

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

## Applying CoS Forwarding Classes to Prioritize Inspected Packets

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

To apply CoS forwarding classes and queues to DAI packets:

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

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

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

- On a specific VLAN:

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

- On all VLANs:

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

### Related Documentation

- [Enabling Dynamic ARP Inspection \(J-Web Procedure\) on page 139](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61](#)
- [Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 104](#)
- [Verifying That DAI Is Working Correctly on page 256](#)
- [Monitoring Port Security on page 253](#)

- [Understanding DAI for Port Security on page 20](#)
- [Understanding DAI for Port Security on page 20](#)
- *class-of-service*
- [secure-access-port on page 231](#)
- *secure-access-port*

## 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 137](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61](#)
- [Verifying That DAI Is Working Correctly on page 256](#)
- [Monitoring Port Security on page 253](#)
- [Understanding DAI for Port Security on page 20](#)

## Configuring MAC Limiting (CLI Procedure)

---

This task uses Junos OS for EX Series switches and QFX3500 and QFX3600 switches that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Configuring MAC Limiting (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

This topic describes various ways of configuring a limitation on MAC addresses in packets that are received and forwarded by the switch.

Before you can change a MAC limit that was previously set for an interface or a VLAN, you must first clear existing entries in the MAC address forwarding table that correspond to the change you want to make. Thus, to change the limit on an interface, first clear the MAC address forwarding table entries for that interface. To change the limit on all interfaces and VLANs, clear all MAC address forwarding table entries. To change the limit on a VLAN, clear the MAC address forwarding table entries for that VLAN.

To clear MAC addresses from the forwarding table:

- 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**):

```
user@switch> clear ethernet-switching-table vlan vlan-abc
```

The different ways of setting a MAC limit are described in the following sections:

- [Configuring MAC Limiting for Port Security by Limiting the Number of MAC Addresses That Can be Learned on Interfaces on page 140](#)
- [Configuring MAC Limiting for Port Security by Specifying MAC Addresses That Are Allowed on page 141](#)
- [Configuring MAC Limiting for VLANs on page 141](#)

## Configuring MAC Limiting for Port Security by Limiting the Number of MAC Addresses That Can be Learned on Interfaces

To configure MAC limiting for port security by setting a maximum number of MAC addresses that can be learned on interfaces.

- Apply the MAC limit 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 10
```

When no action is specified for configuring the MAC limit on an interface, the switch performs the default action **drop** if the limit is exceeded.

- Apply the MAC limit on a single access interface, on the basis of its membership within a specific VLAN (here, the interface is **ge-0/0/1** and the VLAN is **v1**).



```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 vlan v1 mac-limit 5
```

With this type of configuration, the switch drops any additional packets if the limit is exceeded, and also logs a message.

- Apply the limit to all access interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all mac-limit 10
```

When no action is specified for configuring the MAC limit on all interfaces, the switch performs the default action **drop** if the limit is exceeded:

## Configuring MAC Limiting for Port Security by Specifying MAC Addresses That Are Allowed

You must clear existing entries in the MAC address forwarding table prior to changing the MAC address limit.

To configure MAC limiting for port security by specifying 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
```

## Configuring MAC Limiting for VLANs

You must clear existing entries in the MAC address forwarding table before you can change the MAC address limit.

MAC limiting for a VLAN restricts the MAC addresses that can be learned for that VLAN, but does *not* drop the packet. Therefore, setting the MAC limit on a VLAN is not considered a port-security feature.



**NOTE:** The configuration of specific allowed MAC addresses does not apply to VLANs.

To configure MAC limiting for a VLAN using the CLI:

- Limit the number of dynamic MAC addresses on a VLAN:

If the MAC limit on a specific VLAN is exceeded, the switch logs the MAC addresses of packets that cause the limit to be exceeded. No other action is possible.

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



**NOTE:** When you are applying a MAC limit on a VLAN, do not set `mac-limit` to 1 for a VLAN composed of Routed VLAN Interfaces (RVIs) or a VLAN composed of aggregated Ethernet bundles using LACP. In these cases, setting the `mac-limit` to 1 prevents the switch from learning MAC addresses other than the automatic addresses:

- For RVIs, 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.

If the VLAN is composed of regular access or trunk interfaces, you can set the `mac-limit` to 1 if you choose to do so.

#### Related Documentation

- [Configuring MAC Limiting \(J-Web Procedure\) on page 143](#)
- [Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 51](#)
- [Verifying That MAC Limiting Is Working Correctly on page 257](#)
- [Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces \(CLI Procedure\) on page 148](#)
- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 159](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 24](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security](#)
- [Understanding Bridging and VLANs on EX Series Switches](#)
- [no-allowed-mac-log on page 216](#)
- [show vlans](#)

## 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.
    - Drop—Drop the packets and generate a system log entry. (Default)
    - Shutdown—Shut down the VLAN and generate a system log entry. 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 159](#). 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 140](#)
- [Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 66](#)
- [Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 51](#)
- [Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 58](#)
- [Verifying That MAC Limiting Is Working Correctly on page 257](#)
- [Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces \(CLI Procedure\) on page 148](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 24](#)

---

## Configuring MAC Move Limiting (CLI Procedure)

---

When MAC move limiting is configured, MAC address movements are tracked by the switch and, if a MAC address changes more than the configured number of times within 1 second, the changes to MAC addresses are dropped, logged, ignored, or the interface is shut down.



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

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

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

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

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

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

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

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

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

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

The action is not specified, so the switch performs the default action **drop** if it tracks that an individual MAC address within any of the VLANs has moved more than 5 times within 1 second.

#### Related Documentation

- [Configuring MAC Move Limiting \(J-Web Procedure\) on page 147](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Verifying That MAC Move Limiting Is Working Correctly on page 262](#)
- [Monitoring Port Security on page 253](#)
- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 159](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 24](#)
- [\*Understanding MAC Limiting and MAC Move Limiting for Port Security\*](#)
- [\*clear ethernet-switching port-error\*](#)
- [\*clear ethernet-switching port-error\*](#)
- [\*port-error-disable\*](#)
- [\*port-error-disable\*](#)
- [secure-access-port on page 231](#)
- [\*secure-access-port\*](#)

## 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.
- Drop—Drop the packets and generate a system log entry. (Default)
- Shutdown—Shut down the VLAN and generate a system log entry. 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 159](#). 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 145](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Verifying That MAC Move Limiting Is Working Correctly on page 262](#)
- [Monitoring Port Security on page 253](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 24](#)

---

## 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 (Access Port Security) 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 140](#)
- [Configuring MAC Limiting \(J-Web Procedure\) on page 143](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Verifying That MAC Limiting Is Working Correctly on page 257](#)

---

## 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.

While 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.

- [Configuring IP Source Guard on page 149](#)
- [Configuring IPv6 Source Guard on page 150](#)
- [Disabling IP Source Guard on page 151](#)

## Configuring IP Source Guard

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 132](#). 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.

To configure IP source guard:

- On a specific VLAN:  

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

```
[edit vlans]
user@switch# set vlan-name vlan-range vlan-id-low-vlan-id-high
```

2. Associate an interface with the VLAN-range and set the port mode to **access**:

```
[edit interfaces]
user@switch# set interface-name unit 0 family ethernet-switching port-mode access vlan
members vlan-name
```

3. Enable IP source guard on the VLAN:

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

To commit these changes to the active configuration, type the **commit** command at the user prompt.

## Configuring IPv6 Source Guard

Before you configure IPv6 source guard, be sure that you have:

- Explicitly enabled DHCPv6 snooping on the specific VLAN or specific VLANs on which you will configure IPv6 source guard. See [“Enabling DHCP Snooping \(CLI Procedure\)” on page 132](#). If you configure IPv6 source guard on specific VLANs rather than on all VLANs, you must also enable DHCPv6 snooping explicitly on those VLANs. Otherwise, the default value of no DHCPv6 snooping applies to that VLAN.
- Set the maximum number of IPv6 source guard sessions:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set ipv6-source-guard-sessions max-number maximum-number
```



**NOTE:** After setting or changing the maximum number of IPv6 source guard sessions and committing the configuration, you must reboot the switch for the configuration to take effect.

To configure IPv6 source guard:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name ipv6-source-guard
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all ipv6-source-guard
```

- On a VLAN range:

1. Set the VLAN range):

```
[edit vlans]
user@switch# set vlan-name vlan-range vlan-id-low-vlan-id-high
```

2. Associate an interface with a VLAN-range and set the port mode to **access**:

```
[edit interfaces]
user@switch# set interface-name unit 0 family ethernet-switching port-mode access vlan
members vlan-name
```

3. Enable IPv6 source guard on the VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name ipv6-source-guard
```

To commit these changes to the active configuration, type the **commit** command at the user prompt.

## Disabling IP Source Guard

You can disable IP source guard for a specific VLAN after you have enabled the feature for all VLANs, or for all VLANs.

- To disable IP source guard on a specific VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name no-ip-source-guard
```

- To disable IP source guard on all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all no-ipv6-source-guard
```



**NOTE:** Replace `no-ip-source-guard` with `no-ipv6-source-guard` to disable IPv6 source guard.

### Related Documentation

- [Verifying That IP Source Guard Is Working Correctly on page 263](#)
- [Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 87](#)
- [Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 77](#)
- [Understanding IP Source Guard for Port Security on EX Series Switches on page 32](#)

## 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 *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-MAC address binding in the DHCP snooping database:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name static-ip ip-address vlan data-vlan mac mac-address
```

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

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name static-ipv6 ip-address vlan data-vlan mac mac-address
```

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 255](#)
- [Understanding DHCP Snooping for Port Security on page 12](#)
- [secure-access-port on page 231](#)
- *secure-access-port*

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

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

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

- The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as routed VLAN interfaces, or RVIs. The switch relays the clients' requests to the server and then forwards the server's replies to the clients. This topic describes this configuration. The configuration for this topology is the same regardless of whether your switch is running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style or not.
- The switch, DHCP clients, and DHCP server are all on the same VLAN. The switch forwards the clients' requests to the server and forwards the server's replies to the clients. This configuration for this topology differs if your switch is running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style.
  - If your switch is running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, see *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*.
  - If your switch is running Junos OS for EX Series switches without support for ELS, see *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)* on page 156.

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

- Connect and configure the DHCP server.



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

- Configure the VLAN on the switch and associate the interfaces on which the clients connect to the switch with that VLAN.

- Configure the routed VLAN interface (RVI) to allow the switch to relay packets to the server and receive packets from the server. See *Configuring Routed VLAN Interfaces (CLI Procedure)* or *Configuring IRB Interfaces* for the QFX Series.
- Configure the switch as a BOOTP relay agent. See *DHCP/BOOTP Relay for Switches Overview*.

To configure DHCP option 82:



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

1. Specify DHCP option 82 for the BOOTP server:

- On all interfaces that connect to the server:

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

- On a specific interface that connects to the server:

```
[edit forwarding-options helpers bootp]
user@switch# set interface ge-0/0/10 dhcp-option82
```

The remaining steps are optional. They show configurations for all interfaces; include the specific interface designation to configure any of the following options on a specific interface:

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

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

3. To specify that the circuit ID suboption value should contain the interface description rather than the interface name (the default):

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

4. To specify that the circuit ID suboption value should contain the VLAN ID rather than the VLAN name (the default):

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

5. To specify that the remote ID suboption be included in the DHCP option 82 information:

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

6. To configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

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

7. To specify that the prefix for the remote ID suboption be the hostname of the switch rather than the MAC address of the switch (the default):

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

8. To specify that the remote ID suboption value should contain the interface description:

```
[edit forwarding-options helpers bootp]
```

```
user@switch# set dhcp-option82 remote-id use-interface-description
```

9. To specify that the remote ID suboption value should contain a character string:

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

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

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

11. To specify that the vendor ID suboption value contains a character string value that you specify rather than **Juniper** (the default):

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

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

#### Related Documentation

- [Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98](#)
- [\[edit forwarding-options\] Configuration Statement Hierarchy on EX Series Switches on page 168](#)
- [Understanding DHCP Option 82 for Port Security on Switching Devices on page 35](#)
- [Understanding DHCP Option 82 for Port Security](#)
- [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 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 153.

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

- Connect and configure the DHCP server.



.....

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

.....

- Configure a VLAN on the switch and associate the interfaces on which the clients and the server connect to the switch with that VLAN.



To configure DHCP option 82:



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

1. Specify DHCP option 82 for all VLANs associated with the switch or for a specified VLAN. (You can also configure the feature for a VLAN range.)

- On a specific VLAN:

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

- On all VLANs:

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

The remaining steps are optional.

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

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

3. To specify that the circuit ID suboption value should contain the interface description rather than the interface name (the default):

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

4. To specify that the circuit ID suboption value should contain the VLAN ID rather than the VLAN name (the default):

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

5. To specify that the remote ID suboption be included in the DHCP option 82 information:

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

6. To configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

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

7. To specify that the prefix for the remote ID suboption be the hostname of the switch rather than the MAC address of the switch (the default):

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

8. To specify that the remote ID suboption value should contain the interface description:

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

9. To specify that the remote ID suboption value should contain a character string:

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

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

```
[edit ethernet-switching-options secure-access-port]
```

```
user@switch# set vlan employee dhcp-option82 vendor-id
```

11. To specify that the vendor ID suboption value should contain a character string value that you specify rather than **Juniper** (the default):

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

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

#### Related Documentation

- [Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101](#)
- [secure-access-port on page 231](#)
- [secure-access-port](#)
- [Understanding DHCP Option 82 for Port Security on Switching Devices on page 35](#)
- [Understanding DHCP Option 82 for Port Security](#)
- [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 page 43](#)
- [Configuring MAC Limiting \(CLI Procedure\) on page 140](#)
- [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 24](#)
- [Understanding Storm Control on EX Series Switches](#)

## Configuring Persistent MAC Learning (CLI Procedure)

You can configure persistent MAC learning, also known as sticky MAC, to allow dynamically learned MAC addresses to be retained on an interface across restarts of the switch.

Persistent MAC address learning is disabled by default. You can enable it to:

- Help prevent traffic losses for trusted workstations and servers because the interface does not have to relearn the addresses from ingress traffic after a restart.
- Protect the switch against security attacks—use persistent MAC learning in combination with MAC limiting to protect against attacks while still avoiding the need to statically configure MAC addresses. When the initial learning of MAC addresses up to the number

specified by the MAC limit is done, new addresses will not be allowed even after a reboot. The port is secured because after the limit has been reached, additional devices cannot connect to the interface.

The first devices that send traffic after you connect are learned during the initial connection period. You can monitor the MAC addresses and provide the same level of security as if you statically configured each MAC address on each interface, except with less manual effort. Persistent MAC learning also helps prevent traffic loss for trusted workstations and servers because the interface does not have to relearn the addresses from ingress traffic.

To configure persistent MAC learning on an interface and limit the number of allowed MAC addresses:

1. Enable persistent MAC learning on an interface:

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

2. Limit the number of dynamic MAC addresses. You can do one of:

- Allow the switch to take the default action (which is **drop**) regarding packets received on the interface after the limit is reached.
- Configure an action for the switch to take regarding packets received on the interface after the limit is reached. You can configure any one of the following actions--you can also explicitly configure **drop**:
  - **log**—Allow the packets but log a message.
  - **none**—Take no action.
  - **shutdown**—Shut down the interface.

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



**TIP:** If you move a device within your network that has a persistent MAC address entry on the switch, use the *clear ethernet-switching table persistent-mac* command to clear the persistent MAC-address entry. If you move the device to another port on the switch and do not clear the persistent MAC address from the original port it was learned on, then the new port will not learn the MAC address and the device will not be able to connect. If the original port is down when you move the device, then the new port will learn the MAC address and the device can connect—however, unless you cleared the MAC address on the original port, when that port comes back up, the system reinstalls the persistent MAC address in the forwarding table for that port. If this occurs, the address is removed from the new port and the device loses connectivity.

**Related  
Documentation**

- [Example: Configuring Basic Port Security Features on page 43](#)
- [Understanding Persistent MAC Learning \(Sticky MAC\) on page 39](#)

- [Understanding How to Protect Access Ports on EX Series Switches from Common Attacks on page 9](#)

## Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure)

By default, IP-MAC bindings in the DHCP snooping database do not persist through switch reboots. You can configure the IP-MAC bindings in the DHCP snooping database to persist through switch reboots by configuring a storage location for the DHCP snooping database file. When specifying the location for the DHCP snooping database, you must also specify how frequently the switch writes the database entries into the DHCP snooping database file.

The DHCP snooping database of IP-MAC bindings is created when you enable DHCP snooping. DHCP snooping is not enabled by default. You can configure DHCP snooping on a specific VLAN or on all VLANs. See [“Enabling DHCP Snooping \(CLI Procedure\)” on page 132](#).

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

- For DHCPv4 snooping:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcp-snooping-file location local-pathname write-interval seconds
```

For example:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcp-snooping-file location /var/tmp/test.log write-interval 60
```

- For DHCPv6 snooping:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcpv6-snooping-file location local-pathname write-interval seconds
```

For example:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcpv6-snooping-file location /var/tmp/test.log write-interval 60
```

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

- For DHCPv4 snooping:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcp-snooping-file location remote_url write-interval seconds
```

For example:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcp-snooping-file location ftp://test:Test123@14.1.2.1 write-interval 60
```

- For DHCPv6 snooping:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcpv6-snooping-file location remote_url write-interval
seconds
```

For example:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcpv6-snooping-file location ftp://test:Test123@14.1.2.1
write-interval 60
```



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

When you are storing the DHCP snooping database at a remote location, you might also want to specify a timeout value for remote read and write operations. See [timeout](#). This is optional.

---

**Related  
Documentation**

- [Understanding DHCP Snooping for Port Security on page 12](#)

## CHAPTER 5

# Configuration Statements

- [\[edit ethernet-switching-options\] Configuration Statement Hierarchy on EX Series Switches on page 165](#)
- [\[edit forwarding-options\] Configuration Statement Hierarchy on EX Series Switches on page 168](#)
- [\[edit security\] Configuration Statement Hierarchy on EX Series Switches on page 172](#)
- [allowed-mac on page 176](#)
- [arp-inspection on page 177](#)
- [cak on page 178](#)
- [circuit-id on page 179](#)
- [ckn on page 180](#)
- [connectivity-association on page 181](#)
- [connectivity-association \(MACsec Interfaces\) on page 182](#)
- [direction on page 183](#)
- [dhcp-option82 on page 184](#)
- [dhcp-snooping-file on page 185](#)
- [dhcp-trusted on page 186](#)
- [disable-timeout on page 187](#)
- [encryption on page 188](#)
- [ethernet-switching-options on page 189](#)
- [examine-dhcp on page 193](#)
- [examine-dhcpv6 on page 195](#)
- [exclude-protocol on page 196](#)
- [forwarding-class \(for DHCP Snooping or DAI Packets\) on page 197](#)
- [id on page 198](#)
- [include-sci on page 199](#)
- [interface \(Access Port Security\) on page 200](#)
- [interfaces \(MACsec\) on page 201](#)
- [ip-source-guard on page 202](#)

- [ipv6-source-guard-sessions](#) on page 203
- [key](#) on page 204
- [key-server-priority](#) on page 205
- [location \(DHCP Snooping Database\)](#) on page 206
- [mac](#) on page 207
- [mac-address \(MACsec\)](#) on page 208
- [mac-limit \(Access Port Security\)](#) on page 209
- [mac-move-limit](#) on page 211
- [macsec](#) on page 213
- [mka](#) on page 214
- [must-secure](#) on page 215
- [no-allowed-mac-log](#) on page 216
- [no-encryption](#) on page 217
- [no-examine-dhcpv6](#) on page 218
- [no-gratuitous-arp-request](#) on page 219
- [no-option-37](#) on page 219
- [offset](#) on page 220
- [persistent-learning](#) on page 221
- [port-error-disable](#) on page 222
- [port-id](#) on page 223
- [pre-shared-key](#) on page 224
- [prefix \(Circuit ID for Option 82\)](#) on page 225
- [prefix \(Remote ID for Option 82\)](#) on page 227
- [remote-id](#) on page 228
- [replay-protect](#) on page 229
- [replay-window-size](#) on page 230
- [secure-access-port](#) on page 231
- [secure-channel](#) on page 233
- [security-association](#) on page 234
- [security-mode](#) on page 235
- [static-ip](#) on page 236
- [timeout](#) on page 237
- [traceoptions \(Access Port Security\)](#) on page 238
- [transmit-interval \(MACsec\)](#) on page 240
- [use-interface-description](#) on page 241
- [use-string](#) on page 243
- [use-vlan-id](#) on page 244



- [vendor-id](#) on page 245
- [vlan \(Access Port Security\)](#) on page 247
- [vlan \(DHCP Bindings on Access Ports\)](#) on page 249
- [write-interval](#) on page 250

## [edit ethernet-switching-options] Configuration Statement Hierarchy on EX Series Switches

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

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

This topic lists:

- [Supported Statements in the \[edit ethernet-switching-options\] Hierarchy Level](#) on page 165
- [Unsupported Statements in the \[edit ethernet-switching-options\] Hierarchy Level](#) on page 168

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

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

```
ethernet-switching-options {
  analyzer {
    name {
      input {
        egress {
          interface (all | interface-name);
        }
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      }
    }
    loss-priority priority;
    output {
      interface interface-name;
      vlan (vlan-id | vlan-name);
    }
    ratio number;
  }
  authentication-whitelist {
```

```
    interface;
    vlan-assignment;
}
bpdu-block {
    disable-timeout timeout;
    interface (all | [interface-name]) {
        (disable | drop | shutdown);
    }
}
dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100);
}
interfaces interface-name {
    no-mac-learning;
}
mac-lookup-length number-of-entries;
}
mac-notification {
    notification-interval seconds;
}
mac-table-aging-time seconds;
port-error-disable {
    disable-timeout timeout;
}
redundant-trunk-group {
    group name {
        description;
        interface interface-name {
            primary;
        }
        preempt-cutover-timer seconds;
    }
}
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 {
            mac mac-address;
            vlan vlan-name;
        }
    }
}
uac-policy;
}
vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection );
```

```

dhcp-option82 {
  disable;
  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;
}
}
static {
  vlan vlan-id {
    mac mac-address next-hop interface-name;
  }
}
storm-control {
  action-shutdown;
  interface (all | interface-name) {
    bandwidth bandwidth;
    multicast;
    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]) {
    forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
      network-control);
    vlan vlan-name;
  }
}
}

```

```
}
```

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

All statements in the [edit ethernet-switching-options] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

### Related Documentation

- *Example: Setting Up Q-in-Q Tunneling on EX Series Switches*
- *Example: Configuring Redundant Trunk Links for Faster Recovery*
- *Configuring MAC Table Aging (CLI Procedure)*
- *Configuring MAC Notification (CLI Procedure)*
- *Configuring Q-in-Q Tunneling (CLI Procedure)*
- *Configuring Redundant Trunk Links for Faster Recovery (CLI Procedure)*
- *Configuring Nonstop Bridging on EX Series Switches (CLI Procedure)*

## [edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches

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

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

This topic lists:

- [Supported Statements in the \[edit forwarding-options\] Hierarchy Level on page 168](#)
- [Unsupported Statements in the \[edit forwarding-options\] Hierarchy Level on page 170](#)

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

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

```
forwarding-options {  
  dhcp-relay {  
    group group-name {  
      interface interface-name {  
        overrides {  
          always-write-giaddr;  
          always-write-option-82;  
          client-discover-match <option60-and-option82>;  
          interface-client-limit number;
```

```

        layer2-unicast-replies;
        no-arp;
        trust-option-82;
    }
}
exclude {
    overrides {
        ...
    }
    trace;
    upto upto-interface-name;
}
overrides {
    ...
}
relay-option {
    ...
}
}
relay-option-82 {
    circuit-id {
        prefix prefix;
        use-interface-description (logical | device);
    }
}
server-group {
    server-group-name {
        server-ip-address;
    }
}
}
helpers{
    bootp {
        client-response-ttl number;
        description text-description;
        dhcp-option82 {
            circuit-id {
                prefix (Circuit ID for Option 82) hostname;
                use-interface-description;
                use-vlan-id;
            }
            disable;
            remote-id {
                prefix hostname | mac | none;
                use-interface-description;
                use-string string;
            }
            vendor-id <string>;
        }
    }
    interface (interface-name | interface-group) {
        broadcast;
        client-response-ttl number;
        description text-description;
        dhcp-option82 {
            circuit-id {
                prefix (Circuit ID for Option 82) hostname;

```

```

        use-interface-description;
        use-vlan-id;
    }
    disable;
    remote-id {
        prefix hostname | mac | none;
        use-interface-description;
        use-string string;
    }
    vendor-id <string>;
}
maximum-hop-count number;
minimum-wait-time seconds;
no-listen;
server address {
    routing-instance [ routing-instance-names ];
}
}
maximum-hop-count number;
minimum-wait-time seconds;
no-listen;
relay-agent-option;
server address {
    routing-instance [ routing-instance-names ];
}
source-address-giaddr;
}
}

```

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

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

**Table 15: Unsupported [edit forwarding-options] Configuration Statements on EX Series Switches**

Statement	Hierarchy Level
<i>NOTE:</i> Variables, such as <i>filename</i> , are not shown in the statements or hierarchies.	
accounting	[edit forwarding-options]
aggregate-export-interval	[edit forwarding-options accounting output]
broadcast	[edit forwarding-options helpers domain interface] [edit forwarding-options helpers port interface] [edit forwarding-options helpers tftp interface]
description	[edit forwarding-options helpers domain] [edit forwarding-options helpers domain interface] [edit forwarding-options helpers port interface] [edit forwarding-options helpers tftp] [edit forwarding-options helpers tftp interface]

Table 15: Unsupported [edit forwarding-options] Configuration Statements on EX Series Switches (*continued*)

Statement	Hierarchy Level
domain	[edit forwarding-options helpers]
engine-id	[edit forwarding-options accounting output interface]
file	[edit forwarding-options helpers traceoption]
flag	[edit forwarding-options helpers traceoption]
flow-active-timeout	[edit forwarding-options accounting output]
flow-inactive-timeout	[edit forwarding-options accounting output]
hash-seed	[edit forwarding-options load-balance per-prefix]
indexed-next-hop	[edit forwarding-options load-balance]
interface	[edit forwarding-options accounting output] [edit forwarding-options helpers domain] [edit forwarding-options helpers port] [edit forwarding-options helpers tftp]
level	[edit forwarding-options helpers traceoption]
load-balance	[edit forwarding-options]
no-listen	[edit forwarding-options helpers domain interface] [edit forwarding-options helpers port interface] [edit forwarding-options helpers tftp interface]
no-remote-trace	[edit forwarding-options helpers traceoption]
output	[edit forwarding-options accounting]
per-prefix	[edit forwarding-options load-balance]
port	[edit forwarding-options helpers]
routing-instance	[edit forwarding-options helpers domain interface server] [edit forwarding-options helpers domain server] [edit forwarding-options helpers port interface server] [edit forwarding-options helpers rtsdb-client-traceoptions] [edit forwarding-options helpers tftp interface server] [edit forwarding-options helpers tftp server]
rtsdb-client-traceoptions	[edit forwarding-options helpers]

Table 15: Unsupported [edit forwarding-options] Configuration Statements on EX Series Switches (*continued*)

Statement	Hierarchy Level
server	<a href="#">[edit forwarding-options helpers domain]</a> <a href="#">[edit forwarding-options helpers domain interface]</a> <a href="#">[edit forwarding-options helpers port]</a> <a href="#">[edit forwarding-options helpers port interface]</a> <a href="#">[edit forwarding-options helpers tftp]</a> <a href="#">[edit forwarding-options helpers tftp interface]</a>
source-address	<a href="#">[edit forwarding-options accounting output interface]</a>
tftp	<a href="#">[edit forwarding-options helpers]</a>
traceoptions	<a href="#">[edit forwarding-options helpers]</a>

#### Related Documentation

- [Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98](#)
- [Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 153](#)
- [DHCP/BOOTP Relay for Switches Overview](#)
- [For more information about the \[edit forwarding-options\] hierarchy and its options, see \*Junos OS Policy Framework Configuration Guide\*](#)

## [edit security] Configuration Statement Hierarchy on EX Series Switches

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

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

This topic lists:

- [Supported Statements in the \[edit security\] Hierarchy Level on page 172](#)
- [Unsupported Statements in the \[edit security\] Hierarchy Level on page 175](#)

### Supported Statements in the [edit security] Hierarchy Level

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



```

security {
  alarms {
    potential-violation {
      authentication failures;
      cryptographic-self-test;
      key-generation-self-test;
      non-cryptographic-self-test;
      policy number per (minute | second);
      replay-attacks {
        threshold value;
      }
      security-log-percent-full;
    }
  }
  certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority ca-profile-name {
      ca-name certificate-authority-name;
      crl filename;
      encoding (binary | pem);
      enrollment-url url;
      file certificate-filename;
      ldap-url url-name;
    }
    enrollment-retry number;
    local certificate-name {
      certificate-key-string;
      load-key-file URL-or-path;
    }
    maximum-certificates number;
    path-length bytes;
  }
  ipsec {
    security-association sa-name {
      description text-description;
      manual {
        direction (bidirectional | inbound | outbound) {
        }
      }
      mode (transport | tunnel);
    }
  }
  log {
    cache {
      exclude name {
        destination-address;
        destination-port;
        event-id;
        failure;
        interface-name;
        policy-name;
        process;
        source-address;
        source-port;
        success;
        username;
      }
    }
  }
}

```

```

    }
    limit number;
  }
}
macsec {
  connectivity-association connectivity-association-name {
    exclude-protocol protocol-name;
    include-sci;
    mka {
      must-secure;
      key-server-priority priority-number;
      transmit-interval interval;
    }
    no-encryption;
    offset (0|30|50);
    pre-shared-key {
      cak hexadecimal-number;
      ckn hexadecimal-number;
    }
    replay-protect {
      replay-window-size number-of-packets;
    }
    secure-channel secure-channel-name {
      direction (inbound | outbound);
      encryption;
      id {
        mac-address mac-address;
        port-id port-id-number;
      }
      offset (0|30|50);
      security-association security-association-number {
        key key-string;
      }
    }
    security-mode security-mode;
  }
  interfaces interface-name {
    connectivity-association connectivity-association-name;
  }
}
pki {
  auto-re-enrollment {
    certificate-id certificate-id {
      ca-profile-name profile-name;
      challenge-password password;
      re-enroll-trigger-time-percentage percentage;
      re-generate-keypair;
    }
  }
  traceoptions {
    file <filename> <files number> <match regular-expression> <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
  }
}
ssh-known-hosts {

```

```

fetch-from-server (hostname | address);
host (hostname | address) {
    dsa-key key;
    ecdsa-sha2-nistp256-key key;
    ecdsa-sha2-nistp384-key key;
    ecdsa-sha2-nistp521-key key;
    rsa-key key;
    rsa1-key key;
}
load-key-file filename;
}
traceoptions {
    file <filename> <files number> <match regular-expression> <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    level level;
    no-remote-trace;
    rate-limit rate;
}
}

```

### Unsupported Statements in the [edit security] Hierarchy Level

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

**Table 16: Unsupported [edit security] Configuration Statements on EX Series Switches**

Statement	Hierarchy
<b>NOTE:</b> Variables, such as <i>filename</i> , are not shown in the statements or hierarchies.	
audible	[edit security alarms]
continuous	[edit security alarms audible]

## allowed-mac

---



<b>Syntax</b>	<code>allowed-mac {     mac-address-list; }</code>
<b>Hierarchy Level</b>	[edit <a href="#">ethernet-switching-options secure-access-port interface</a> (all   <i>interface-name</i> ) ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	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.

<b>Default</b>	Allowed MAC addresses take precedence over dynamic MAC values that have been applied with the <b>mac-limit</b> statement.
<b>Options</b>	<b>mac-address-list</b> —One or more MAC addresses configured as allowed MAC addresses for a specified interface or all interfaces.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system—control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">mac-limit (Access Port Security) on page 209</a></li><li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li><li>• <a href="#">Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 66</a></li><li>• <a href="#">Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 51</a></li><li>• <a href="#">Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 58</a></li><li>• <a href="#">Configuring MAC Limiting (CLI Procedure) on page 140</a></li><li>• <a href="#">Configuring MAC Limiting (J-Web Procedure) on page 143</a></li></ul>

## arp-inspection

<b>Syntax</b>	<pre>arp-inspection {     forwarding-class class-name; }</pre>
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with ELS:           <ul style="list-style-type: none"> <li>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security],</li> <li>[edit forwarding-options dhcp-relay ]</li> </ul> </li> <li>For platforms without ELS:           <ul style="list-style-type: none"> <li>[edit ethernet-switching-options secure-access-port vlan (all   <i>vlan-name</i>)],</li> <li>[edit forwarding-options dhcp-relay ]</li> </ul> </li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p>
<b>Description</b>	<p>Perform dynamic ARP inspection (DAI) on all VLANs or on the specified VLAN.</p> <p>When DAI is enabled, the switch logs invalid ARP packets that it receives on each interface, along with the sender's IP and MAC addresses. ARP probe packets, which have the sender IP address 0.0.0.0, are validated by DAI.</p>
<div>  <p><b>NOTE:</b> If you configure DAI at the [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] hierarchy level:</p> <ul style="list-style-type: none"> <li>DAI can be configured only for a specific VLAN, not for a list or a range of VLAN IDs.</li> <li>DHCP snooping is automatically enabled on the specified VLAN.</li> <li>The forwarding-class statement is not available at the [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] hierarchy level.</li> </ul> <p>See <i>Enabling Dynamic ARP Inspection (CLI Procedure)</i> for more information about this configuration.</p> </div>	
<div>  <p><b>NOTE:</b> On EX9200 switches, DAI is not supported in an MC-LAG scenario.</p> </div> <p>The remaining statement is explained separately.</p>	
<b>Default</b>	Disabled.

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69</a></li><li>• <a href="#">Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61</a></li><li>• <a href="#">Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing</a></li><li>• <a href="#">Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 104</a></li><li>• <a href="#">Enabling Dynamic ARP Inspection (CLI Procedure) on page 137</a></li><li>• <a href="#">Enabling Dynamic ARP Inspection (J-Web Procedure) on page 139</a></li></ul>

---

## cak

---

<b>Syntax</b>	<code>ckn <i>hexadecimal-number</i>;</code>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec connectivity-association</a> <a href="#">connectivity-association-name</a> <a href="#">pre-shared-key</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies the connectivity association key (CAK) for a pre-shared key.</p> <p>A pre-shared key includes a connectivity association key name (CKN) and a CAK. A pre-shared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using dynamic security keys. The MACsec Key Agreement (MKA) protocol is enabled once the pre-shared keys are successfully exchanged. The pre-shared key—the CKN and CAK—must match on both ends of a link</p>
<b>Default</b>	No CAK exists, by default.
<b>Options</b>	<p><b><i>hexadecimal-number</i></b>—The key name, in hexadecimal format.</p> <p>The key name is 32 hexadecimal characters in length. If you enter a key name that is less than 32 characters long, the remaining characters are set to 0.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>

## circuit-id

<b>Syntax</b>	<pre> circuit-id {   prefix {     host-name;     logical-system-name;     routing-instance-name;   }   use-interface-description (device   logical);   use-vlan-id; } </pre>
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with Enhanced Layer 2 Software (ELS): [edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 ]</li> <li>For platforms without ELS: [edit <a href="#">ethernet-switching-options secure-access-port vlan</a> (all   <i>vlan-name</i>) <a href="#">dhcp-option82</a>], [edit forwarding-options helpers bootp <a href="#">dhcp-option82</a>] , [edit forwarding-options helpers bootp interface <i>interface-name</i> <a href="#">dhcp-option82</a>]</li> <li>For MX Series platforms: [edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82]</li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 14.1 for the MX Series.</p>
<b>Description</b>	<p>Configure the <b>circuit-id</b> suboption (suboption 1) of DHCP option 82 (the DHCP relay agent information option) in DHCP packets destined for a DHCP server. This suboption identifies the circuit (the interface, the VLAN, or both) on which the DHCP request arrived.</p> <p>The remaining statements are explained separately.</p>
<b>Default</b>	<p>If DHCP option 82 is enabled on the switch, the circuit ID is supplied by default in the format <i>interface-name:vlan-name</i> or, on a Layer 3 interface, just <i>interface-name</i>.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)</a></li> <li><a href="#">Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101</a></li> <li><a href="#">Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98</a></li> </ul>

- [Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 156](#)
- [Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 153](#)
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>

---

## ckn

---

<b>Syntax</b>	<code>ckn hexadecimal-number;</code>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec connectivity-association</a> <a href="#">connectivity-association-name</a> <a href="#">pre-shared-key</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies the connectivity association key name (CKN) for a pre-shared key.</p> <p>A pre-shared key includes a CKN and a connectivity association key (CAK). A pre-shared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using dynamic security keys. The MACsec Key Agreement (MKA) protocol is enabled once the pre-shared keys are successfully exchanged. The pre-shared key—the CKN and CAK—must match on both ends of a link</p>
<b>Default</b>	No CKN exists, by default.
<b>Options</b>	<p><b><i>hexadecimal-number</i></b>—The key name, in hexadecimal format.</p> <p>The key name is 32 hexadecimal characters in length. If you enter a key name that is less than 32 characters long, the remaining characters are set to 0.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>



## connectivity-association

<b>Syntax</b>	<pre> connectivity-association <i>connectivity-association-name</i> {   <i>exclude-protocol</i> <i>protocol-name</i>;   include-sci;   mka {     must-secure;     key-server-priority <i>priority-number</i>;     transmit-interval <i>interval</i>;   }   no-encryption;   offset (0 30 50);   pre-shared-key {     cak <i>hexadecimal-number</i>;     ckn <i>hexadecimal-number</i>;   }   replay-protect {     replay-window-size <i>number-of-packets</i>;   }   secure-channel <i>secure-channel-name</i> {     direction (inbound   outbound);     encryption;     id {       mac-address <i>mac-address</i>;       port-id <i>port-id-number</i>;     }     offset (0 30 50);     security-association <i>security-association-number</i> {       key <i>key-string</i>;     }   }   security-mode <i>security-mode</i>; } </pre>
<b>Hierarchy Level</b>	[edit security <i>macsec</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for the QFX Series.
<b>Description</b>	<p>Create or configure a MACsec connectivity association.</p> <p>A connectivity association is not applying MACsec to traffic until it is associated with an interface. MACsec connectivity associations are associated with interfaces using the <i>interfaces</i> statement in the [edit security macsec] hierarchy.</p>
<b>Default</b>	No connectivity associations are present, by default.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

**Related Documentation** • [Configuring Media Access Control Security \(MACsec\) on page 116](#)

---

## connectivity-association (MACsec Interfaces)

---

<b>Syntax</b>	connectivity-association <i>connectivity-association-name</i> ;
<b>Hierarchy Level</b>	[edit security <a href="#">macsec interfaces</a> <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	Applies a connectivity association to an interface, which enables Media Access Control Security (MACsec) on that interface.
<b>Default</b>	No connectivity associations are associated with any interfaces.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a>

## direction

<b>Syntax</b>	direction (inbound   outbound);
<b>Hierarchy Level</b>	[edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> <b>secure-channel</b> <i>secure-channel-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Configure whether the secure channel applies MACsec security to traffic entering or leaving an interface.</p> <p>If you need to apply MACsec on traffic entering and leaving an interface, you need to create one secure channel to apply MACsec on incoming traffic and another secure channel to apply MACsec on outgoing traffic within the same connectivity association. When you associate the connectivity association with an interface, MACsec is applied on traffic entering and leaving that interface.</p> <p>You only use this configuration option when you are configuring MACsec using static secure association keys (SAK) security mode. When you are configuring MACsec using static connectivity association keys (CAK) security mode, two secure channels that are not user-configurable—one inbound secure channel and one outbound secure channel—are automatically created within the connectivity association.</p>
<b>Default</b>	<p>This statement does not have a default value.</p> <p>If you have configured a secure channel to enable MACsec using static SAK security mode, you must specify whether the secure channel applies MACsec to traffic entering or leaving an interface. A candidate configuration that contains a secure channel that has not configured a direction cannot be committed.</p>
<b>Options</b>	<p><b>inbound</b>—Enable MACsec security on traffic entering the interface that has applied the secure channel.</p> <p><b>outbound</b>—Enable MACsec security on traffic leaving the interface that has applied the secure channel.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## dhcp-option82

---

<b>Syntax</b>	<pre>dhcp-option82 {   circuit-id {     prefix hostname;     use-interface-description;     use-vlan-id;   }   remote-id {     prefix hostname   mac   none;     use-interface-description;     use-string <i>string</i>;   }   vendor-id &lt;<i>string</i>&gt;; }</pre>
<b>Hierarchy Level</b>	<p>[edit <a href="#">ethernet-switching-options secure-access-port vlan</a> (all   <i>vlan-name</i>)]</p> <p>[edit forwarding-options helpers bootp]</p> <p>[edit forwarding-options helpers bootp interface <i>interface-name</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
<b>Description</b>	<p>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.</p> <p>The remaining statements are explained separately.</p>
<b>Default</b>	Insertion of DHCP option 82 information is not enabled.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101</a></li><li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98</a></li><li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 156</a></li><li>• <a href="#">Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 153</a></li><li>• <a href="#">[edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches on page 168</a></li></ul>

- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.

## dhcp-snooping-file


<b>Syntax</b>	<pre>dhcp-snooping-file {   location ( local_pathname   remote_URL );   timeout seconds;   write-interval seconds; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">ethernet-switching-options secure-access-port</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4 for EX Series switches.
<b>Description</b>	<p>Ensure that IP-MAC bindings persist through switch reboots by specifying a local pathname or a remote URL for the storage location of the DHCP snooping database file.</p> <p>The remaining statements are explained separately.</p>
<b>Default</b>	The IP-MAC bindings in the DHCP snooping database file are not persistent. If the switch is rebooted, the bindings are lost.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 161</a></li> <li>• <a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li> </ul>

## dhcp-trusted

---

<b>Syntax</b>	(dhcp-trusted   no-dhcp-trusted);
<b>Hierarchy Level</b>	[edit <a href="#">ethernet-switching-options secure-access-port interface</a> (all   <i>interface-name</i> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	<p>Allow DHCP responses from the specified interfaces (ports) or all interfaces.</p> <ul style="list-style-type: none"><li>• <b>dhcp-trusted</b>—Allow DHCP responses.</li><li>• <b>no-dhcp-trusted</b>—Deny DHCP responses.</li></ul>
<b>Default</b>	Trusted for trunk ports, untrusted for access ports.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li><li>• <a href="#">Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 54</a></li><li>• <a href="#">Enabling a Trusted DHCP Server (CLI Procedure) on page 136</a></li><li>• <a href="#">Enabling a Trusted DHCP Server (J-Web Procedure) on page 136</a></li></ul>

## disable-timeout

<b>Syntax</b>	<code>disable-timeout <i>timeout</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">ethernet-switching-options port-error-disable</a> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6 for EX Series switches.
<b>Description</b>	Specify how long the Ethernet switching interfaces remain in a disabled state because of MAC limiting, MAC move limiting, or storm control errors.
<div>  <p><b>NOTE:</b> If you modify the timeout value of an existing disable timeout setting, 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.</p> <p>You can bring up the currently disabled interfaces by running the operational command <code>clear ethernet-switching port-error</code>.</p> </div>	
<b>Default</b>	The disable timeout is not enabled.
<b>Options</b>	<p><b><i>timeout</i></b>—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.</p> <p><b>Range:</b> 10 through 3600 seconds</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches</i></li> <li>• <a href="#">Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)</a> on page 159</li> </ul>

## encryption

---

<b>Syntax</b>	encryption;
<b>Hierarchy Level</b>	[edit security <a href="#">macsec connectivity-association connectivity-association-name secure-channel secure-channel-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Enable MACsec encryption within a secure channel.</p> <p>You can enable MACsec without enabling encryption. If a connectivity association with a secure channel that has not enabled MACsec encryption is associated with an interface, traffic is forwarded across the Ethernet link in clear text. You are, therefore, able to view this unencrypted traffic when you are monitoring the link. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic has not been tampered with and does not represent a security threat.</p> <p>Traffic traversing a MAC-enabled point-to-point Ethernet link traverses the link at the same speed regardless of whether encryption is enabled or disabled. You cannot increase the speed of traffic traversing a MACsec-enabled Ethernet link by disabling encryption.</p> <p>This command is used to enable encryption when MACsec is configured using secure association key (SAK) security mode only. When MACsec is configuring using static connectivity association key (CAK) security mode, the encryption setting is configured outside of the secure channel using the <a href="#">no-encryption</a> configuration statement.</p>
<b>Default</b>	MACsec encryption is disabled when MACsec is configured using static SAK security mode, by default.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>



## 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]) {
            (disable | drop | shutdown);
        }
    }
    dot1q-tunneling {
        ether-type (0x8100 | 0x88a8 | 0x9100);
    }
    interfaces interface-name {
        no-mac-learning;
    }
    mac-lookup-length number-of-entries;
    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;
}
dhcpv6-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 (drop | log | none | shutdown);
    no-allowed-mac-log;
    persistent-learning;
    static-ip ip-address {
        vlan vlan-name;
        mac mac-address;
    }
    static-ipv6 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-dhcpv6 | no-examine-dhcpv6) {
        forwarding-class class-name;
    }
    examine-fip {
        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    (ipv6-source-guard | no-ipv6-source-guard);
    mac-move-limit limit action (drop | log | none | shutdown);

```

```

    }
    (neighbor-discovery-inspection | no-neighbor-discovery-inspection);
no-option-37;
static {
    vlan name {
        mac mac-address {
            next-hop interface-name;
        }
    }
}
storm-control {
    action-shutdown;
    interface (all | interface-name) {
        bandwidth bandwidth;
        level level;
        multicast;
        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*
- [Understanding Port Security on page 7](#)
- *Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches*
- *Understanding Redundant Trunk Links*
- *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*
- *Understanding MAC Notification on EX Series Switches*
- *Understanding FIP Snooping*
- *Understanding Nonstop Bridging on EX Series Switches*

## examine-dhcp

<b>Syntax</b>	( <code>examine-dhcp</code>   <code>no-examine-dhcp</code> ) { <code>forwarding-class class-name</code> ; }
<b>Hierarchy Level</b>	[edit <code>ethernet-switching-options secure-access-port vlan</code> (all   <code>vlan-name</code> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	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 (DHCP OFFER, DHCP DECLINE, DHCP ACK, and DHCP NAK 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.

<b>Default</b>	Disabled.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li> <li>• <a href="#">Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69</a></li> <li>• <a href="#">Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61</a></li> <li>• <a href="#">Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 104</a></li> </ul>

- [Enabling DHCP Snooping \(CLI Procedure\) on page 132](#)
- [Enabling DHCP Snooping \(J-Web Procedure\) on page 135](#)

## examine-dhcpv6

<b>Syntax</b>	<code>examine-dhcpv6 {     forwarding-class <i>class-name</i>; }</code>
<b>Hierarchy Level</b>	[edit <code>ethernet-switching-options secure-access-port vlan</code> (all   <i>vlan-name</i> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
<b>Description</b>	Enable DHCPv6 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.

When DHCP snooping is enabled, the switch logs DHCP packets (DHCP OFFER, DHCP DECLINE, DHCP ACK, and DHCP NAK 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.

<b>Default</b>	Disabled.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li> <li>• <a href="#">Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69</a></li> <li>• <a href="#">Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61</a></li> <li>• <a href="#">Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 104</a></li> <li>• <a href="#">Enabling DHCP Snooping (CLI Procedure) on page 132</a></li> <li>• <a href="#">Enabling DHCP Snooping (J-Web Procedure) on page 135</a></li> </ul>


## exclude-protocol

---

<b>Syntax</b>	<code>exclude-protocol <i>protocol-name</i>;</code>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies protocols whose packets are not secured using Media Access Control Security (MACsec) when MACsec is enabled on a link using static connectivity association key (CAK) security mode.</p> <p>When this option is enabled in a connectivity association that is attached to an interface, MACsec is not enabled for all packets of the specified protocols that are sent and received on the link.</p>
<b>Default</b>	<p>Disabled.</p> <p>All packets are secured on a link when MACsec is enabled, with the exception of all types of Spanning Tree Protocol (STP) packets.</p>
<b>Options</b>	<p><b><i>protocol-name</i></b>—Specifies the name of the protocol that should not be MACsec-secured. Options include:</p> <ul style="list-style-type: none"><li>• <b>cdp</b>—Cisco Discovery Protocol.</li><li>• <b>lcp</b>—Link Aggregation Control Protocol.</li><li>• <b>lldp</b>—Link Level Discovery Protocol.</li></ul>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>



## forwarding-class (for DHCP Snooping or DAI Packets)

<b>Syntax</b>	forwarding-class class <i>class-name</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">ethernet-switching-options secure-access-port vlan</a> (all   <i>vlan-name</i> ) ( <a href="#">examine-dhcp</a>   <a href="#">arp-inspection</a> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches. Statement introduced in Junos OS Release 12.1 for the QFX Series.
<b>Description</b>	Assign a user-defined or a predefined forwarding class to the packets that have been checked for DHCP snooping or dynamic ARP inspection (DAI).
<div>  <p><b>NOTE:</b> To assign a user-defined class, you must first configure the user-defined class by using the <i>forwarding-classes</i> configuration statement at the [edit <i>class-of-service</i>] hierarchy level.</p> </div>	
<b>Default</b>	Disabled.
<b>Options</b>	<i>class-name</i> —Name of the forwarding class. The forwarding class can be one of the predefined forwarding classes (best-effort, assured-forwarding, expedited-forwarding, network-control) or it can be a user-defined forwarding class.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 104</a></li> <li>• <a href="#">Understanding Junos OS CoS Components for EX Series Switches</a></li> <li>• <a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li> <li>• <a href="#">Understanding DAI for Port Security on page 20</a></li> </ul>

## id

---

<b>Syntax</b>	<pre>id {     <a href="#">mac-address</a> <i>mac-address</i>;     <a href="#">port-id</a> <i>port-id-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec</a> <a href="#">connectivity-association</a> <i>connectivity-association-name</i> <a href="#">secure-channel</a> <i>secure-channel-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	Specify a MAC address and a port that traffic on the link must be from to be accepted by the interface when MACsec is enabled using static secure association key (SAK) security mode.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>

## include-sci

---

<b>Syntax</b>	include-sci;
<b>Hierarchy Level</b>	[edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies that the SCI tag should be appended to each packet on a link that has enabled MACsec.</p> <p>You must enable SCI tagging on a switch that is enabling MACsec on an Ethernet link connecting to an EX4300 switch.</p> <p>SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. This option is, therefore, not available on EX4300 switches.</p> <p>You should only use this option when connecting a switch to an EX4300 switch, or to a host device that requires SCI tagging. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.</p>
<b>Default</b>	<p>SCI tagging is enabled on EX4300 switches that have enabled MACsec using static connectivity association key (CAK) security mode, by default.</p> <p>SCI tagging is disabled on all other interfaces, by default.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## interface (Access Port Security)

```
Syntax  interface (all | interface-name) {
        allowed-mac {
            mac-address-list;
        }
        (dhcp-trusted | no-dhcp-trusted);
        fcoe-trusted;
        mac-limit limit action (drop | log | none | shutdown);
        no-allowed-mac-log;
        persistent-learning;
        static-ip ip-address {
            vlan vlan-name;
            mac mac-address;
        }
        static-ipv6 ip-address {
            vlan vlan-name;
            mac mac-address;
        }
        }
        }
        vlan vlan-name {
            mac-limit limit action (drop | log | none | shutdown);
        }
    }
```

**Hierarchy Level** [edit [ethernet-switching-options secure-access-port](#)]

**Release Information** Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Support for the **ipv6-source-guard** statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

**Description** Apply port security features to all interfaces or to the specified interface.

**Options** **all**—Apply port security features to all interfaces.

***interface-name***—Apply port security features to 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**

- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 66](#)
- [Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 51](#)
- [Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 58](#)

- [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 54](#)
- [Configuring MAC Limiting \(CLI Procedure\) on page 140](#)
- [Enabling a Trusted DHCP Server \(CLI Procedure\) on page 136](#)
- [Configuring Static IP Addresses for DHCP Bindings on Access Ports \(CLI Procedure\) on page 152](#)

## interfaces (MACsec)

<b>Syntax</b>	<code>interfaces <i>interface-name</i> {     connectivity-association <i>connectivity-association-name</i>; }</code>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Applies the specified connectivity association to the specified interface to enable MACsec.</p> <p>One connectivity association can be applied to multiple interfaces.</p> <p>You must always use this statement to apply a connectivity association to an interface to enable MACsec. You must complete this configuration step regardless of whether MACsec is enabled using static connectivity association key (CAK) security mode or static secure association key (SAK) security mode.</p> <p>If you are enabling MACsec using static SAK security mode and need to configure MACsec on inbound and outbound traffic on the same interface, you must configure a connectivity association with one secure channel for inbound traffic and a second secure channel for outbound traffic. The connectivity association is then applied to the interface using this statement to enable MACsec for traffic entering and leaving the interface.</p>
<b>Default</b>	Interfaces are not associated with any connectivity associations, by default.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## ip-source-guard


<b>Syntax</b>	<code>ip-source-guard;</code>
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with ELS: [edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</li> <li>For platforms without ELS: [edit <b>ethernet-switching-options secure-access-port</b> <i>vlan</i> (all   <i>vlan-name</i>)]</li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p>
<b>Description</b>	<p>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.</p> <ul style="list-style-type: none"> <li><b>ip-source-guard</b>—Enable IP source guard checking.</li> <li><b>no-ip-source-guard</b>—(Not available in [edit vlans <i>vlan-name</i> forwarding-options dhcp-security]) Disable IP source guard checking.</li> </ul> <p>If you configure IP source guard at the [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] hierarchy level:</p> <ul style="list-style-type: none"> <li>IP source guard can be configured only for a specific VLAN, not for a list or a range of VLAN IDs.</li> <li>DHCP snooping is automatically enabled.</li> </ul> <p>See <i>Configuring IP Source Guard (CLI Procedure)</i> for more information about this configuration.</p> <p>If you configure IP source guard at the [edit <b>ethernet-switching-options secure-access-port</b> <i>vlan</i> (all   <i>vlan-name</i>)] hierarchy level:</p> <ul style="list-style-type: none"> <li>You must enable DHCP snooping on all VLANs if you configure IP source guard on all VLANs.</li> <li>You must enable DHCP snooping for the specific VLAN if you configure IP source guard on that specific VLAN. Otherwise, the default behavior of no DHCP snooping applies to that VLAN.</li> </ul> <p>See “<a href="#">Enabling DHCP Snooping (CLI Procedure)</a>” on <a href="#">page 132</a> for more information about this configuration.</p>



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

<b>Default</b>	Disabled.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 87</a></li> <li>• <a href="#">Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 77</a></li> <li>• <a href="#">Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing</a></li> <li>• <a href="#">Configuring IP Source Guard (CLI Procedure) on page 148</a></li> <li>• <a href="#">Configuring IP Source Guard (CLI Procedure)</a></li> </ul>

## ipv6-source-guard-sessions

<b>Syntax</b>	<pre>ipv6-source-guard-sessions {     max-number <i>max-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">ethernet-switching-options secure-access-port</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
<b>Description</b>	Specify the maximum number of IPv6 source guard sessions for TCAM space provisioning.
	<div>  <p><b>NOTE:</b> After setting or changing the maximum number of IPv6 source guard sessions and committing the configuration, you must reboot the switch for the configuration to take effect.</p> </div>
<b>Default</b>	Disabled.
<b>Options</b>	<b>max-number <i>max-number</i></b> —The maximum number of IPv6 source guard sessions. <b>Range:</b> 50 through 300.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect the Switch from IPv6 Address Spoofing</a></li> <li>• <a href="#">Configuring IP Source Guard (CLI Procedure)</a></li> </ul>

## key

---

<b>Syntax</b>	<code>key key-string;</code>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec connectivity-association connectivity-association-name secure-channel secure-channel-name security-association security-association-number</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies the static security key to exchange to enable MACsec using static secure association key (SAK) security mode.</p> <p>The key string is a 32-digit hexadecimal number. The key string and the security association must match on both sides of an Ethernet connection to secure traffic using MACsec when enabling MACsec using SAK security mode.</p> <p>You must configure at least two security associations with unique security association numbers and key strings to enable MACsec using static SAK security mode. MACsec initially establishes a secure connection when a security association number and key match on both ends of an Ethernet link. After a certain number of Ethernet frames are securely transmitted across the Ethernet link, MACsec automatically rotates to a new security association with a new security association number and key to maintain the secured Ethernet link. This rotation continues each time a certain number of Ethernet frames are securely transmitted across the secured Ethernet link, so you must always configure MACsec to have at least two security associations.</p>
<b>Default</b>	This statement does not have a default value.
<b>Options</b>	<b>key-string</b> —Specifies the key to exchange with the other end of the link on the secure channel. The <i>key-string</i> is a 32-digit hexadecimal string that is created by the user.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>



## key-server-priority

---

<b>Syntax</b>	<code>key-server-priority <i>priority-number</i>;</code>
<b>Hierarchy Level</b>	[edit security <code>macsec connectivity-association</code> <i>connectivity-association-name</i> mka]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies the key server priority used by the MACsec Key Agreement (MKA) protocol to select the key server when MACsec is enabled using static connectivity association key (CAK) security mode.</p> <p>The switch with the lower <i>priority-number</i> is selected as the key server.</p> <p>If the <i>priority-number</i> is identical on both sides of a point-to-point link, the MKA protocol selects the device with the lower MAC address as the key server.</p>
<b>Default</b>	The default key server priority number is 16.
<b>Options</b>	<p><i>priority-number</i>—Specifies the MKA server election priority number.</p> <p>The <i>priority-number</i> can be any number between 0 and 255. The lower the number, the higher the priority.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## location (DHCP Snooping Database)

---

<b>Syntax</b>	<code>location (<i>local_pathname</i>   <i>remote_url</i>);     <code>timeout</code> <i>seconds</i>;     <code>write-interval</code> <i>seconds</i>; }</code>
<b>Hierarchy Level</b>	[edit <code>ethernet-switching-options secure-access-port dhcp-snooping-file</code> ]; [edit <code>ethernet-switching-options secure-access-port dhcpv6-snooping-file</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4 for EX Series switches. Support at the [edit <code>ethernet-switching-options secure-access-port dhcpv6-snooping-file</code> ] hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
<b>Description</b>	<p>Configure IP-MAC address bindings to persist through switch reboots by specifying a location in which to store the DHCP snooping database. When specifying the location for the DHCP snooping database, you must also specify how frequently the switch writes (<code>write-interval</code>) the database entries into the DHCP snooping database file.</p> <p>If you choose to store the DHCP snooping database on a remote FTP site, you might want to specify the time (<code>timeout</code>) that the switch waits for a remote system to respond when the DHCP snooping database is stored on a remote FTP site. This is optional.</p>
<b>Options</b>	<p><i>local_pathname</i>   <i>remote_url</i></p> <ul style="list-style-type: none"><li>• <i>local_pathname</i>—Use <i>/path</i> to store the database file on the local switch.</li><li>• <i>remote_url</i>—Use <code>ftp://ip-address</code> or <code>ftp:// hostname/path</code> to store the database on a remote FTP site.</li></ul>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 161</a></li><li>• <a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li></ul>

## mac

<b>Syntax</b>	<code>mac mac-address;</code>
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with Enhanced Layer 2 Software (ELS):  <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security group <i>group-name</i> interface <i>interface-name</i> static-ip <i>ip-address</i>]</code> </li> <li>For platforms without ELS:  <code>[edit ethernet-switching-options secure-access-port interface (all   <i>interface-name</i>) static-ip <i>ip-address</i> vlan <i>vlan-name</i>]</code> </li> <li>For MX Series platforms:  <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security group <i>group-name</i> interface <i>interface-name</i> static-ip <i>ip-address</i>]</code> </li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Hierarchy level <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Hierarchy level <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.</p>
<b>Description</b>	Configure the media access control (MAC) address or hardware address of the device connected to the specified interface.
<b>Options</b>	<i>mac-address</i> —Value (in hexadecimal format) of the address assigned to this device.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 152</a></li> <li><a href="#">Configuring Static IP Addresses for DHCP and DHCPv6 Bindings on Access Ports (CLI Procedure)</a></li> <li><a href="#">Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure)</a></li> </ul>

## mac-address (MACsec)

---

<b>Syntax</b>	<code>mac-address <i>mac-address</i>;</code>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> <a href="#">secure-channel</a> <i>secure-channel-name</i> id]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specify a MAC address to enable MACsec using static secure association key (SAK) security mode. The <b>mac-address</b> variables must match on the sending and receiving ends of a link to enable MACsec using static SAK security mode.</p> <p>If you are configuring a MAC address on a secure channel in the outbound direction, you should specify the MAC address of the interface as the <b>mac-address</b>.</p> <p>If you are configuring a MAC address on a secure channel in the inbound direction, you should specify the MAC address of the interface at the other end of the link as the <b>mac-address</b>.</p> <p>You only use this configuration option when you are configuring MACsec using static SAK security mode. This option does not need to be specified when you are enabling MACsec using static connectivity association key (CAK) security mode.</p>
<b>Default</b>	No MAC address is specified in the secure channel, by default.
<b>Options</b>	<b>mac-address</b> —The MAC address, in six groups of two hexadecimal digits.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>

## mac-limit (Access Port Security)

<b>Syntax</b>	<code>mac-limit <i>limit</i> action <i>action</i>;</code>
<b>Hierarchy Level</b>	[edit <b>ethernet-switching-options secure-access-port interface</b> (all   <i>interface-name</i> )], [edit ethernet-switching-options secure-access-port interface <i>interface-name</i> ) vlan <i>vlan-name</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	<p>Set a limit on the number of MAC addresses that can be added to the Ethernet switching table.</p> <ul style="list-style-type: none"> <li>[edit ethernet-switching options secure-access-port interface]—Set the MAC address learning limit for a specific interface, for a range of interfaces, or for all interfaces on the switch.</li> <li>[edit ethernet-switching options secure-access-port interface <i>interface-name</i> vlan <i>vlan-name</i>]—Set the MAC address learning limit for a specific interface as a member of a specific VLAN (VLAN membership MAC limit).</li> </ul>



**NOTE:** If you set the MAC address limit on a specific interface as a member of a specific VLAN (VLAN membership MAC limit), the switch drops any additional packets when the VLAN membership MAC limit is exceeded and logs the MAC addresses of those packets. You cannot specify a different action for this specific configuration. If a single interface belongs to more than one VLAN, you can set separate VLAN membership MAC limits for the same interface.

When you reset the number of MAC addresses, the MAC address table is not automatically cleared. Previous entries remain in the table after you reduce the number of addresses, so you should clear the forwarding table for the specified interface or MAC address. Use the **clear ethernet-switching table** command to clear the existing MAC addresses from the table.

<b>Default</b>	The default action is <b>drop</b> .
<b>Options</b>	<p><b>action <i>action</i></b>—(Optional) Action to take when the MAC address limit for an interface or for all interfaces is exceeded:</p> <ul style="list-style-type: none"> <li><b>drop</b>—Drop the packet and generate a system log entry.</li> <li><b>log</b>—Do not drop the packet but generate a system log entry.</li> <li><b>none</b>—No action.</li> <li><b>shutdown</b>—Disable the interface and generate a system log entry. If you have configured the switch with the <b>port-error-disable</b> statement, the disabled interface recovers automatically upon expiration of the specified disable timeout. If you have not</li> </ul>

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.

*limit*—Maximum number of MAC addresses.

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system—control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">allowed-mac on page 176</a></li><li>• <i>clear ethernet-switching table</i></li><li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li><li>• <a href="#">Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 51</a></li><li>• <a href="#">Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 58</a></li><li>• <a href="#">Configuring MAC Limiting (CLI Procedure) on page 140</a></li><li>• <a href="#">Configuring MAC Limiting (J-Web Procedure) on page 143</a></li><li>• <a href="#">Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 159</a></li></ul>

## mac-move-limit

<b>Syntax</b>	<pre>mac-move-limit {     limit;     &lt;action action   packet-action action&gt;; }</pre>
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with ELS:            [edit vlans <i>vlan-name</i> switch-options]         </li> <li>For platforms without ELS:            [edit <b>ethernet-switching-options secure-access-port</b> <i>vlan</i> (all   <i>vlan-name</i>)]         </li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Hierarchy level [edit vlans <i>vlan-name</i> switch-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p>
<b>Description</b>	Specify the number of times a MAC address can move to a new interface (port) in one second and the action to be taken by the switch if the MAC address move limit is exceeded.
<b>Default</b>	If you do not specify <b>mac-move-limit</b> , the default MAC address move limit is unlimited.
<b>Options</b>	<p><b>limit</b> <i>limit</i>—Maximum number of moves to a new interface per second.</p> <ul style="list-style-type: none"> <li><b>action</b> <i>action</i>—(Optional) (Available <i>only</i> under the hierarchy level [edit <b>ethernet-switching-options secure-access-port</b> <i>vlan</i> (all   <i>vlan-name</i>) <b>mac-move-limit</b>]) Action to take when the MAC address move limit is reached:           <ul style="list-style-type: none"> <li><b>drop</b>—Drop the packet and generate a system log entry. This is the default.</li> <li><b>log</b>—Do not drop the packet but generate a system log entry.</li> <li><b>none</b>—No action.</li> <li><b>shutdown</b>—Disable the interface and generate a system log entry. If you have configured the switch with the <b>port-error-disable</b> 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 <b>clear ethernet-switching port-error</b> command.</li> </ul> </li> <li><b>packet-action</b> <i>action</i>—(Optional) (Available <i>only</i> under the hierarchy level, [edit vlans <i>vlan-name</i> switch-options <b>mac-move-limit</b>]) Action to take when the MAC address move limit is reached:</li> </ul>



**NOTE:** There is no default action.

- drop**—Drop the packet and do not generate an alarm.

- **drop and log**—Drop the packet and generate an alarm, an SNMP trap, or system log entry.
- **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 or an SNMP trap. If you have configured the interface with the **recovery-timeout** statement, the disabled interface recovers automatically upon expiration of the specified timeout. If you have not configured the interface for a recovery timeout, you can bring up the disabled interface by running the operational command **clear ethernet-switching recovery-timeout**.

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

- Related Documentation**
- [Example: Configuring Basic Port Security Features on page 43](#)
  - [Configuring MAC Move Limiting \(CLI Procedure\) on page 145](#)
  - [Configuring MAC Move Limiting \(CLI Procedure\) \(ELS\)](#)
  - [Configuring Persistent MAC Learning \(CLI Procedure\)](#)
  - [Configuring MAC Move Limiting \(J-Web Procedure\) on page 147](#)
  - [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 159](#)
  - [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\)](#)



## macsec

```
Syntax  macsec {
        connectivity-association connectivity-association-name {
            exclude-protocol protocol-name;
            include-sci;
            mka {
                must-secure;
                key-server-priority priority-number;
                transmit-interval interval;
            }
            no-encryption;
            offset (0|30|50);
            pre-shared-key {
                cak hexadecimal-number;
                ckn hexadecimal-number;
            }
            replay-protect {
                replay-window-size number-of-packets;
            }
            secure-channel secure-channel-name {
                direction (inbound | outbound);
                encryption;
                id {
                    mac-address mac-address;
                    port-id port-id-number;
                }
                offset (0|30|50);
                security-association security-association-number {
                    key key-string;
                }
            }
            security-mode security-mode;
        }
        interfaces interface-name {
            connectivity-association connectivity-association-name;
        }
    }
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.  
Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.

**Description** Configure Media Access Control Security (MACsec)..

**Options** The remaining statements are explained separately.

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

**Related Documentation**

- [Configuring Media Access Control Security \(MACsec\) on page 116](#)

## mka

---

<b>Syntax</b>	<pre>mka {     must-secure;     key-server-priority <i>priority-number</i>;     transmit-interval <i>interval</i>; }</pre>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15. Statement introduced in Junos OS Release 14.1X53-D15 for the QFX Series.
<b>Description</b>	Specify parameters for the MACsec Key Agreement (MKA) protocol.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>

## must-secure

---

<b>Syntax</b>	must-secure;
<b>Hierarchy Level</b>	[edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> <b>mka</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1X53-D10. Statement introduced in Junos OS Release 14.1X53-D15 for the QFX Series.
<b>Description</b>	<p>Specifies that all traffic travelling on the MACsec-secured link must be MACsec-secured to be forwarded onward.</p> <p>When the <b>must-secure</b> option is enabled, all traffic that is not MACsec-secured that is received on the interface is dropped.</p> <p>When the <b>must-secure</b> option is disabled, all traffic from devices that support MACsec is MACsec-secured while traffic received from devices that do not support MACsec is forwarded through the network.</p> <p>The <b>must-secure</b> option is particularly useful in scenarios where multiple devices, such as a phone and a PC, are accessing the network through the same Ethernet interface. If one of the devices supports MACsec while the other device does not support MACsec, the device that doesn't support MACsec can continue to send and receive traffic over the network—provided the <b>must-secure</b> option is disabled—while traffic to and from the device that supports MACsec is MACsec-secured. In this scenario, traffic to the device that is not MACsec-secured must be VLAN-tagged.</p>
<b>Default</b>	The <b>must-secure</b> option is disabled.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## no-allowed-mac-log

---

<b>Syntax</b>	no-allowed-mac-log;
<b>Hierarchy Level</b>	[edit <a href="#">ethernet-switching-options secure-access-port interface</a> (all   <i>interface-name</i> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3 for EX Series switches.
<b>Description</b>	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.
<b>Default</b>	The switch logs messages when it receives packets from invalid MAC addresses on an interface that has been configured for particular (allowed) MAC addresses.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system—control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">allowed-mac on page 176</a></li><li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li><li>• <a href="#">Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 66</a></li><li>• <a href="#">Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 58</a></li><li>• <a href="#">Configuring MAC Limiting (CLI Procedure) on page 140</a></li><li>• <a href="#">Configuring MAC Limiting (J-Web Procedure) on page 143</a></li></ul>

## no-encryption

---

<b>Syntax</b>	no-encryption;
<b>Hierarchy Level</b>	[edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Disables MACsec encryption for a connectivity association that is configured to enable MACsec using static connectivity association key (CAK) or dynamic security mode.</p> <p>You can enable MACsec without enabling encryption. If a connectivity association that has not enabled MACsec encryption is associated with an interface, traffic is forwarded across the Ethernet link in clear text. You are, therefore, able to view this unencrypted traffic when you are monitoring the link. The MACsec header is still applied to the packet, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic does not represent a security threat.</p> <p>This command is used to disable encryption when MACsec is configured using static CAK or dynamic security mode only. When MACsec is configuring using static secure association key (SAK) security mode, the encryption setting is managed in the secure channel using the <b>encryption</b> configuration statement.</p>
<b>Default</b>	MACsec encryption is enabled if MACsec is enabled using static CAK or dynamic security mode.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## no-examine-dhcpv6

---

<b>Syntax</b>	<code>no-examine-dhcpv6 {     forwarding-class class-name; }</code>
<b>Hierarchy Level</b>	[edit <code>ethernet-switching-options secure-access-port vlan</code> (all   <i>vlan-name</i> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
<b>Description</b>	<p>Disable DHCPv6 snooping on all VLANs or on the specified VLAN.</p> <p>The remaining statement is explained separately.</p>
<b>Default</b>	Disabled.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">examine-dhcpv6 on page 195</a></li><li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li><li>• <a href="#">Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69</a></li><li>• <a href="#">Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61</a></li><li>• <a href="#">Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 104</a></li><li>• <a href="#">Enabling DHCP Snooping (CLI Procedure) on page 132</a></li><li>• <a href="#">Enabling DHCP Snooping (J-Web Procedure) on page 135</a></li></ul>


## no-gratuitous-arp-request

<b>Syntax</b>	no-gratuitous-arp-request;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure the switch not to respond to gratuitous ARP requests. You can disable responses to gratuitous ARP requests on Layer 2 Ethernet switching interfaces, and integrated routing and bridging (IRB) interfaces or routed VLAN interfaces (RVIs). (On EX Series switches that use Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, the feature is known as an IRB interface. On EX Series switches that use Junos OS that does not support ELS, the feature is known as an RVI.)
<b>Default</b>	Gratuitous ARP responses are enabled on all Ethernet switching interfaces, and IRB interfaces or RVIs.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Configuring Proxy ARP on an EX Series Switch</i></li> <li>• <i>Configuring Proxy ARP (CLI Procedure)</i></li> <li>• <i>Configuring Proxy ARP (CLI Procedure)</i></li> </ul>

## no-option-37

<b>Syntax</b>	no-option-37;
<b>Hierarchy Level</b>	[edit ethernet-switching-options <a href="#">secure-access-port</a> vlan <i>vlan-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
<b>Description</b>	Configure the VLAN <i>not</i> to transmit DHCP option 37 information, even if the VLAN is configured to perform DHCPv6 snooping.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>option-82</i></li> <li>• <a href="#">Understanding DHCP Option 82 for Port Security on Switching Devices on page 35</a></li> <li>• <a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li> </ul>

## offset

<b>Syntax</b>	offset (0  30   50);
<b>Hierarchy Level</b>	[edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i> ] [edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i> <b>secure-channel</b> <i>secure-channel-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies the number of octets in an Ethernet frame that are sent in unencrypted plain-text when encryption is enabled for MACsec.</p> <p>Setting the offset to 30 allows a feature to see the IPv4 header and the TCP/UDP header while encrypting the remaining traffic. Setting the offset to 50 allows a feature to see the IPv6 header and the TCP/UDP header while encrypting the remaining traffic.</p> <p>You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.</p> <p>You configure the <b>offset</b> in the [edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i>] hierarchy when you are enabling MACsec using static connectivity association key (CAK) or dynamic security mode.</p> <p>You configure the <b>offset</b> in the [edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i> <b>secure-channel</b> <i>secure-channel-name</i>] hierarchy when you are enabling MACsec using static secure association key (SAK) security mode.</p>
<b>Default</b>	0
<b>Options</b>	<p><b>0</b>—Specifies that no octets are unencrypted. When you set the offset to 0, all traffic on the interface where the connectivity association or secure channel is applied is encrypted.</p> <p><b>30</b>—Specifies that the first 30 octets of each Ethernet frame are unencrypted.</p>
	<p> <b>NOTE:</b> In IPv4 traffic, setting the offset to 30 allows a feature to see the IPv4 header and the TCP/UDP header while encrypting the rest of the traffic. An offset of 30, therefore, is typically used when a feature needs this information to perform a task on IPv4 traffic.</p>
	<p><b>50</b>—Specified that the first 50 octets of each Ethernet frame are unencrypted.</p>





**NOTE:** In IPv6 traffic, setting the offset to 50 allows a feature to see the IPv6 header and the TCP/UDP header while encrypting the rest of the traffic. An offset of 50, therefore, is typically used when a feature needs this information to perform a task on IPv6 traffic.

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

**Related Documentation**

- [Configuring Media Access Control Security \(MACsec\) on page 116](#)

## persistent-learning

**Syntax** persistent-learning;

**Hierarchy Level**

- For platforms without ELS:  
[edit **ethernet-switching-options** **secure-access-port** **interface** (all | *interface-name*)]
- For platforms with ELS:  
[edit switch-options **interface** *interface-name*]

**Release Information** Statement introduced in Junos OS Release 11.4 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.  
Hierarchy level [edit switch-options interface interface-name] introduced in Junos OS Release 13.2X50-D10

**Description** Specify that learned MAC addresses persist on the specified interfaces across restarts of the switch and link-down conditions. This feature is also known as sticky MAC.


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

**Related Documentation**

- [Example: Configuring Basic Port Security Features on page 43](#)
- [Configuring Persistent MAC Learning \(CLI Procedure\) on page 159](#)
- [Configuring Persistent MAC Learning \(CLI Procedure\)](#)

## port-error-disable

---

Syntax	<pre>port-error-disable {     disable-timeout <i>timeout</i> ; }</pre>
Hierarchy Level	[edit <a href="#">ethernet-switching-options</a> ],
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches.
Description	<p>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:</p> <ul style="list-style-type: none"><li>• If you have enabled MAC limiting with the <b>shutdown</b> option and you enable <b>port-error-disable</b>, the switch disables (rather than shuts down) the interface when the MAC address limit is reached.</li><li>• If you have enabled MAC move limiting with the <b>shutdown</b> option and you enable <b>port-error-disable</b>, the switch disables (rather than shuts down) the interface when the maximum number of moves to a new interface is reached.</li><li>• If you have enabled storm control with the <b>action-shutdown</b> option and you enable <b>port-error-disable</b>, 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.</li></ul>
	<div> <b>NOTE:</b> The <b>port-error-disable</b> configuration does not apply to pre-existing error conditions. It impacts only error conditions that are detected after <b>port-error-disable</b> has been enabled and committed. To clear a pre-existing error condition and restore the interface to service, use the operational command that appears in your CLI:</div> <ul style="list-style-type: none"><li>• <code>clear ethernet-switching port-error</code></li></ul>
	<p>The remaining statement is explained separately.</p>
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	<ul style="list-style-type: none"><li>• <a href="#">action-shutdown</a></li><li>• <a href="#">Configuring MAC Move Limiting (CLI Procedure) on page 145</a></li></ul>

## port-id

---

<b>Syntax</b>	<code>port-id <i>port-id-number</i>;</code>
<b>Hierarchy Level</b>	[edit security <code>macsec connectivity-association connectivity-association-name secure-channel secure-channel-name id</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specify a port ID in a secure channel when enabling MACsec using static secure association key (SAK) security mode. The port IDs must match on a sending and receiving secure channel on each side of a link to enable MACsec.</p> <p>Once the port numbers match, MACsec is enabled for all traffic on the connection.</p> <p>You only use this configuration option when you are configuring MACsec using static SAK security mode. This option does not need to be specified when you are enabling MACsec using static connectivity association key (CAK) security mode.</p>
<b>Default</b>	No port ID is specified.
<b>Options</b>	<i>port-id-number</i> —The port ID number.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## pre-shared-key

---

<b>Syntax</b>	<pre>pre-shared-key {     cak hexadecimal-number;     ckn hexadecimal-number; }</pre>
<b>Hierarchy Level</b>	[edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies the pre-shared key used to enable MACsec using static connectivity association key (CAK) security mode.</p> <p>A pre-shared key includes a connectivity association key name (CKN) and a connectivity association key (CAK). A pre-shared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using static CAK security mode. The MACsec Key Agreement (MKA) protocol is enabled after the pre-shared keys are successfully verified and exchanged. The pre-shared key—the CKN and CAK—must match on both ends of a link.</p>
<b>Default</b>	No pre-shared keys exist, by default.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>

## prefix (Circuit ID for Option 82)

<b>Syntax</b>	<pre> prefix {     host-name;     logical-system-name;     routing-instance-name; } </pre>
<b>For Platforms with Enhanced Layer 2 Software (ELS)</b>	[edit vlans forwarding-options dhcp-security option-82 <b>circuit-id</b> ]
<b>For Platforms Without ELS</b>	[edit <b>ethernet-switching-options secure-access-port</b> <b>vlan</b> (all   <i>vlan-name</i> ) <b>dhcp-option82 circuit-id</b> ], [edit forwarding-options helpers bootp <b>dhcp-option82 circuit-id</b> ], [edit forwarding-options helpers bootp interface <i>interface-name</i> <b>dhcp-option82 circuit-id</b> ]
<b>For MX Series Platforms</b>	[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82 <b>circuit-id</b> ]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 <b>circuit-id</b>] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 14.1 for the MX Series.</p>
<b>Description</b>	Configure an optional prefix for the circuit ID suboption in the DHCP option 82 information that is inserted by the switch or router into the packet header of a DHCP request before it forwards or relays the request to a DHCP server.
<b>Default</b>	If the <b>prefix</b> statement is not explicitly specified, no prefix is prepended to the circuit ID.
<b>Options</b>	<p><b>host-name</b>—Add router host name to DHCP option 82 circuit ID.</p> <p><b>logical-system-name</b>—Add logical system name to DHCP option 82 circuit ID.</p> <p>This option is not used for the <b>prefix</b> statement at any of the above hierarchy levels.</p> <p><b>routing-instance-name</b>—Add routing instance name to DHCP option 82 circuit ID.</p> <p>This option is not used for the <b>prefix</b> statement occurring at the following hierarchy levels:</p> <ul style="list-style-type: none"> <li>• [edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82<b>circuit-id</b>]</li> <li>• Any of the hierarchy levels for the platforms without ELS</li> </ul>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

**Related  
Documentation**

- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- [Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101](#)
- [Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 156](#)
- [Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 153](#)
- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>

## prefix (Remote ID for Option 82)

<b>Syntax</b>	prefix (hostname   mac   none);
<b>Hierarchy Level</b>	<p>[edit <b>ethernet-switching-options secure-access-port vlan</b> (all   <i>vlan-name</i>) <b>dhcp-option82 remote-id</b>]</p> <p>[edit forwarding-options helpers bootp <b>dhcp-option82 remote-id</b>]</p> <p>[edit forwarding-options helpers bootp interface <i>interface-name</i> <b>dhcp-option82 remote-id</b>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p>
<b>Description</b>	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.
<b>Default</b>	If <b>prefix</b> is not explicitly specified, no prefix is appended to the remote ID.
<b>Options</b>	<p><b>hostname</b>—Name of the host system (the switch) that is forwarding or relaying the DHCP request from the DHCP client to the DHCP server.</p> <p><b>mac</b>—MAC address of the host system (the switch) that is forwarding or relaying the DHCP request from the DHCP client to the DHCP server.</p> <p><b>none</b>—No prefix is applied to the remote ID.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101</a></li> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 156</a></li> <li>• <a href="#">Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 153</a></li> <li>• <a href="#">[edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches on page 168</a></li> <li>• RFC 3046, <i>DHCP Relay Agent Information Option</i>, at <a href="http://tools.ietf.org/html/rfc3046">http://tools.ietf.org/html/rfc3046</a>.</li> </ul>

## remote-id

<b>Syntax</b>	<pre>remote-id {     host-name <i>host-name</i>;     mac;     prefix ( hostname   mac   none );     use-interface-description ( logical   device );     use-string <i>string</i>; }</pre>
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with Enhanced Level 2 Software (ELS): [edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82]</li> <li>For platforms without ELS: [edit ethernet-switching-options secure-access-port <i>vlan</i> (all   <i>vlan-name</i>) dhcp-option82], [edit forwarding-options helpers bootp dhcp-option82], [edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82]</li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p>
<b>Description</b>	<p>Insert the <b>remote-id</b> 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.</p> <p>The remaining statements are explained separately, and their availability depends on the hierarchy level at which the <b>remote-id</b> suboption is specified, as follows:</p> <ul style="list-style-type: none"> <li>The statement <b>prefix</b>, is <i>not</i> supported at the [edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82] hierarchy level.</li> <li>The statement <b>host-name</b> is supported <i>only</i> at the [edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82] hierarchy level.</li> </ul>
<b>Default</b>	<p>If the <b>remote-id</b> statement is not explicitly set, no remote ID value is inserted in the DHCP request packet header.</p> <p>If the <b>remote-id</b> statement is explicitly set, but is not qualified by a keyword, the following are true:</p> <ul style="list-style-type: none"> <li>At the [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] hierarchy level, the default keyword value is <i>interface-name</i>.</li> <li>At all other hierarchy levels, the default value of the <b>remote-id</b> keyword is the MAC address of the switch.</li> </ul>



<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101</a></li> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 156</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)</a></li> <li>• <a href="#">Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 153</a></li> <li>• RFC 3046, <i>DHCP Relay Agent Information Option</i>, at <a href="http://tools.ietf.org/html/rfc3046">http://tools.ietf.org/html/rfc3046</a></li> </ul>

## replay-protect

<b>Syntax</b>	<pre>replay-protect {     replay-window-size number-of-packets; }</pre>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Enable replay protection for MACsec.</p> <p>A replay window size specified using the <a href="#">replay-window-size number-of-packets</a> statement must be specified to enable replay protection.</p>
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## replay-window-size

---

<b>Syntax</b>	<code>replay-window-size <i>number-of-packets</i>;</code>
<b>Hierarchy Level</b>	[edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> replay-protect]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies the size of the replay protection window.</p> <p>This statement has to be configured to enable replay protection.</p> <p>When MACsec is enabled on an Ethernet link, an ID number is assigned to each packet entering the link. The ID number of the packet is checked by the receiving interface after the packet has traversed the MACsec-enabled link.</p> <p>When replay protection is enabled, the sequence of the ID number of received packets are checked. If the packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.</p> <p>Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.</p> <p>Replay protection should not be enabled in cases where packets are expected to arrive out of order.</p>
<b>Default</b>	Replay protection is disabled.
<b>Options</b>	<p><i>number-of-packets</i>—Specifies the size of the replay protection window, in packets.</p> <p>When this variable is set to 0, all packets that arrive out-of-order are dropped.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>

## secure-access-port

```
Syntax  secure-access-port {
        dhcp-snooping-file {
            location local_pathname | remote_URL;
            timeout seconds;
            write-interval seconds;
        }
        dhcpv6-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 (drop | log | none | shutdown);
            no-allowed-mac-log;
            persistent-learning;
            static-ipip-address {
                vlan vlan-name;
                mac mac-address;
            }
            static-ipv6ip-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-dhcpv6 | no-examine-dhcpv6) {
                forwarding-class class-name;
            }
        }
    }
```

```
    examine-fip {  
        fc-map fc-map-value;  
    }  
    (ip-source-guard | no-ip-source-guard);  
    (ipv6-source-guard | no-ipv6-source-guard);  
    mac-move-limit limit action (drop | log | none | shutdown);  
    }  
    (neighbor-discovery-inspection | no-neighbor-discovery-inspection);  
    no-option37;  
    }  
}
```

**Hierarchy Level** [edit [ethernet-switching-options](#)]

**Release Information** Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Support for IPv6 introduced in Junos OS Release 14.1X53-D10 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 page 43](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
- [Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 87](#)
- [Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101](#)
- [Example: Configuring an FCoE Transit Switch](#)

## secure-channel

<b>Syntax</b>	<pre>secure-channel <i>secure-channel-name</i> {   <i>direction</i> (inbound   outbound);   encryption;   id {     <i>mac-address</i> <i>mac-address</i>;     <i>port-id</i> <i>port-id-number</i>;   }   <i>offset</i> (0 30 50);   <i>security-association</i> <i>security-association-number</i> {     <i>key</i> <i>key-string</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit security <i>macsec</i> <i>connectivity-association</i> <i>connectivity-association-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Create and configure a secure channel to enable and configure MACsec when MACsec is enabled using static secure association key (SAK) security mode.</p> <p>You do not need to use this option to enable MACsec using static connectivity association key (CAK) security mode. All configuration for MACsec using static CAK security mode is done inside of the connectivity association but outside of the secure channel. When MACsec is enabled using static CAK security mode, an inbound and an outbound secure channel—neither of which is user-configurable—is automatically created within the connectivity association.</p>
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## security-association


---

<b>Syntax</b>	<code>security-association <i>security-association-number</i> {     key <i>key-string</i>; }</code>
<b>Hierarchy Level</b>	[edit security <i>macsec connectivity-association connectivity-association-name secure-channel secure-channel-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies the number of one of the security associations in the secure channel when MACsec is enabled using static secure association key (SAK) security mode. Because SAKs are created by the key server when MACsec is enabled using static connectivity association key (CAK) security mode, the <b>security-association</b> statement is not used when enabling MACsec using static CAK security mode.</p> <p>You must configure at least two security associations to enable MACsec using static SAK security mode. MACsec initially establishes a secure connection when a security association number and key match on both ends of an Ethernet link. After a certain number of Ethernet frames are securely transmitted across the Ethernet link, MACsec automatically rotates to a new security association with a new security association number and key to maintain the secured Ethernet link. This rotation continues each time a certain number of Ethernet frames are securely transmitted across the secured Ethernet link, so you must always configure MACsec to have at least two security associations.</p>
<b>Default</b>	No security keys are configured, by default.
<b>Options</b>	<p><b><i>security-association-number</i></b>—Specifies the security association number and creates the SAK.</p> <p>The security association number is a whole number between 0 and 3. You can configure two security associations in a secure channel when enabling MACsec using static security keys.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>

## security-mode

<b>Syntax</b>	<code>security-mode <i>security-mode</i>;</code>
<b>Hierarchy Level</b>	[edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15. The <b>dynamic</b> security mode option was introduced in Junos OS Release 14.1X53-D10. Statement introduced in Junos OS Release 14.1X53-D15 for the QFX Series.
<b>Description</b>	Configure the MACsec security mode for the connectivity association.  We recommend enabling MACsec on switch-to-switch Ethernet links using static connectivity association key (CAK) security mode. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available when you enable MACsec using static CAK security mode.
<b>Options</b>	<p><b>security-mode</b>—Specifies the MACsec security mode. Options include:</p> <ul style="list-style-type: none"> <li>• <b>dynamic</b>—Dynamic mode.  Dynamic security mode is used to enable MACsec on switch-to-host Ethernet links. In dynamic mode, a master key is retrieved from a RADIUS server by a switch and a host as part of the AAA handshake in separate transactions. The MKA protocol is enabled when the master key is exchanged between the switch and the host.</li> <li>• <b>static-cak</b>—Static connectivity association key (CAK) mode.  Static CAK security mode is used to enable MACsec on switch-to-switch Ethernet links. In <b>static-cak</b> mode, the switch at one end of the point-to-point link acts as the key server and regularly transmits a randomized key using a process that does not transmit any traffic outside of the MACsec-secured point-to-point link.</li> <li>• <b>static-sak</b>—Static secure association key (SAK) mode.  Static SAK security mode is used to enable MACsec on switch-to-switch Ethernet links. In <b>static-sak</b> mode, one of two user-configured security keys is used to secure the point-to-point link. The two security keys are regularly rotated.</li> </ul>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li> </ul>

## static-ip

<b>Syntax</b>	<pre>static-ip ip-addresses {     vlan vlan-name;     mac mac-address; }</pre>
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with ELS:            [edit vlans <i>vlan-name</i> forwarding-options dhcp-security group <i>group-name</i> interface <i>interface-name</i>]         </li> <li>For platforms without ELS:            [edit ethernet-switching-options secure-access-port interface (all   <i>interface-name</i>)]         </li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p>
<b>Description</b>	Configure a static IP address to MAC address (IP-MAC) binding to be added to the DHCP snooping database.
<div style="display: flex; align-items: center;">  <div> <p><b>NOTE:</b> The VLAN is specified at the higher hierarchy level when <code>static-ip</code> is configured at [edit vlans <i>vlan-name</i> forwarding-options dhcp-security group <i>group-name</i> interface <i>interface-name</i>].</p> </div> </div>	
<b>Options</b>	<p><b><i>ip-address</i></b>—Static IP address assigned to a device connected on the specified interface.</p> <p><b><i>mac mac-address</i></b>—Static MAC address assigned to a device connected on the specified interface.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 152</a></li> <li><a href="#">Configuring Static IP Addresses for DHCP and DHCPv6 Bindings on Access Ports (CLI Procedure)</a></li> </ul>



## timeout

---

<b>Syntax</b>	<code>timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[ <a href="#">edit ethernet-switching-options secure-access-port dhcp-snooping-file</a> ]; [ <a href="#">edit ethernet-switching-options secure-access-port dhcpv6-snooping-file</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4 for EX Series switches. Support at the [ <a href="#">edit ethernet-switching-options secure-access-port dhcpv6-snooping-file</a> ] hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
<b>Description</b>	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 the remote FTP site.
<b>Default</b>	None
<b>Options</b>	<i>seconds</i> —Value in seconds. <b>Range:</b> 10 through 3600.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 161</a></li> <li>• <a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li> </ul>

## traceoptions (Access Port Security)

---

Syntax	<pre>traceoptions {     file (<i>file-name</i>   files <i>files</i>   match <i>match</i>   no-world-readable   size <i>size</i>   world-readable);     flag ( all   async   chassis-scheduler   cos-adjustment   dynamic   hardware-database           init   parse   performance-monitor   process   restart   route-socket   show   snmp   util);     no-remote-trace; }</pre>
Hierarchy Level	[edit <a href="#">ethernet-switching-options</a> ], [edit class-of-service]
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 <b>traceoptions</b> feature is disabled by default.
Options	<p><b>disable</b>—(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 <b>all</b>.</p> <p><b>file <i>filename</i></b>—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 <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and so on, until the maximum number of trace files is reached (<b>xk</b> to specify KB, <b>xm</b> to specify MB, or <b>xg</b> 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"><li>• <b>access-security</b>—Trace access security events.</li><li>• <b>all</b>—All tracing operations.</li><li>• <b>config-internals</b>—Trace internal configuration operations.</li><li>• <b>forwarding-database</b>—Trace forwarding database and next-hop events.</li><li>• <b>general</b>—Trace general events.</li><li>• <b>interface</b>—Trace interface events.</li><li>• <b>ip-source-guard</b>—Trace IP source guard events.</li><li>• <b>krt</b>—Trace communications over routing sockets.</li><li>• <b>lib</b>—Trace library calls.</li></ul>

- **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:** **xk** to specify KB, **xm** to specify MB, or **xg** to specify gigabytes

**Range:** 10 KB through 1 gigabyte

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**no-remote-trace**—(Optional) Disable remote tracing.

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

<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Understanding Port Security on page 7</a></li> <li>• <a href="#">EX Series Switches Interfaces Overview</a></li> <li>• <a href="#">Understanding IP Source Guard for Port Security on EX Series Switches on page 32</a></li> <li>• <a href="#">Understanding Redundant Trunk Links</a></li> <li>• <a href="#">Understanding STP for EX Series Switches</a></li> <li>• <a href="#">Understanding Bridging and VLANs on EX Series Switches</a></li> </ul>
------------------------------	--

## transmit-interval (MACsec)

---

<b>Syntax</b>	transmit-interval <i>interval</i> ;
<b>Hierarchy Level</b>	[edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> mka]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
<b>Description</b>	<p>Specifies the transmit interval for MACsec Key Agreement (MKA) protocol data units (PDUs).</p> <p>The MKA transmit interval setting sets the frequency for how often the MKA PDU is sent to the directly connected device to maintain MACsec on a point-to-point Ethernet link. A lower <i>interval</i> increases bandwidth overhead on the link; a higher <i>interval</i> optimizes the MKA protocol data unit exchange process.</p> <p>The transmit interval settings must be identical on both ends of the link when MACsec using static connectivity association key (CAK) security mode is enabled.</p> <p>We recommend increasing the interval to 6000 ms in high-traffic load environments.</p>
<b>Default</b>	The default transmit interval is 2000 milliseconds.
<b>Options</b>	<i>interval</i> —Specifies the transmit interval, in milliseconds.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 116</a></li></ul>

## use-interface-description

<b>Syntax</b>	<code>use-interface-description (device   logical);</code>
<b>For Platforms with Enhanced Layer 2 Software (ELS)</b>	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 <a href="#">circuit-id</a>]</code>
<b>For Platforms Without ELS</b>	<code>[edit <a href="#">ethernet-switching-options secure-access-port vlan</a> (all   <i>vlan-name</i>) <a href="#">dhcp-option82 circuit-id</a>],</code> <code>[edit forwarding-options helpers bootp <a href="#">dhcp-option82 circuit-id</a>],</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> <a href="#">dhcp-option82 circuit-id</a>],</code> <code>[edit <a href="#">ethernet-switching-options secure-access-port vlan</a> (all   <i>vlan-name</i>) <a href="#">dhcp-option82 remote-id</a>],</code> <code>[edit forwarding-options helpers bootp <a href="#">dhcp-option82 remote-id</a>],</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> <a href="#">dhcp-option82 remote-id</a>]</code>
<b>For MX Series Platforms</b>	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82<a href="#">circuit-id</a>]</code>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Hierarchy level <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Hierarchy level <code>[edit bridge-domains <i>bridge domain name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.</p>
<b>Description</b>	Use the interface description rather than the interface name (which is the default value) in the circuit ID or remote ID value in the DHCP option 82 information.
<b>Options</b>	<p><b>device</b>—Use the device interface description. Only available for MX Series platform configuration.</p> <p><b>logical</b>—Use the logical interface description. Only available for MX Series platform configuration.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101</a></li> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 156</a></li> <li>• <a href="#">Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 153</a></li> </ul>

- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>

## use-string

<b>Syntax</b>	<code>use-string <i>string</i>;</code>
<b>For Platforms with Enhanced Layer 2 Software (ELS)</b>	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 <a href="#">remote-id</a>]</code>
<b>For Platforms Without ELS</b>	<code>[edit <a href="#">ethernet-switching-options secure-access-port vlan</a> (all   <i>vlan-name</i>) <a href="#">dhcp-option82 remote-id</a>],</code> <code>[edit forwarding-options helpers bootp <a href="#">dhcp-option82 remote-id</a>],</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> <a href="#">dhcp-option82 remote-id</a>]</code>
<b>For MX Series Platforms</b>	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82 <a href="#">circuit-id</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Hierarchy level <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.) Hierarchy level <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.
<b>Description</b>	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.
<b>Options</b>	<b><i>string</i></b> —Character string used as the remote ID value.  <b>Range:</b> 1–255 characters
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)</a></li> <li>• <a href="#">Understanding DHCP Option 82 for Port Security on Switching Devices on page 35</a></li> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101</a></li> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 156</a></li> <li>• <a href="#">Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 153</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)</a></li> </ul>

- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>

## use-vlan-id

<b>Syntax</b>	use-vlan-id;
<b>For Platforms with Enhanced Layer 2 Software (ELS)</b>	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 <a href="#">circuit-id</a> ]
<b>For Platforms Without ELS</b>	[edit forwarding-options helpers bootp dhcp-option82-circuit-id], [edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82-circuit-id]
<b>For MX Series Platforms</b>	[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82 <a href="#">circuit-id</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.) Hierarchy level [edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 14.1 for the MX Series.
<b>Description</b>	Use the VLAN ID rather than the VLAN name (the default) in the circuit ID value in the DHCP option 82 information.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)</a></li> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101</a></li> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 156</a></li> <li>• <a href="#">Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 153</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)</a></li> <li>• RFC 3046, <i>DHCP Relay Agent Information Option</i>, at <a href="http://tools.ietf.org/html/rfc3046">http://tools.ietf.org/html/rfc3046</a></li> </ul>



## vendor-id

<b>Syntax</b>	<code>vendor-id &lt;string&gt;;</code>
<b>For Platforms with Enhanced Layer 2 Software (ELS)</b>	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82]</code>
<b>For Platforms Without ELS</b>	<code>[edit ethernet-switching-options secure-access-port <i>vlan</i> (all   <i>vlan-name</i>) dhcp-option82],</code> <code>[edit forwarding-options helpers bootp dhcp-option82],</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82]</code>
<b>For MX Series Platforms</b>	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Hierarchy level <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.) Hierarchy level <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.
<b>Description</b>	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.
<b>Default</b>	If <b>vendor-id</b> is not explicitly configured for DHCP option 82, then no vendor ID is set.
<b>Options</b>	<b>string</b> —(Optional) A single string that designates the vendor ID.  <b>Range:</b> 1–255 characters  <b>Default:</b> If you specify <b>vendor-id</b> with no <b>string</b> value, then the default vendor ID <b>Juniper Networks</b> is configured.
<b>Required Privilege Level</b>	<b>system</b> —To view this statement in the configuration. <b>system-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)</a></li> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101</a></li> <li>• <a href="#">Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 98</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 156</a></li> <li>• <a href="#">Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)</a></li> </ul>

- [Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server \(CLI Procedure\)](#) on page 153

## vlan (Access Port Security)

```
Syntax  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-dhcpv6 | no-examine-dhcpv6) {
        forwarding-class class-name;
    }
    examine-fip {
        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    (ipv6-source-guard | no-ipv6-source-guard);
    mac-move-limit limit action (drop | log | none | shutdown);
    }
    (neighbor-discovery-inspection | no-neighbor-discovery-inspection);
    no-option37;
}
```

**Hierarchy Level** [edit [ethernet-switching-options secure-access-port](#)]

**Release Information** Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for the **examine-dhcpv6**, **no-option37**, **neighbor-discovery-inspection**, and **ipv6-source-guard** statements introduced in Junos OS Release 14.1x53-D10 for EX Series switches.

**Description** Apply any of the following security options to a VLAN:

- DHCP snooping
- DHCPv6 snooping with DHCP option 37
- DHCP option 82
- Dynamic ARP inspection (DAI)
- IPv6 neighbor discovery inspection

- FIP snooping
- IP source guard
- IPv6 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.

<b>Options</b>	<b>all</b> —Apply the feature to all VLANs.
	<b>vlan-name</b> —Apply the feature to the specified VLAN.
<b>Required Privilege Level</b>	system—To view this statement in the configuration.
	system-control—To add this statement to the configuration.
<b>Related Documentation</b>	• <a href="#">Example: Configuring Basic Port Security Features on page 43</a>
	• <a href="#">Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 77</a>
	• <a href="#">Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 101</a>
	• <a href="#">Example: Configuring an FCoE Transit Switch</a>

---

## vlan (DHCP Bindings on Access Ports)

---

<b>Syntax</b>	<code>vlan <i>vlan-name</i>;</code>
<b>Hierarchy Level</b>	[edit <code>ethernet-switching-options secure-access-port interface (all   <i>interface-name</i>) static-ip <i>ip-address</i></code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2 for EX Series switches.
<b>Description</b>	Associate the static IP address with the specified VLAN associated with the specified interface.
<b>Options</b>	<i>vlan-name</i> —Name of a specific VLAN associated with the specified interface.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 152</a></li></ul>

## write-interval

<b>Syntax</b>	<code>write-interval seconds;</code>
<b>For Platforms with Enhanced Layer 2 Software (ELS)</b>	(See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS) [edit system processes dhcp-service dhcp-snooping-file], [edit system processes dhcp-service dhcpv6-snooping-file]
<b>For Platforms Without ELS</b>	[edit <a href="#">ethernet-switching-options secure-access-port dhcp-snooping-file</a> ]; [edit <a href="#">ethernet-switching-options secure-access-port dhcpv6-snooping-file</a> ]
<b>For MX Series Platforms</b>	[edit system processes dhcp-service dhcp-snooping-file]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4 for EX Series switches. Support at the [edit system processes dhcp-service dhcp-snooping-file] hierarchy level introduced in Junos OS Release 13.2X50-D10. Support at the [edit system processes dhcp-service dhcpv6-snooping-file] hierarchy level introduced in Junos OS Release 13.2X51-D20. Statement introduced in Junos OS Release 14.1 for the MX Series. Support at the [edit ethernet-switching-options secure-access-port dhcpv6-snooping-file] hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
<b>Description</b>	Specify how frequently the device writes the database entries from memory into the DHCP snooping database file. <ul style="list-style-type: none"> <li>If you are configuring <b>write-interval</b> at the [edit ethernet-switching-options secure-access-port dhcp-snooping-file] or the [edit ethernet-switching-options secure-access-port dhcpv6-snooping-file] hierarchy level, see <a href="#">“Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure)”</a> on page 161.</li> <li>If you are configuring <b>write-interval</b> at the [edit system processes dhcp-service dhcp-snooping-file] or the [edit system processes dhcp-service dhcpv6-snooping-file] hierarchy level, see <i>Configuring Persistent Bindings in the DHCP or DHCPv6 Snooping Database to Improve Performance (CLI Procedure)</i>.</li> </ul>
<b>Options</b>	<b>seconds</b> —Value in seconds. <b>Range:</b> 60 through 86,400 seconds.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li> </ul>

## PART 3

# Administration

- [Routine Monitoring on page 253](#)
- [Operational Commands on page 267](#)





## CHAPTER 6

# Routine Monitoring

- [Monitoring Port Security on page 253](#)
- [Verifying That DHCP Snooping Is Working Correctly on page 255](#)
- [Verifying That a Trusted DHCP Server Is Working Correctly on page 256](#)
- [Verifying That DAI Is Working Correctly on page 256](#)
- [Verifying That MAC Limiting Is Working Correctly on page 257](#)
- [Verifying That MAC Move Limiting Is Working Correctly on page 262](#)
- [Verifying That IP Source Guard Is Working Correctly on page 263](#)
- [Verifying That the Port Error Disable Setting Is Working Correctly on page 263](#)
- [Verifying That Persistent MAC Learning Is Working Correctly on page 264](#)

## Monitoring Port Security

---

### Purpose



**NOTE:** This topic applies only to the J-Web Application package.

Use the monitoring functionality to view these port security details:

- DHCP snooping database for a VLAN or all VLANs
- ARP inspection details for all interfaces

### Action

To monitor port security in the J-Web interface, select **Monitor > Security > Port Security**.

To monitor and manipulate the DHCP snooping database and ARP inspection statistics in the CLI, enter the following commands:

- **show dhcp snooping binding**
- **clear dhcp snooping binding**—In addition to clearing the whole database, you can clear database entries for specified VLANs or MAC addresses.
- **show arp inspection statistics**
- **clear arp inspection statistics**



**NOTE:** On EX4300 switches, to monitor and manipulate the DHCP snooping database and ARP inspection statistics in the CLI, enter the following commands:

- **show dhcp-security binding**
- **clear dhcp-security binding**—In addition to clearing the whole database, you can clear database entries for specified VLANs or IP Address.
- **show dhcp-security arp inspection statistics**
- **clear arp inspection statistics**

**Meaning** The J-Web Port Security Monitoring page comprises two sections:

- **DHCP Snooping Details**—Displays the DHCP snooping database for all the VLANs for which DHCP snooping is enabled. To view the DHCP snooping database for a specific VLAN, select the specific VLAN from the list.
- **ARP Inspection Details**—Displays the ARP inspection details for all interfaces. The information includes details of the number of packets that passed ARP inspection and the number of packets that failed the inspection. The pie chart graphically represents these statistics when you select an interface. To view ARP inspection statistics for a specific interface, select the interface from the list.

You can use the following options on the page to clear DHCP snooping and ARP inspection details:

- **Clear All**—Clears the DHCP snooping database, either for all VLANs if the option **ALL** has been selected in the Select VLANs list or for the specific VLAN that has been selected in that list.
- **Clear**—Deletes a specific IP address from the DHCP snooping database.

To clear ARP inspection details on the page, click **Clear All** in the ARP inspection details section.



**NOTE:** Clear All button in the ARP inspection details section is not supported on EX4300 switches.

Use the CLI commands to show and clear DHCP snooping database and ARP inspection statistics details.

**Related Documentation**

- [Configuring Port Security \(CLI Procedure\) on page 110](#)
- [Configuring Port Security \(J-Web Procedure\) on page 112](#)
- [Example: Configuring Basic Port Security Features on page 43](#)

## 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 132](#)
  - [Enabling DHCP Snooping \(J-Web Procedure\) on page 135](#)
  - [Configuring Static IP Addresses for DHCP Bindings on Access Ports \(CLI Procedure\) on page 152](#)
  - [Example: Configuring Basic Port Security Features on page 43](#)
  - [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
  - [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61](#)
  - [Monitoring Port Security on page 253](#)
  - [Troubleshooting Port Security on page 307](#)

## 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 136](#)
  - [Enabling a Trusted Port for DHCP](#)
  - [Enabling a Trusted DHCP Server \(J-Web Procedure\) on page 136](#)
  - [Example: Configuring Basic Port Security Features on page 43](#)
  - [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 54](#)
  - [Monitoring Port Security on page 253](#)
  - [Troubleshooting Port Security on page 307](#)

## 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 137](#)
- [Enabling Dynamic ARP Inspection \(J-Web Procedure\) on page 139](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 69](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 61](#)
- [Monitoring Port Security on page 253](#)

## Verifying That MAC Limiting Is Working Correctly

MAC limiting protects against flooding of the Ethernet switching table.

Junos OS provides two methods for MAC limiting for port security:

- Maximum number of dynamic MAC addresses allowed—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.

Junos OS also allows you to set a MAC limit on VLANs. However, setting a MAC limit on VLANs is not considered a port security feature, because the switch does not prevent

incoming packets that cause the MAC limit to be exceeded from being forwarded; it only logs the MAC addresses of these packets..

To verify MAC limiting configurations:

1. [Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly on page 258](#)
2. [Verifying That MAC Limiting for a Specific Interface Within a Specific VLAN Is Working Correctly on page 258](#)
3. [Verifying That Allowed MAC Addresses Are Working Correctly on page 259](#)
4. [Verifying Results of Various Action Settings When the MAC Limit Is Exceeded on page 259](#)
5. [Customizing the Ethernet Switching Table Display to View Information for a Specific Interface on page 261](#)

## 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 default 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 MAC Limiting for a Specific Interface Within a Specific VLAN Is Working Correctly

**Purpose** Verify that MAC limiting for a specific interface based on its membership within a specific VLAN is working on the switch.

**Action** Display the detailed statistics for MAC addresses that have been learned:

```
user@switch> show ethernet-switching statistics mac-learning interface ge-0/0/28 detail
```

```
Interface: ge-0/0/28.0
Learning message from local packets: 0
Learning message from transit packets: 5
Learning message with error: 0
Invalid VLAN: 0 Invalid MAC: 0
Security violation: 0 Interface down: 0
Incorrect membership: 0 Interface limit: 0
MAC move limit: 0 VLAN limit: 0
VLAN membership limit: 20
Invalid VLAN index: 0 Interface not learning: 0
No nexthop: 0 MAC learning disabled: 0
Others: 0
```

**Meaning** The **VLAN membership limit** shows the number of packets that were dropped because of the VLAN membership MAC limit for interface ge-0/0/28.0 was exceeded. In this case, 20 packets were dropped.

## Verifying That Allowed MAC Addresses Are Working Correctly

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

**Action** Display the MAC address cache information after allowed MAC addresses have been configured on an interface. The following sample shows the MAC address cache after 5 allowed MAC addresses were on interface ge-0/0/2. In this instance, the interface was also set to a dynamic MAC limit of 4 with the default 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 was set to 4, only four of the five configured allowed addresses were learned and thus added to the MAC address 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**, **shutdown** and **none**—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 148.

**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 already existing error conditions. It impacts only error conditions that are detected after **port-error-disable** has been enabled and committed. To clear an already 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 about the MAC addresses learned on a specific interface.

**Action** For example, to display the MAC addresses 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 was set to 1, and the output shows that only one MAC address was learned and thus added to the MAC address 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 140](#)
  - [Configuring MAC Limiting \(J-Web Procedure\) on page 143](#)
  - [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 159](#)
  - [Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 66](#)
  - [Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 51](#)
  - [Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 58](#)
  - [Monitoring Port Security on page 253](#)

---

## Verifying That MAC Move Limiting Is Working Correctly

---

- Purpose** Verify that MAC move limiting is working on the switch.
- Action** Display the MAC addresses in the Ethernet switching table when MAC move limiting has been configured for a VLAN. The following sample shows the results after two of the hosts on **ge-0/0/2** sent packets after the MAC addresses for those hosts had moved to other interfaces more than five times in 1 second. The VLAN, **employee-vlan**, was set to a MAC move limit of **5** with the action **drop**:
- ```
user@switch> show ethernet-switching table
```
- Ethernet-switching table: 7 entries, 4 learned
- | VLAN          | MAC address       | Type  | Age | Interfaces |
|---------------|-------------------|-------|-----|------------|
| employee-vlan | 00:05:85:3A:82:77 | Learn | 0   | ge-0/0/1.0 |
| employee-vlan | 00:05:85:3A:82:79 | Learn | 0   | ge-0/0/1.0 |
| employee-vlan | 00:05:85:3A:82:80 | Learn | 0   | ge-0/0/2.0 |
| employee-vlan | 00:05:85:3A:82:81 | Learn | 0   | ge-0/0/2.0 |
| employee-vlan | *                 | Flood | -   | ge-0/0/2.0 |
| employee-vlan | *                 | Flood | -   | ge-0/0/2.0 |
- Meaning** The last two lines of the sample output show that MAC addresses for two hosts on **ge-0/0/2** were not learned, because the hosts had been moved back and forth from the original interfaces more than five times in 1 second.
- Related Documentation**
- [Configuring MAC Move Limiting \(CLI Procedure\) on page 145](#)
  - [Configuring MAC Move Limiting \(J-Web Procedure\) on page 147](#)

- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 159](#)
- [Example: Configuring Basic Port Security Features on page 43](#)
- [Monitoring Port Security on page 253](#)

## 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 148](#)

## 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 because of 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 because of a MAC move limit error. The disabled interface is automatically restored to service when the [disable-timeout](#) expires.
- **Storm control in effect** —The interface is temporarily disabled because of a storm control error. The disabled interface is automatically restored to service when the [disable-timeout](#) expires.

**Related Documentation**

- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\)](#) on page 159

---

## Verifying That Persistent MAC Learning Is Working Correctly

---

**Purpose** Verify that persistent MAC learning, also known as sticky MAC, is working on the interface. Persistent MAC learning allows retention of dynamically learned MAC addresses on an interface across restarts of the switch (or if the interface goes down).

**Action** Display the MAC addresses that have been learned. The following sample output shows the results when persistent MAC learning is enabled on interface ge-0/0/42:

**show ethernet-switching table persistent-mac**

```
user@switch> show ethernet-switching table
Ethernet-switching table: 8 entries, 2 learned, 5 persistent entries
VLAN      MAC address      Type      Age Interfaces
default   *                Flood     - All-members
default   00:10:94:00:00:02 Persistent      0 ge-0/0/42.0
default   00:10:94:00:00:03 Persistent      0 ge-0/0/42.0
default   00:10:94:00:00:04 Persistent      0 ge-0/0/42.0
default   00:10:94:00:00:05 Persistent      0 ge-0/0/42.0
default   00:10:94:00:00:06 Persistent      0 ge-0/0/42.0
default   00:21:59:c8:0c:50 Learn          0 ae0.0
default   02:21:59:c8:0c:44 Learn          0 ae0.0
```

**Meaning** The sample output shows that learned MAC addresses are stored in the Ethernet switching table as persistent entries. If the switch is rebooted or the interface goes down and comes back up, these addresses will be restored to the table.

- Related Documentation**
- [Configuring Port Security \(CLI Procedure\) on page 110](#)
  - [Example: Configuring Basic Port Security Features on page 43](#)



## CHAPTER 7

# Operational Commands

- clear arp inspection statistics
- clear dhcp snooping binding
- clear dhcp snooping statistics
- clear dhcpv6 snooping binding
- clear dhcpv6 snooping statistics
- clear dot1x
- clear neighbor-discovery-inspection statistics
- clear security mka statistics
- show arp inspection statistics
- show dhcp snooping binding
- show dhcp snooping statistics
- show dhcpv6 snooping binding
- show dhcpv6 snooping statistics
- show ethernet-switching table
- show ip-source-guard
- show ipv6-source-guard
- show neighbor-discovery-inspection statistics
- show security macsec connections
- show security macsec statistics
- show security mka sessions
- show security mka statistics
- show system statistics arp

## clear arp inspection statistics

---

|                                 |                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear arp inspection statistics<br><interface <i>interface</i> >                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                                                             |
| <b>Description</b>              | Clear ARP inspection statistics.                                                                                                                                                                                                                                                  |
| <b>Options</b>                  | <b>none</b> —Clears ARP statistics on all interfaces.<br><br><b>interface <i>interface-names</i></b> —(Optional) Clear ARP statistics on one or more interfaces.                                                                                                                  |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show arp inspection statistics on page 277</a></li><li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li><li>• <a href="#">Verifying That DAI Is Working Correctly on page 256</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">clear arp inspection statistics on page 268</a>                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                  |

## Sample Output

### clear arp inspection statistics

```
user@switch> clear arp inspection statistics
```



## clear dhcp snooping binding

|                                 |                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcp snooping binding<br><mac (all   <i>mac-address</i> )><br><vlan (all   <i>vlan-name</i> )><br><vlan (all   <i>vlan-name</i> ) mac (all   <i>mac-address</i> )>                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                                                                       |
| <b>Description</b>              | Clear the DHCP snooping database information.                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>mac (all   <i>mac-address</i>)</b>—(Optional) Clear DHCP snooping information for the specified MAC address or all MAC addresses.</p> <p><b>vlan (all   <i>vlan-name</i>)</b>—(Optional) Clear DHCP snooping information for the specified VLAN or all VLANs.</p>                     |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dhcp snooping binding on page 278</a></li> <li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li> <li>• <a href="#">Verifying That DHCP Snooping Is Working Correctly on page 255</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">clear dhcp snooping binding on page 269</a>                                                                                                                                                                                                                                     |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                            |

## Sample Output

### clear dhcp snooping binding

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

## clear dhcp snooping statistics

---

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>clear dhcp snooping statistics</code>                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.4 for EX Series switches.                                                                                                                             |
| <b>Description</b>              | Clear all Dynamic Host Configuration Protocol (DHCP) snooping statistics.                                                                                                                      |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dhcp snooping statistics on page 280</a></li><li>• <a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">clear dhcp snooping statistics on page 270</a>                                                                                                                                     |
| <b>Output Fields</b>            | See <a href="#">show dhcp snooping statistics</a> 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
```

## clear dhcpv6 snooping binding

|                                 |                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcpv6 snooping binding<br><mac (all   <i>mac-address</i> )><br><vlan (all   <i>vlan-name</i> )><br><vlan (all   <i>vlan-name</i> ) mac (all   <i>mac-address</i> )>                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.                                                                                                                                                                                                                    |
| <b>Description</b>              | Clear the DHCPv6 snooping database information.                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>mac (all   <i>mac-address</i>)</b>—(Optional) Clear DHCPv6 snooping information for the specified MAC address or all MAC addresses.</p> <p><b>vlan (all   <i>vlan-name</i>)</b>—(Optional) Clear DHCPv6 snooping information for the specified VLAN or all VLANs.</p>                   |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dhcpv6 snooping binding on page 281</a></li> <li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li> <li>• <a href="#">Verifying That DHCP Snooping Is Working Correctly on page 255</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">clear dhcpv6 snooping binding on page 271</a>                                                                                                                                                                                                                                     |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                              |

### Sample Output

#### clear dhcpv6 snooping binding

```
user@switch> clear dhcpv6 snooping binding
```

## clear dhcpv6 snooping statistics

---

|                                 |                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>clear dhcpv6 snooping statistics</code>                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.                                                                                                                       |
| <b>Description</b>              | Clear all Dynamic Host Configuration Protocol for IPv6 (DHCPv6) snooping statistics.                                                                                                             |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dhcpv6 snooping statistics on page 283</a></li><li>• <a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">clear dhcpv6 snooping statistics on page 272</a>                                                                                                                                     |
| <b>Output Fields</b>            | See <a href="#">show dhcpv6 snooping statistics</a> for an explanation of the output fields.                                                                                                     |

## Sample Output

### clear dhcpv6 snooping statistics

The following sample output displays the DHCPv6 snooping statistics before and after the `clear dhcpv6 snooping statistics` command is issued.

```
user@switch> show dhcpv6 snooping statistics
Successful Transfers :      0   Failed Transfers :      21
Successful Reads    :      0   Failed Reads    :      0
Successful Writes   :      0   Failed Writes   :      21
```

```
user@switch> clear dhcpv6 snooping statistics
user@switch> show dhcpv6 snooping statistics
Successful Transfers :      0   Failed Transfers :      0
Successful Reads    :      0   Failed Reads    :      0
Successful Writes   :      0   Failed Writes   :      0
```

## clear dot1x

**Syntax** `clear dot1x (firewall <counter-name> | interface <[interface-name]> | mac-address [mac-addresses] | statistics <interface interface-name>)`

**Release Information** Command introduced in Junos OS Release 9.0 for EX Series switches.  
**firewall** option added in Junos OS Release 9.5 for EX Series switches.

**Description** Reset the authentication state of an interface or delete 802.1X statistics from the switch. When you reset an interface using the **interface** or **mac-address** options, reauthentication on the interface is also triggered. The switch sends out a multicast message on the interface to restart the authentication of all connected supplicants. If a MAC address is reset, then the switch sends out a unicast message to that specific MAC address to restart authentication.

If a supplicant is sending traffic when the **clear dot1x interface** command is issued, the authenticator immediately initiates reauthentication. This process happens quickly, and it might seem that reauthentication did not occur. To verify that reauthentication has happened, issue the **show dot1x interface detail** command. The values for **Reauthentication due** and **Reauthentication interval** will be about the same.



**CAUTION:** When you clear the learned MAC addresses from an interface using the **clear dot1x interface** command, all MAC addresses are cleared, including those in static MAC bypass list.

If you have enabled Media Access Control Security (MACsec) using static secure association key (SAK) security mode on an EX Series switch, the SAKs are rotated when the **clear dot1x** command is entered. The **clear dot1x** command has no impact on MACsec when MACsec is enabled using static connectivity association keys (CAK) or any other security mode.

**Options** **firewall <counter-name>**—Clear 802.1X firewall counter statistics. If the *counter-name* option is specified, clear 802.1X firewall statistics for that counter.

**interface <[interface-name]>**—Reset the authentication state of all the supplicants (also, clears all the authentication bypassed clients) connected to the specified interface (when the interface is an authenticator) or reset the authentication state for the interface itself (when the interface is a supplicant).

**mac-address [mac-addresses]**—Reset the authentication state of the specified MAC addresses.

**statistics <interface interface-name>**—Clear 802.1X statistics on all 802.1X-enabled interfaces. If the **interface** option is specified, clear 802.1X firewall statistics for that interface or interfaces.

**Required Privilege Level**    view

**Related Documentation**

- [show dot1x](#)
- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch](#)
- [Filtering 802.1X Supplicants Using RADIUS Server Attributes](#)

**List of Sample Output**

- [clear dot1x firewall c1 on page 274](#)
- [clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0 on page 274](#)
- [clear dot1x mac-address 00:04:ae:cd:23:5f on page 274](#)
- [clear dot1x statistics interface ge-1/0/1 on page 274](#)

## Sample Output

[clear dot1x firewall c1](#)

```
user@switch> clear dot1x firewall c1
```

[clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0](#)

```
user@switch> clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0
```

[clear dot1x mac-address 00:04:ae:cd:23:5f](#)

```
user@switch> clear dot1x mac-address 00:04:ae:cd:23:5f
```

[clear dot1x statistics interface ge-1/0/1](#)

```
user@switch> clear dot1x statistics interface ge-1/0/1
```

## clear neighbor-discovery-inspection statistics

---

|                                 |                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear neighbor-discovery-inspection statistics<br><interface <i>interface-name</i> >                                                                                                                               |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.                                                                                                                                         |
| <b>Description</b>              | Clear IPv6 neighbor discovery inspection statistics.                                                                                                                                                               |
| <b>Options</b>                  | <b>none</b> —Clear neighbor discovery inspection statistics on all interfaces.<br><br><b>interface <i>interface-name</i></b> —(Optional) Clear neighbor discovery inspection statistics on one or more interfaces. |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show neighbor-discovery-inspection statistics on page 293</a></li><li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">clear neighbor-discovery-inspection statistics on page 275</a>                                                                                                                                         |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                   |

### Sample Output

#### clear neighbor-discovery-inspection statistics

```
user@switch> clear neighbor-discovery-inspection statistics
```

## clear security mka statistics

---

|                                 |                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear security mka statistics<br><interface <i>interface-name</i> >                                                                                                                                                                                                   |
| <b>Release Information</b>      | Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                             |
| <b>Description</b>              | <p>Clear—reset to zero (0)—all MACsec Key Agreement (MKA) protocol statistics.</p> <p>You are clearing the statistics that are viewed using the <b>show security mka statistics</b> when you enter this command.</p>                                                  |
| <b>Options</b>                  | <p><b>none</b>—Clear all MKA counters for all interfaces on the switch.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Clear MKA traffic counters for the specified interface only.</p>                                                                     |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show security mka statistics on page 302</a></li><li>• <a href="#">show security mka sessions on page 300</a></li><li>• <a href="#">Understanding Media Access Control Security (MACsec) on page 26</a></li></ul> |

## Sample Output

### clear security mka statistics

```
user@switch> clear security mka statistics
```



## show arp inspection statistics

|                                 |                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show arp inspection statistics                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                                                                  |
| <b>Description</b>              | Display ARP inspection statistics.                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear arp inspection statistics on page 268</a></li> <li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li> <li>• <a href="#">Verifying That DAI Is Working Correctly on page 256</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show arp inspection statistics on page 277</a>                                                                                                                                                                                                                             |
| <b>Output Fields</b>            | <a href="#">Table 17 on page 277</a> lists the output fields for the <b>show arp inspection statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                                                            |

**Table 17: 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

|                                 |                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show dhcp snooping binding</b><br><b>&lt;interface <i>interface-name</i>&gt;</b><br><b>&lt;vlan <i>vlan-name</i>&gt;</b>                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                                                                        |
| <b>Description</b>              | Display the DHCP snooping database information.                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <b>interface <i>interface-name</i></b> —(Optional) Display the DHCP snooping database information for an interface.<br><br><b>vlan <i>vlan-name</i></b> —(Optional) Display the DHCP snooping database information for a VLAN.                                                               |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcp snooping binding on page 269</a></li> <li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li> <li>• <a href="#">Verifying That DHCP Snooping Is Working Correctly on page 255</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dhcp snooping binding on page 278</a>                                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | <a href="#">Table 18 on page 278</a> lists the output fields for the <b>show dhcp snooping binding</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                      |

Table 18: 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

|                                 |                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show dhcp snooping statistics</b>                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.4 for EX Series switches.                                                                                                                                 |
| <b>Description</b>              | Display statistics for read and write operations to the DHCP snooping database.                                                                                                                    |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcp snooping statistics on page 270</a></li> <li>• <a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dhcp snooping statistics on page 280</a>                                                                                                                                          |
| <b>Output Fields</b>            | Table 19 on page 280 lists the output fields for the <b>show dhcp snooping statistics</b> command. Output fields are listed in the approximate order in which they appear.                         |

Table 19: show dhcp snooping statistics Output Fields

| Field Name                  | Field Description                                                                          |
|-----------------------------|--------------------------------------------------------------------------------------------|
| <b>Successful Transfers</b> | Number of entries successfully transferred from memory to the DHCP snooping database.      |
| <b>Successful Reads</b>     | Number of entries successfully read from memory to the DHCP snooping database.             |
| <b>Successful Writes</b>    | Number of entries successfully written from memory to the DHCP snooping database.          |
| <b>Failed Transfers</b>     | Number of entries that failed being transferred from memory to the DHCP snooping database. |
| <b>Failed Reads</b>         | Number of entries that failed being read from memory to the DHCP snooping database.        |
| <b>Failed Writes</b>        | 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 dhcpv6 snooping binding

|                                 |                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show dhcpv6 snooping binding</code><br><code>&lt;interface <i>interface-name</i>&gt;</code><br><code>&lt;vlan <i>vlan-name</i>&gt;</code>                                                                                                                                              |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.                                                                                                                                                                                                                   |
| <b>Description</b>              | Display the DHCPv6 snooping database information.                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><code>interface <i>interface-name</i></code>—(Optional) Display the DHCPv6 snooping database information for an interface.</p> <p><code>vlan <i>vlan-name</i></code>—(Optional) Display the DHCPv6 snooping database information for a VLAN.</p>                                          |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcp snooping binding on page 269</a></li> <li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li> <li>• <a href="#">Verifying That DHCP Snooping Is Working Correctly on page 255</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dhcpv6 snooping binding on page 281</a>                                                                                                                                                                                                                                     |
| <b>Output Fields</b>            | Table 18 on page 278 lists the output fields for the <code>show dhcpv6 snooping binding</code> command. Output fields are listed in the approximate order in which they appear.                                                                                                              |

Table 20: 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 dhcpv6 snooping binding

```
user@switch> show dhcpv6 snooping binding
```

## DHCP Snooping Information:

| MAC address       | IP address            | Lease (seconds) | Type    | VLAN | Interface  |
|-------------------|-----------------------|-----------------|---------|------|------------|
| 00:10:94:00:00:01 | 3000::10:10:0:3       | 3599992         | dynamic | v1   | ge-0/0/0.0 |
| 00:10:94:00:00:01 | fe80::210:94ff:fe00:1 | 3599992         | dynamic | v1   | ge-0/0/0.0 |
| 00:10:94:00:00:02 | 3000::10:10:0:4       | 3599992         | dynamic | v1   | ge-0/0/0.0 |
| 00:10:94:00:00:02 | fe80::210:94ff:fe00:2 | 3599992         | dynamic | v1   | ge-0/0/0.0 |
| 00:10:94:00:00:03 | 3000::10:10:0:5       | 3599992         | dynamic | v1   | ge-0/0/0.0 |
| 00:10:94:00:00:03 | fe80::210:94ff:fe00:3 | 3599992         | dynamic | v1   | ge-0/0/0.0 |
| 00:10:94:00:00:04 | 3000::10:10:0:6       | 3599992         | dynamic | v1   | ge-0/0/0.0 |
| 00:10:94:00:00:04 | fe80::210:94ff:fe00:4 | 3599992         | dynamic | v1   | ge-0/0/0.0 |
| 00:10:94:00:00:05 | 3000::10:10:0:7       | 3599992         | dynamic | v1   | ge-0/0/0.0 |
| 00:10:94:00:00:05 | fe80::210:94ff:fe00:5 | 3599992         | dynamic | v1   | ge-0/0/0.0 |

## show dhcpv6 snooping statistics

|                                 |                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show dhcpv6 snooping statistics</b>                                                                                                                                                             |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.                                                                                                                         |
| <b>Description</b>              | Display statistics for read and write operations performed on the DHCPv6 snooping database.                                                                                                        |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcp snooping statistics on page 270</a></li> <li>• <a href="#">Understanding DHCP Snooping for Port Security on page 12</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dhcpv6 snooping statistics on page 283</a>                                                                                                                                        |
| <b>Output Fields</b>            | Table 19 on page 280 lists the output fields for the <b>show dhcpv6 snooping statistics</b> command. Output fields are listed in the approximate order in which they appear.                       |

Table 21: show dhcpv6 snooping statistics Output Fields

| Field Name                  | Field Description                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------|
| <b>Successful Transfers</b> | Number of entries successfully transferred from memory to the DHCPv6 snooping database.      |
| <b>Successful Reads</b>     | Number of entries successfully read from memory to the DHCPv6 snooping database.             |
| <b>Successful Writes</b>    | Number of entries successfully written from memory to the DHCPv6 snooping database.          |
| <b>Failed Transfers</b>     | Number of entries that failed being transferred from memory to the DHCPv6 snooping database. |
| <b>Failed Reads</b>         | Number of entries that failed being read from memory to the DHCPv6 snooping database.        |
| <b>Failed Writes</b>        | Number of entries that failed being written from memory to the DHCPv6 snooping database.     |

## Sample Output


### show dhcpv6 snooping statistics

```

user@switch> show dhcpv6 snooping statistics
DHCP Snoop Persistence statistics
Successful Remote Transfers: 0          Failed Remote Transfers: 0
Successful Record Reads   : 0          Failed Record Reads   : 0
Successful Record Writes  : 0          Failed Record Writes  : 0

```

## show ethernet-switching table

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show ethernet-switching table &lt;brief   detail   extensive   summary&gt; &lt;interface <i>interface-name</i>&gt; &lt;management-vlan&gt; &lt;persistent-mac &lt;interface <i>interface-name</i>&gt;&gt; &lt;sort-by (<i>name</i>   <i>tag</i>)&gt; &lt;vlan <i>vlan-name</i>&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Options <b>summary</b>, <b>management-vlan</b>, and <b>vlan <i>vlan-name</i></b> introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Option <b>sort-by</b> and field name <b>tag</b> introduced in Junos OS Release 10.1 for EX Series switches.</p> <p>Option <b>persistent-mac</b> introduced in Junos OS Release 11.4 for EX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | <p> <b>NOTE:</b> If your EX Series switch CLI displays different options for the <b>show ethernet-switching table</b> command than the options shown in this document, see <i>show ethernet-switching table</i>.</p> <p>Display the Ethernet switching table.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>none</b>—(Optional) Display brief information about the Ethernet switching table.</p> <p><b>brief   detail   extensive   summary</b>—(Optional) Display the specified level of output.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Display the Ethernet switching table for a specific interface.</p> <p><b>management-vlan</b>—(Optional) Display the Ethernet switching table for a management VLAN.</p> <p><b>persistent-mac &lt;interface <i>interface-name</i>&gt;</b>—(Optional) Display the persistent MAC addresses learned for all interfaces or a specified interface. You can use this command to view entries that you want to clear for an interface that you intentionally disabled.</p> <p><b>sort-by (<i>name</i>   <i>tag</i>)</b>—(Optional) Display VLANs in ascending order of VLAN IDs or VLAN names.</p> <p><b>vlan <i>vlan-name</i></b>—(Optional) Display the Ethernet switching table for a specific VLAN.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><i>clear ethernet-switching table</i></li> <li><i>Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



- *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 286](#)  
[show ethernet-switching table brief on page 286](#)  
[show ethernet-switching table detail on page 287](#)  
[show ethernet-switching table extensive on page 287](#)  
[show ethernet-switching table persistent-mac on page 288](#)  
[show ethernet-switching table persistent-mac interface ge-0/0/16.0 on page 288](#)

**Output Fields** [Table 22 on page 285](#) lists the output fields for the **show ethernet-switching table** command. Output fields are listed in the approximate order in which they appear.

**Table 22: show ethernet-switching table Output Fields**

| Field Name                | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                              | Level of Output                         |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| <b>VLAN</b>               | The name of a VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                                            | All levels                              |
| <b>Tag</b>                | The VLAN ID tag name or number.                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>extensive</b>                        |
| <b>MAC or MAC address</b> | The MAC address associated with the VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                      | All levels                              |
| <b>Type</b>               | The type of MAC address. Values are: <ul style="list-style-type: none"> <li>• <b>static</b>—The MAC address is manually created.</li> <li>• <b>learn</b>—The MAC address is learned dynamically from a packet's source MAC address.</li> <li>• <b>flood</b>—The MAC address is unknown and flooded to all members.</li> <li>• <b>persistent</b>—The learned MAC addresses that will persist across restarts of the switch or interface-down events.</li> </ul> | All levels except <b>persistent-mac</b> |
| <b>Type</b>               | The type of MAC address. Values are: <ul style="list-style-type: none"> <li>• <b>installed</b>—addresses that are in the Ethernet switching table.</li> <li>• <b>uninstalled</b>—addresses that could not be installed in the table or were uninstalled in an interface-down event and will be reinstalled in the table when the interface comes back up.</li> </ul>                                                                                           | <b>persistent-mac</b>                   |
| <b>Age</b>                | The time remaining before the entry ages out and is removed from the Ethernet switching table.                                                                                                                                                                                                                                                                                                                                                                 | All levels                              |
| <b>Interfaces</b>         | Interface associated with learned MAC addresses or <b>All-members</b> (flood entry).                                                                                                                                                                                                                                                                                                                                                                           | All levels                              |
| <b>Learned</b>            | For learned entries, the time which the entry was added to the Ethernet switching table.                                                                                                                                                                                                                                                                                                                                                                       | <b>detail, extensive</b>                |
| <b>Nexthop index</b>      | The next-hop index number.                                                                                                                                                                                                                                                                                                                                                                                                                                     | <b>detail, extensive</b>                |

Table 22: show ethernet-switching table Output Fields (*continued*)

| Field Name            | Field Description                                                                                                                                                                                                                                                                                 | Level of Output |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>persistent-mac</b> | <b>installed</b> indicates MAC addresses that are in the Ethernet switching table and <b>uninstalled</b> indicates MAC addresses that could not be installed in the table or were uninstalled in an interface-down event (and will be reinstalled in the table when the interface comes back up). |                 |

## Sample Output

### show ethernet-switching table

```

user@switch> show ethernet-switching table
Ethernet-switching table: 57 entries, 15 learned, 2 persistent
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 Persistent 0 ge-0/0/46.0
T1         00:00:5e:00:01:00 Static    - Router
T1         00:19:e2:50:63:e0 Persistent 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, 15 learned, 2 persistent entries
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 Persistent 0 ge-0/0/46.0
T1          00:00:5e:00:01:00 Static      - Router
T1          00:19:e2:50:63:e0 Persistent 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 entries
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, 5 persistent entries

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 persistent-mac

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

| VLAN    | MAC address       | Type        | Interface   |
|---------|-------------------|-------------|-------------|
| default | 00:10:94:00:00:02 | installed   | ge-0/0/42.0 |
| default | 00:10:94:00:00:03 | installed   | ge-0/0/42.0 |
| default | 00:10:94:00:00:04 | installed   | ge-0/0/42.0 |
| default | 00:10:94:00:00:05 | installed   | ge-0/0/42.0 |
| default | 00:10:94:00:00:06 | installed   | ge-0/0/42.0 |
| default | 00:10:94:00:05:02 | uninstalled | ge-0/0/16.0 |
| default | 00:10:94:00:06:03 | uninstalled | ge-0/0/16.0 |
| default | 00:10:94:00:07:04 | uninstalled | ge-0/0/16.0 |

#### show ethernet-switching table persistent-mac interface ge-0/0/16.0

| VLAN    | MAC address       | Type        | Interface   |
|---------|-------------------|-------------|-------------|
| default | 00:10:94:00:05:02 | uninstalled | ge-0/0/16.0 |
| default | 00:10:94:00:06:03 | uninstalled | ge-0/0/16.0 |
| default | 00:10:94:00:07:04 | uninstalled | ge-0/0/16.0 |

## show ip-source-guard

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show ip-source-guard</code>                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.2 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Display IP source guard database information.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 87</a></li> <li>• <a href="#">Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 77</a></li> <li>• <a href="#">Verifying That IP Source Guard Is Working Correctly on page 263</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show ip-source-guard on page 289</a>                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Output Fields</b>            | <a href="#">Table 23 on page 289</a> lists the output fields for the <b>show ip-source-guard</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                            |

**Table 23: show ip-source-guard Output Fields**

| Field Name         | Field Description                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VLAN</b>        | VLAN on which IP source guard is enabled.                                                                                                                                                                                                        |
| <b>Interface</b>   | Access interface associated with the VLAN in column 1.                                                                                                                                                                                           |
| <b>Tag</b>         | VLAN ID for the VLAN in column 1. Possible values are: <ul style="list-style-type: none"> <li>• 0, indicating the VLAN is not tagged.</li> <li>• 1 – 4093</li> </ul>                                                                             |
| <b>IP Address</b>  | 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.  |
| <b>MAC Address</b> | 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
```

## show ipv6-source-guard

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show ipv6-source-guard</b>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | (For non-ELS switches) Display IPv6 source guard database information.                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 87</a></li> <li>• <a href="#">Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 77</a></li> <li>• <a href="#">Verifying That IP Source Guard Is Working Correctly on page 263</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show ipv6-source-guard on page 291</a>                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Output Fields</b>            | Table 23 on page 289 lists the output fields for the <b>show ipv6-source-guard</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                          |

**Table 24: show ipv6-source-guard Output Fields**

| Field Name         | Field Description                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VLAN</b>        | VLAN on which IPv6 source guard is enabled.                                                                                                                                                                                               |
| <b>Interface</b>   | Access interface associated with the VLAN described in row 1.                                                                                                                                                                             |
| <b>Tag</b>         | VLAN ID for the VLAN described in row 1. Possible values are: <ul style="list-style-type: none"> <li>• 0, indicating the VLAN is not tagged.</li> <li>• 1 through 4093</li> </ul>                                                         |
| <b>IP Address</b>  | Source IP address for a device connected to the interface described in row 2. A * (asterisk) indicates that IPv6 source guard is not enabled on this VLAN, but the interface is shared with a VLAN that is enabled for IPv6 source guard. |
| <b>MAC Address</b> | Source MAC address for a device connected to the interface described in row 2. A * (asterisk) indicates that IPv6 source guard is not enabled on this VLAN but the interface is shared with a VLAN that is enabled for IPv6 source guard. |

## Sample Output

### show ipv6-source-guard

```

user@switch> show ipv6-source-guard
IP source guard information:
Interface    Tag    IP Address                MAC Address                VLAN
ge-0/0/6.0   0      2000::10:10:0:105        00:10:94:10:00:01        vlan1

```

|            |   |                       |                   |       |
|------------|---|-----------------------|-------------------|-------|
| ge-0/0/6.0 | 0 | fe80::210:94ff:fe10:1 | 00:10:94:10:00:01 | vlan1 |
| ge-0/0/7.0 | 0 | 2000::10:10:0:104     | 00:10:94:10:00:02 | vlan1 |
| ge-0/0/7.0 | 0 | fe80::210:94ff:fe10:2 | 00:10:94:10:00:02 | vlan1 |



## show neighbor-discovery-inspection statistics

|                                 |                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show neighbor-discovery-inspection statistics                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.                                                                                                                                                                                                             |
| <b>Description</b>              | Display neighbor discovery inspection statistics.                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear arp inspection statistics on page 268</a></li> <li>• <a href="#">Example: Configuring Basic Port Security Features on page 43</a></li> <li>• <a href="#">Verifying That DAI Is Working Correctly on page 256</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show neighbor-discovery-inspection statistics on page 293</a>                                                                                                                                                                                                              |
| <b>Output Fields</b>            | <a href="#">Table 17 on page 277</a> lists the output fields for the <b>show neighbor-discovery-inspection statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                                             |

**Table 25: show neighbor-discovery-inspection statistics Output Fields**

| Field Name           | Field Description                                                           | Level of Output |
|----------------------|-----------------------------------------------------------------------------|-----------------|
| Interface            | Interface on which neighbor discovery inspection has been applied.          | All levels      |
| Packets received     | Total number of packets total that underwent neighbor discovery inspection. | All levels      |
| ND inspection pass   | Total number of packets that passed neighbor discovery inspection.          | All levels      |
| ND inspection failed | Total number of packets that failed neighbor discovery inspection.          | All levels      |

## Sample Output

### show neighbor-discovery-inspection statistics

```

user@switch> show neighbor-discovery-inspection statistics
Interface    Packets received    ND inspection pass    ND inspection failed
ge-0/0/0      5                   1                     4
ge-0/0/1      0                   0                     0

```

## show security macsec connections

|                                 |                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show security macsec connections</code><br><code>&lt;interface <i>interface-name</i>&gt;</code>                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                              |
| <b>Description</b>              | Display the status of the active MACsec connections on the switch.                                                                                                                                                     |
| <b>Options</b>                  | <b>none</b> —Display MACsec connection information for all interfaces on the switch.<br><br><b>interface <i>interface-name</i></b> —(Optional) Display MACsec connection information for the specified interface only. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show security macsec statistics on page 296</a></li> </ul>                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show security macsec connections on page 295</a>                                                                                                                                                           |
| <b>Output Fields</b>            | <a href="#">Table 26 on page 294</a> lists the output fields for the <b>show security macsec connections</b> command. Output fields are listed in the approximate order in which they appear.                          |

Table 26: show security macsec connections Output Fields

| Field Name           | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fields for Interface |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Interface name       | Name of the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| CA name              | Name of the connectivity association.<br><br>A connectivity association is named using the <b>connectivity-association</b> statement when you are enabling MACsec.                                                                                                                                                                                                                                                                                     |
| Cipher suite         | Name of the cipher suite used for encryption.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Encryption           | Encryption setting. Encryption is enabled when this output is <b>on</b> and disabled when this output is <b>off</b> .<br><br>The encryption setting is set using the <b>no-encryption</b> statement in the connectivity association when using static connectivity association key (CAK) security mode and is set using the <b>encryption</b> statement in the secure channel when using static secure association key (SAK) or dynamic security mode. |
| Key server offset    | Offset setting.<br><br>The offset is set using the <b>offset</b> statement when configuring the connectivity association when using static connectivity association key (CAK) or dynamic security mode or the secure channel when using static secure association key (SAK) security mode.                                                                                                                                                             |

Table 26: show security macsec connections Output Fields (*continued*)

| Field Name            | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Include SCI</b>    | <p>SCI tagging. The SCI tag is included on packets in a secure channel when this output is <b>yes</b>, and not included on packets in a secure channel when this output is <b>no</b>.</p> <p>SCI tagging is automatically enabled on EX4300 switch interfaces that have enabled MACsec using static connectivity association key (CAK) or dynamic security mode. You can enable SCI tagging using the <b>include-sci</b> statement in the connectivity association.</p> |
| <b>Replay protect</b> | <p>Replay protection setting. Replay protection is enabled when this output is <b>on</b> and disabled when this output is <b>off</b>.</p> <p>You can enable replay protection using the <b>replay-protect</b> statement in the connectivity association.</p>                                                                                                                                                                                                            |
| <b>Replay window</b>  | <p>Replay protection window setting. This output is set to <b>0</b> when replay protection is disabled, and is the size of the replay window, in number of packets, when replay protection is enabled.</p> <p>The size of the replay window is configured using the <b>replay-window-size</b> statement in the connectivity association.</p>                                                                                                                            |

## Sample Output

### show security macsec connections

```

user@host> show security macsec connections
Interface name: xe-0/1/0
  CA name: CA1
  Cipher suite: GCM-AES-128   Encryption: on
  Key server offset: 0        Include SCI: no
  Replay protect: off         Replay window: 0

```

## show security macsec statistics

**Syntax** show security macsec statistics  
<brief | detail>  
<interface *interface-name*>

**Release Information** Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.  
Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.

**Description** Display Media Access Control Security (MACsec) statistics.

**Options** **none**—Display MACsec statistics in brief form for all interfaces on the switch.

**brief | detail**—(Optional) Display the specified level of output. Using the **brief** option is equivalent to entering the command with no options (the default). The **detail** option displays additional fields that are not visible in the **brief** output.



**NOTE:** The field names that only appear in this command output when you enter the **detail** option are mostly useful for debugging purposes by Juniper Networks support personnel.

**interface interface-name**—(Optional) Display MACsec statistics for the specified interface only.

**Required Privilege Level** view

**Related Documentation** • [show security macsec connections on page 294](#)

**List of Sample Output** [show security macsec statistics interface xe-0/1/0 detail on page 298](#)

**Output Fields** [Table 27 on page 296](#) lists the output fields for the **show security macsec statistics** command. Output fields are listed in the approximate order in which they appear.

The field names that appear in this command output only when you enter the **detail** option are mostly useful for debugging purposes by Juniper Networks support personnel. Those field names are, therefore, not included in this table.

**Table 27: show security macsec statistics Output Fields**

| Field Name                                   | Field Description      | Level of Output |
|----------------------------------------------|------------------------|-----------------|
| <b>Interface name</b>                        | Name of the interface. | All levels      |
| <b>Fields for Secure Channel transmitted</b> |                        |                 |

Table 27: show security macsec statistics Output Fields (*continued*)

| Field Name                                       | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                 | Level of Output |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Encrypted packets</b>                         | <p>Total number of packets transmitted out of the interface in the secure channel that were secured and encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>                                                                                                                                                              | All levels      |
| <b>Encrypted bytes</b>                           | <p>Total number of bytes transmitted out of the interface in the secure channel that were secured and encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>                                                                                                                                                                | All levels      |
| <b>Protected packets</b>                         | <p>Total number of packets transmitted out of the interface in the secure channel that were secured but not encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>                                                                                                                                                          | All levels      |
| <b>Protected bytes</b>                           | <p>Total number of bytes transmitted out of the interface in the secure channel that were secured but not encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>                                                                                                                                                            | All levels      |
| <b>Fields for Secure Association transmitted</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                   |                 |
| <b>Encrypted packets</b>                         | <p>Total number of packets transmitted out of the interface in the connectivity association that were secured and encrypted using MACsec.</p> <p>The total includes the data packets transmitted in the secure channel and secured using a SAK and the control packets secured using a connectivity association key (CAK).</p>                                                                                                    | All levels      |
| <b>Protected packets</b>                         | <p>Total number of packets transmitted out of the interface in the connectivity association that were secured but not encrypted using MACsec.</p> <p>The total includes the data packets transmitted in the secure channel and secured using a SAK and the control packets secured using a connectivity association key (CAK).</p>                                                                                                | All levels      |
| <b>Fields for Secure Channel received</b>        |                                                                                                                                                                                                                                                                                                                                                                                                                                   |                 |
| <b>Accepted packets</b>                          | <p>The number of received packets that have been accepted by the secure channel on the interface. The secure channel is used to send all data plane traffic on a MACsec-enabled link.</p> <p>A packet is considered accepted for this counter when it has been received by this interface and it has passed the MACsec integrity check.</p> <p>This counter increments for traffic that is and is not encrypted using MACsec.</p> | All levels      |

Table 27: show security macsec statistics Output Fields (*continued*)

| Field Name                                    | Field Description                                                                                                                                                                                                                                                                                                                                                                                     | Level of Output |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Validated bytes</b>                        | <p>The number of bytes that have been validated by the MACsec integrity check and received on the secure channel on the interface. The secure channel is used to send all data plane traffic on a MACsec-enabled link.</p> <p>This counter does not increment when MACsec encryption is disabled.</p>                                                                                                 | All levels      |
| <b>Decrypted bytes</b>                        | <p>The number of bytes received in the secure channel on the interface that have been decrypted. The secure channel is used to send all data plane traffic on a MACsec-enabled link.</p> <p>An encrypted byte has to be decrypted before it can be received on the receiving interface. The decrypted bytes counter is incremented for received traffic that was encrypted using MACsec.</p>          | All levels      |
| <b>Fields for Secure Association received</b> |                                                                                                                                                                                                                                                                                                                                                                                                       |                 |
| <b>Accepted packets</b>                       | <p>The number of received packets that have been accepted in the connectivity association on the interface. The counter includes all control and data plane traffic accepted on the interface.</p> <p>A packet is considered accepted for this counter when it has been received by this interface and it has passed the MACsec integrity check.</p>                                                  | All levels      |
| <b>Validated bytes</b>                        | <p>The number of bytes that have been validated by the MACsec integrity check and received on the connectivity association on the interface. The counter includes all control and data plane traffic accepted on the interface.</p> <p>This counter does not increment when MACsec encryption is disabled.</p>                                                                                        | All levels      |
| <b>Decrypted bytes</b>                        | <p>The number of bytes received in the connectivity association on the interface that have been decrypted. The counter includes all control and data plane traffic accepted on the interface.</p> <p>An encrypted byte has to be decrypted before it can be received on the receiving interface. The decrypted bytes counter is incremented for received traffic that was encrypted using MACsec.</p> | All levels      |

## Sample Output

### show security macsec statistics interface xe-0/1/0 detail

```
user@host> show security macsec statistics interface xe-0/1/0 detail
```

```
Interface name: xe-0/1/0
Secure Channel transmitted
  Encrypted packets: 123858
  Encrypted bytes:   32190903
  Protected packets: 0
  Protected bytes:   0
Secure Association transmitted
```

```
    Encrypted packets: 123858
    Protected packets: 0
Secure Channel received
    Accepted packets: 123877
    Validated bytes: 0
    Decrypted bytes: 32196238
Secure Association received
    Accepted packets: 123877
    Validated bytes: 0
    Decrypted bytes: 32196238
Error and debug
Secure Channel transmitted packets
    Untagged: 0, Too long: 0
Secure Channel received packets
    Control: 0, Tagged miss: 3202804
    Untagged hit: 0, Untagged: 0
    No tag: 0, Bad tag: 0
    Unknown SCI: 0, No SCI: 0
    Control pass: 0, Control drop: 0
    Uncontrol pass: 123877, Uncontrol drop: 0
    Hit dropped: 0, Invalid accept: 0
    Late drop: 0, Delayed accept: 0
    Unchecked: 0, Not valid drop: 0
    Not using SA drop: 0, Unused SA accept: 0
```

## show security mka sessions

|                                 |                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security mka sessions<br><interface <i>interface-name</i> >                                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                             |
| <b>Description</b>              | Display MACsec Key Agreement (MKA) session information.                                                                                                                                                                                               |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li><b>interface <i>interface-name</i></b>—(Optional) Display the MKA session information for the specified interface only.</li> </ul>                                                                             |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">show security mka statistics on page 302</a></li> <li><a href="#">show security macsec connections on page 294</a></li> <li><a href="#">show security macsec statistics on page 296</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show security mka sessions on page 301</a>                                                                                                                                                                                                |
| <b>Output Fields</b>            | Table 28 on page 300 lists the output fields for the <b>show security mka sessions</b> command. Output fields are listed in the approximate order in which they appear.                                                                               |

Table 28: show security mka sessions Output Fields

| Field Name        | Field Description                                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface name    | Name of the interface.                                                                                                                               |
| Member identifier | Name of the member identifier.                                                                                                                       |
| CAK name          | Name of the Connectivity Association Key (CAK).<br>The CAK is configured using the <b>cak</b> keyword when configuring the pre-shared key.           |
| Transmit interval | The transmit interval.                                                                                                                               |
| Outbound SCI      | Name of the outbound secure channel identifier.                                                                                                      |
| Message number    | Number of the last data message.                                                                                                                     |
| Key number        | Key number.                                                                                                                                          |
| Key server        | Key server status.<br>The switch is the key server when this output is <b>yes</b> . The switch is not the key server when this output is <b>no</b> . |



Table 28: show security mka sessions Output Fields (*continued*)

| Field Name           | Field Description                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------------|
| Key server priority  | The key server priority.<br><br>The key server priority can be set using the <b>key-server-priority</b> statement. |
| Latest SAK AN        | Name of the latest secure association key (SAK) association number.                                                |
| Latest SAK KI        | Name of the latest secure association key (SAK) key identifier.                                                    |
| Fields for Peer list |                                                                                                                    |
| Member identifier    | Name of the member identifier.                                                                                     |
| Hold time            | Hold time, in seconds.                                                                                             |
| Message number       | Number of the last data message                                                                                    |
| SCI                  | Name of the secure channel identifier.                                                                             |
| Lowest acceptable PN | Number of the lowest acceptable packet number (PN).                                                                |

## Sample Output

### show security mka sessions

```
user@host> show security mka sessions
```

```
Interface name: xe-0/1/0
Member identifier: 0CCBEE42F8778300F8D0C1DC
CAK name: 1234567890
Transmit interval: 2000(ms)
Outbound SCI: 2C:6B:F5:9D:4B:1B/1
Message number: 1526465    Key number: 0
Key server: no             Key server priority: 15
Latest SAK AN: 0           Latest SAK KI: 4F18CE25228178FD15976E4C/1
Previous SAK AN: 0         Previous SAK KI: 000000000000000000000000/0
Peer list
1. Member identifier: 4F18CE25228178FD15976E4C (live)
   Message number: 1526484 Hold time: 14500 (ms)
   SCI: 2C:6B:F5:9D:3A:1B/1
   Lowest acceptable PN: 121198
```

## show security mka statistics

|                                 |                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security mka statistics<br><interface <i>interface-name</i> >                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                           |
| <b>Description</b>              | Display MACsec Key Agreement (MKA) protocol statistics.<br><br>The output for this command does not include statistics for MACsec data traffic. For MACsec data traffic statistics, see <a href="#">show security macsec statistics</a> .           |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li><b>interface <i>interface-name</i></b>—(Optional) Display the MKA information for the specified interface only.</li> </ul>                                                                                   |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">show security mka sessions on page 300</a></li> <li><a href="#">show security macsec statistics on page 296</a></li> <li><a href="#">show security macsec connections on page 294</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show security mka statistics on page 303</a>                                                                                                                                                                                            |
| <b>Output Fields</b>            | <a href="#">Table 29 on page 302</a> lists the output fields for the <b>show security mka statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                           |

**Table 29: show security mka statistics Output Fields**

| Field Name                      | Field Description                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Received packets</b>         | <p>Number of received MKA control packets.</p> <p>This counter increments for received MKA control packets only. This counter does not increment when data packets are received.</p>                                                                                                                        |
| <b>Transmitted packets</b>      | <p>Number of transmitted MKA packets</p> <p>This counter increments for transmitted MKA control packets only. This counter does not increment when data packets are transmitted.</p>                                                                                                                        |
| <b>Version mismatch packets</b> | Number of version mismatch packets.                                                                                                                                                                                                                                                                         |
| <b>CAK mismatch packets</b>     | <p>Number of Connectivity Association Key (CAK) mismatch packets.</p> <p>This counter increments when the connectivity association key (CAK) and connectivity association key name (CKN), which are user-configured values that have to match to enable MACsec, do not match for an MKA control packet.</p> |

Table 29: show security mka statistics Output Fields (*continued*)

| Field Name                           | Field Description                                                                                                                                                                 |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICV mismatch packets                 | Number of ICV mismatched packets.<br><br>This counter increments when the connectivity association key (CAK) value does not match on both ends of a MACsec-secured Ethernet link. |
| Duplicate message identifier packets | Number of duplicate message identifier packets.                                                                                                                                   |
| Duplicate message number packets     | Number of duplicate message number packets.                                                                                                                                       |
| Duplicate address packets            | Number of duplicate source MAC address packets.                                                                                                                                   |
| Invalid destination address packets  | Number of invalid destination MAC address packets.                                                                                                                                |
| Formatting error packets             | Number of formatting error packets.                                                                                                                                               |
| Old Replayed message number packets  | Number of old replayed message number packets.                                                                                                                                    |

## Sample Output

### show security mka statistics

```
user@host> show security mka statistics
```

```

Received packets:          1525844
Transmitted packets:       1525841
Version mismatch packets:  0
CAK mismatch packets:      0
ICV mismatch packets:      0
Duplicate message identifier packets: 0
Duplicate message number packets: 0
Duplicate address packets:  0
Invalid destination address packets: 0
Formatting error packets:   0
Old Replayed message number packets: 0

```

## show system statistics arp

---

|                                 |                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show system statistics arp                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.6 for EX Series switches.                                                                                                            |
| <b>Description</b>              | Display system-wide Address Resolution Protocol (ARP) statistics.                                                                                                             |
| <b>Required Privilege Level</b> | view                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Example: Configuring Proxy ARP on an EX Series Switch</i></li><li>• <i>Verifying That Proxy ARP Is Working Correctly</i></li></ul> |

## show system statistics arp

```
user@switch> show system statistics arp
arp:
    90060 datagrams received
    34 ARP requests received
    610 ARP replies received
    0 resolution request received
    0 unrestricted proxy requests
    0 restricted proxy requests
    0 received proxy requests
    0 unrestricted proxy requests not proxied
    0 restricted proxy requests not proxied
    0 datagrams with bogus interface
    0 datagrams with incorrect length
    0 datagrams for non-IP protocol
    0 datagrams with unsupported op code
    0 datagrams with bad protocol address length
    0 datagrams with bad hardware address length
    0 datagrams with multicast source address
    0 datagrams with multicast target address
    0 datagrams with my own hardware address
    0 datagrams for an address not on the interface
    0 datagrams with a broadcast source address
    294 datagrams with source address duplicate to mine
    89113 datagrams which were not for me
    0 packets discarded waiting for resolution
    0 packets sent after waiting for resolution
    309 ARP requests sent
    35 ARP replies sent
    0 requests for memory denied
    0 requests dropped on entry
    0 requests dropped during retry
    0 requests dropped due to interface deletion
    0 requests on unnumbered interfaces
    0 new requests on unnumbered interfaces
    0 replies for from unnumbered interfaces
    0 requests on unnumbered interface with non-subnetted donor
    0 replies from unnumbered interface with non-subnetted donor
```

## PART 4

# Troubleshooting

- [Troubleshooting Procedures on page 307](#)



## CHAPTER 8

# Troubleshooting Procedures

- [Troubleshooting Port Security on page 307](#)

## 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 on page 307](#)
- [Multiple DHCP Server Packets Have Been Received on Untrusted Interfaces on page 307](#)

### MAC Addresses That Exceed the MAC Limit or MAC Move Limit Are Not Listed in the Ethernet Switching Table

**Problem**    **Description:** 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 (Access Port Security) 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**    **Description:**

You see log messages that DHCP server packets were received on an untrusted interface—for example:

```
5 untrusted DHCPPOFFER 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 page 43](#)
  - [Verifying That a Trusted DHCP Server Is Working Correctly on page 256](#)
  - [Verifying That MAC Limiting Is Working Correctly on page 257](#)
  - [Enabling a Trusted DHCP Server \(CLI Procedure\) on page 136](#)
  - [Configuring MAC Limiting \(CLI Procedure\) on page 140](#)