


```

unit 0 {
    family ethernet-switching {
        port-mode trunk;
        vlan {
            members 20;
        }
    }
}
}
}
}
vlands {
    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 77](#)
- [Verifying That DAI Is Working Correctly on Switch 1 on page 78](#)
- [Verifying That MAC Limiting Is Working Correctly on Switch 1 on page 78](#)

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 45](#)
- [Configuring Port Security \(CLI Procedure\) on page 112](#)
- [Configuring Port Security \(J-Web Procedure\) on page 114](#)
- [secure-access-port on page 235](#)

- *secure-access-port*
- [show arp inspection statistics on page 281](#)
- [show dhcp snooping binding on page 282](#)
- [show ethernet-switching table on page 288](#)
- *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 79](#)
- [Overview and Topology on page 80](#)
- [Configuring IP Source Guard with 802.1X Authentication, DHCP Snooping, and Dynamic ARP Inspection on page 81](#)
- [Configuring IP Source Guard on a Guest VLAN on page 84](#)
- [Verification on page 87](#)

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 87](#)
- [Verifying the VLAN Association with the Interface on page 88](#)
- [Verifying That DHCP Snooping Is Working on the VLAN on page 88](#)
- [Verifying That IP Source Guard Is Working on the VLAN on page 88](#)

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 45](#)
- [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 89](#)
- [Configuring IP Source Guard \(CLI Procedure\) on page 151](#)

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 89](#)
- [Overview and Topology on page 90](#)
- [Configuration on page 91](#)
- [Verification on page 93](#)

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 93](#)
- [Verifying the VLAN Association with the Interface on page 94](#)
- [Verifying That DHCP Snooping and IP Source Guard Are Working on the Data VLAN on page 94](#)

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 79](#)
 - [Example: Configuring Basic Port Security Features on page 45](#)
 - [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
 - [Configuring IP Source Guard \(CLI Procedure\) on page 151](#)

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 96](#)
- [Overview and Topology on page 96](#)
- [Configuration on page 98](#)
- [Verification on page 98](#)

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

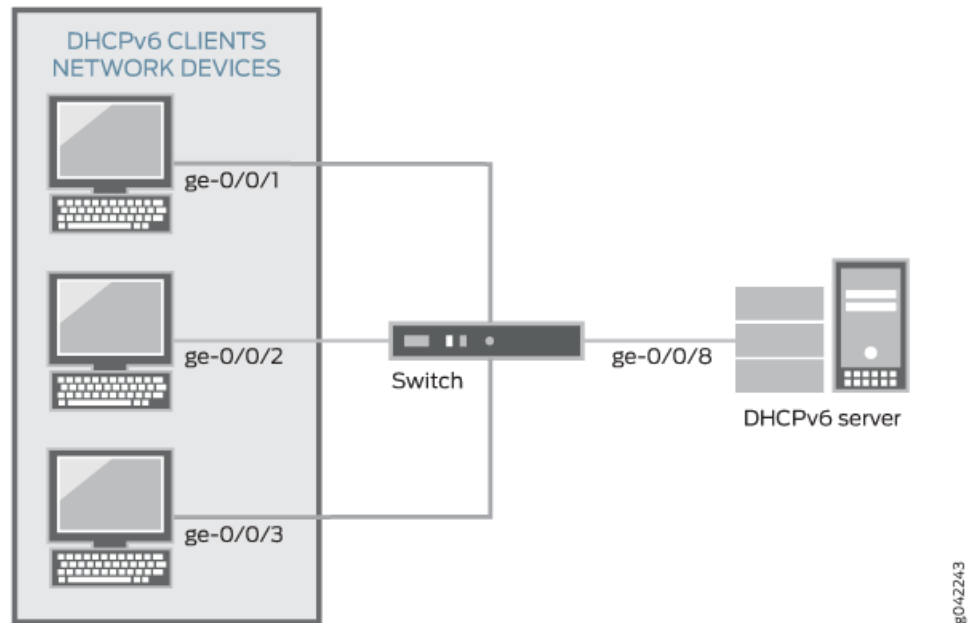
the DHCPv6 snooping table. If there is no match in the table, the switch does not forward the packet—that is, the packet is discarded. Neighbor discovery inspection verifies neighbor discovery messages sent between IPv6 nodes on the same network link against the DHCPv6 snooping table, and also discards 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 65](#) 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 9 on page 65](#).

Table 12: 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 sales	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8

Table 12: 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 99](#)
- [Verifying That Neighbor Discovery Inspection Is Working Correctly on the Switch on page 99](#)

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 151](#)
 - [Enabling DHCP Snooping \(CLI Procedure\) on page 135](#)
 - [Configuring Port Security \(CLI Procedure\) on page 112](#)

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 100](#)
- [Overview and Topology on page 101](#)
- [Configuration on page 101](#)

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 103](#)
- [Setting Up DHCP Option 82 with the Switch as a 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>.
- *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 103](#)
- [Overview and Topology on page 104](#)
- [Configuration on page 105](#)

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.

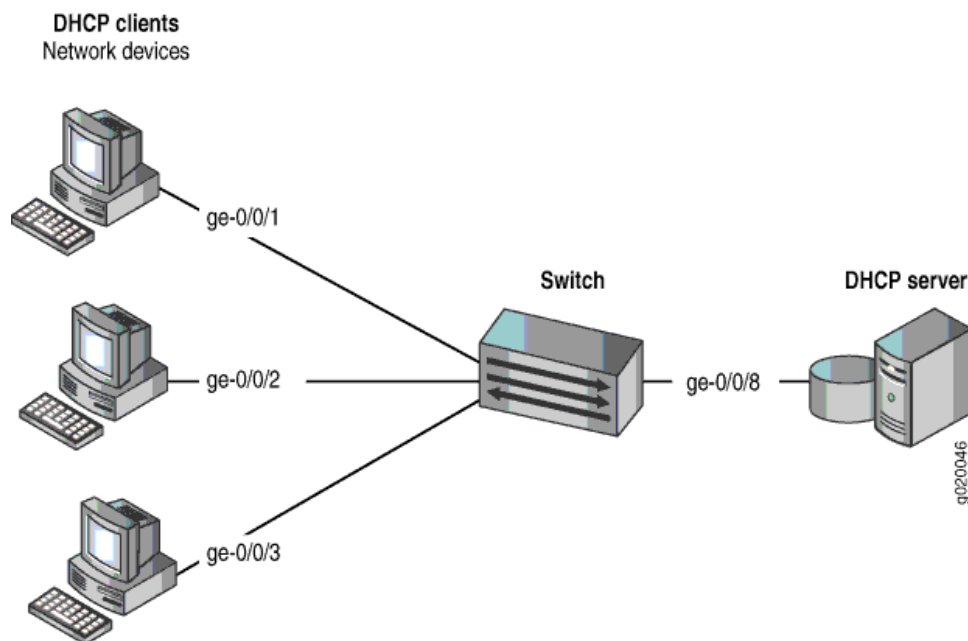
DHCP option 82 is enabled on an individual VLAN or on all VLANs on the switch.

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 104 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 100](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 159](#)
- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.
- [secure-access-port on page 235](#)
- *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 107](#)
- [Overview and Topology on page 107](#)
- [Configuration on page 108](#)
- [Verification on page 109](#)

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.

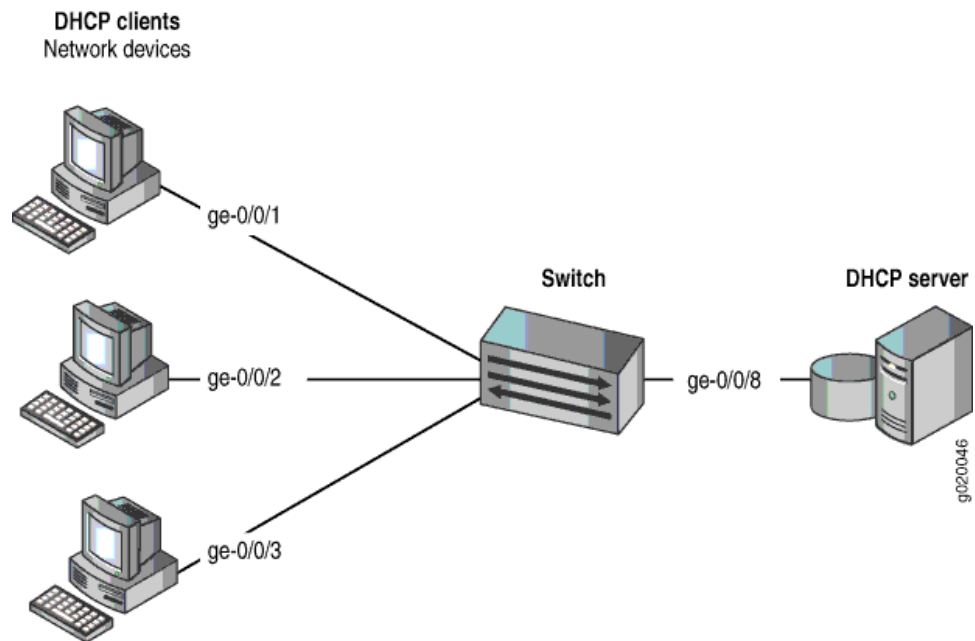
In the default switch configuration:

- 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 108](#) 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 13 on page 108](#).

Table 13: 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 109](#)
- [Verifying That Prioritized Forwarding Is Working Correctly on the DAI Inspected Packets on page 110](#)

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 63](#)

CHAPTER 4

Configuration Tasks

- [Configuring Port Security \(CLI Procedure\) on page 112](#)
- [Configuring Port Security \(J-Web Procedure\) on page 114](#)
- [Configuring Media Access Control Security \(MACsec\) on page 118](#)
- [Enabling DHCP Snooping \(CLI Procedure\) on page 135](#)
- [Enabling DHCP Snooping \(J-Web Procedure\) on page 138](#)
- [Enabling a Trusted DHCP Server \(CLI Procedure\) on page 139](#)
- [Enabling a Trusted DHCP Server \(J-Web Procedure\) on page 139](#)
- [Enabling Dynamic ARP Inspection \(CLI Procedure\) on page 140](#)
- [Enabling Dynamic ARP Inspection \(J-Web Procedure\) on page 142](#)
- [Configuring MAC Limiting \(CLI Procedure\) on page 143](#)
- [Configuring MAC Limiting \(J-Web Procedure\) on page 146](#)
- [Configuring MAC Move Limiting \(CLI Procedure\) on page 148](#)
- [Configuring MAC Move Limiting \(J-Web Procedure\) on page 150](#)
- [Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces \(CLI Procedure\) on page 151](#)
- [Configuring IP Source Guard \(CLI Procedure\) on page 151](#)
- [Configuring Static IP Addresses for DHCP Bindings on Access Ports \(CLI Procedure\) on page 155](#)
- [Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 156](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 159](#)
- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 162](#)
- [Configuring Persistent MAC Learning \(CLI Procedure\) on page 162](#)
- [Making IP-MAC Bindings in the DHCP Snooping Database Persistent \(CLI Procedure\) on page 164](#)

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 112](#)
- [Enabling Dynamic ARP Inspection \(DAI\) on page 113](#)
- [Enabling IPv6 Neighbor Discovery Inspection on page 113](#)
- [Limiting Dynamic MAC Addresses on an Interface on page 113](#)
- [Enabling Persistent MAC Learning on an Interface on page 114](#)
- [Limiting MAC Address Movement on page 114](#)
- [Configuring Trusted DHCP Servers on an Interface on page 114](#)

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 114](#)
- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 162](#)
- [Example: Configuring Basic Port Security Features on page 45](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 71](#)
- [Monitoring Port Security on page 257](#)
- [Understanding Port Security on page 7](#)
- [secure-access-port on page 235](#)
- [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 14 on page 115](#) to modify port security settings on VLANs.
Enter information as specified in [Table 15 on page 117](#) 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 14: Port Security Settings on VLANs

Field	Function	Your Action
General tab		
Enable DHCP Snooping on VLAN NOTE: On EX4300 switches, DHCP snooping is enabled implicitly for all VLANs if you configure dhcp-security 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. TIP: 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 14: 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"> log—Generate a system log entry, an SNMP trap, or an alarm. drop—Drop the packets and generate a system log entry, an SNMP trap, or an alarm (default). shutdown—Shut down the VLAN and generate an alarm. You can mitigate the effect of this option by configuring autorecovery from the disabled state and specifying a disable timeout value. See “Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)” on page 162. none—Take no action. <p>EX4300 switches have an additional option:</p> <ul style="list-style-type: none"> drop-and-log—Drop the packet and generate an alarm, an SNMP trap, or a system log entry.
DHCP Groups		
Group Name NOTE: This option is supported only on EX4300 switches.	Specifies the DHCP name of the group.	Enter a name.
Trusted NOTE: This option is supported only on EX4300 switches.	Specifies trusting DHCP packets on the selected interface. By default, trunk ports are dhcp-trusted .	To enable this option, select the check box.
No Option-82 NOTE: 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 NOTE: This option is supported only on EX4300 switches.	Specifies the DHCP interface.	Select the required interface.
Ports		
Interface NOTE: This option is supported only on EX4300 switches.	Name of the interface.	Click the Edit button of the selected interface, to configure the MAC limit and the MAC limit action.

Table 14: Port Security Settings on VLANs (*continued*)

MAC Limit NOTE: 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 NOTE: 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"> • drop—Drop the packet and do not learn. Default is forward. • drop-and-log—Drop the packet and generate an alarm, an SNMP trap, or a system log entry. • log—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry. • none—Forward the packet. • shutdown—Disable the interface and generate an alarm, an SNMP trap, or a system log entry.

Table 15: Port Security on Interfaces

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

Table 15: 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"> • log—Generate a system log entry, an SNMP trap, or an alarm. • drop—Drop the packets and generate a system log entry, an SNMP trap, or an alarm. (Default) • shutdown—Shut down the interface and generate an alarm. You can mitigate the effect of this option by configuring autorecovery from the disabled state and specifying a disable timeout value. See “Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)” on page 162 • none—Take no action. <p>EX4300 switches have an additional option:</p> <ul style="list-style-type: none"> • drop-and-log—Drop the packet and generate an alarm, an SNMP trap, or a system log entry.
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"> 1. Click Add. 2. Enter the MAC address. 3. Click OK.

- Related Documentation**
- [Configuring Port Security \(CLI Procedure\) on page 112](#)
 - [Example: Configuring Basic Port Security Features on page 45](#)
 - [Monitoring Port Security on page 257](#)
 - [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 119](#)
- [Acquiring and Downloading the MACsec Feature License on page 120](#)
- [Configuring the PIC Mode of the MACsec-capable Interfaces \(EX4200 switches only\) on page 121](#)
- [Configuring MACsec Using Static Connectivity Association Key Security Mode \(Recommended for Enabling MACsec on Switch-to-Switch Links\) on page 123](#)
- [Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link on page 127](#)
- [Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link on page 131](#)

Acquiring and Downloading the Junos OS Software

MACsec was initially released on EX4200, EX4300, and EX4550 switches in Junos OS Release 13.2X50-D15. MACsec was released on EX4600 and QFX5100-24Q switches in Junos OS Release 14.1X53-D15, and on EX9200 series switches in Junos OS Release 15.1R1. 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 on EX4200, EX4300, EX4550, EX4600, and QFX5100-24Q switches.

You must download the standard version of your Junos OS software to enable MACsec on EX9200 switches. MACsec is not supported in the limited version of Junos OS on EX9200 switches.

See [“Understanding Media Access Control Security \(MACsec\)” on page 26](#) for additional information on the versions of Junos OS software that are required for MACsec.

You can identify whether a software package is the controlled or standard 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 standard version of Junos OS on an EX9200 switch is named using the following format:

package-name-m.nZx.y-.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 for EX4200, EX4300, EX4550, EX4600, or QFX5100-24Q switches 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.

The standard version of Junos OS software for EX9200 switches contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of this Junos OS software is strictly controlled under United States export laws. The export, import, and use of this Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring this version of your Junos OS software, contact Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

The process for installing the controlled or standard version of Junos OS software onto your switch is identical to installing any other 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:

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,

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 136](#)
- [Applying CoS Forwarding Classes to Prioritize Snooped Packets on page 136](#)

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 138](#)
- [Example: Configuring Basic Port Security Features on page 45](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 71](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 63](#)
- [Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 106](#)
- [Verifying That DHCP Snooping Is Working Correctly on page 259](#)
- [Monitoring Port Security on page 257](#)
- [Understanding DHCP Snooping for Port Security on page 12](#)
- [class-of-service](#)
- [secure-access-port on page 235](#)
- [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 135](#)
- [Example: Configuring Basic Port Security Features on page 45](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 71](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 63](#)
- [Verifying That DHCP Snooping Is Working Correctly on page 259](#)
- [Monitoring Port Security on page 257](#)
- [Understanding DHCP Snooping for Port Security on page 12](#)



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 139](#)
- [Example: Configuring Basic Port Security Features on page 45](#)
- [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 56](#)
- [Verifying That a Trusted DHCP Server Is Working Correctly on page 260](#)
- [Monitoring Port Security on page 257](#)
- [Understanding Trusted DHCP Servers for Port Security on page 33](#)

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 141](#)
- [Applying CoS Forwarding Classes to Prioritize Inspected Packets on page 141](#)

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 143](#)
- [Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 68](#)
- [Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 53](#)
- [Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 60](#)
- [Verifying That MAC Limiting Is Working Correctly on page 261](#)
- [Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces \(CLI Procedure\) on page 151](#)
- [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.

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 259](#)
- [Understanding DHCP Snooping for Port Security on page 12](#)
- [secure-access-port on page 235](#)
- *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 103](#)
- [secure-access-port on page 235](#)
- *secure-access-port*
- [Understanding DHCP Option 82 for Port Security on Switching Devices on page 37](#)
- *Understanding DHCP Option 82 for Port Security*
- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.


```

        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 16: Unsupported [edit forwarding-options] Configuration Statements on EX Series Switches

Statement	Hierarchy Level
NOTE: 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]


```

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 (MACsec);
      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 17: Unsupported [edit security] Configuration Statements on EX Series Switches

Statement	Hierarchy
NOTE: Variables, such as <i>filename</i> , are not shown in the statements or hierarchies.	
audible	[edit security alarms]
continuous	[edit security alarms audible]

- 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 103](#)
 - [Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 100](#)
 - [Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 159](#)
 - [Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server \(CLI Procedure\) on page 156](#)
 - *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

Syntax	<code>ckn hexadecimal-number;</code>
Hierarchy Level	[edit security macsec connectivity-association connectivity-association-name pre-shared-key]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Default	No CKN exists, by default.
Options	<p>hexadecimal-number—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>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on page 118

connectivity-association

Syntax	<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 (MACsec); 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>
Hierarchy Level	[edit security macsec]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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 interfaces statement in the [edit security macsec] hierarchy.</p>
Default	No connectivity associations are present, by default.
Options	The remaining statements are explained separately.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

Related Documentation • [Configuring Media Access Control Security \(MACsec\) on page 118](#)

connectivity-association (MACsec Interfaces)

Syntax	<code>connectivity-association <i>connectivity-association-name</i>;</code>
Hierarchy Level	[edit security macsec interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Applies a connectivity association to an interface, which enables Media Access Control Security (MACsec) on that interface.
Default	No connectivity associations are associated with any interfaces.
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 118

direction

Syntax	direction (inbound outbound);
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Default	<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>
Options	<p>inbound—Enable MACsec security on traffic entering the interface that has applied the secure channel.</p> <p>outbound—Enable MACsec security on traffic leaving the interface that has applied the secure channel.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on page 118

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


dhcp-snooping-file

Syntax	<pre>dhcp-snooping-file { location (local_pathname remote_URL); timeout seconds; write-interval seconds; }</pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port]
Release Information	Statement introduced in Junos OS Release 9.4 for EX Series switches.
Description	<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>
Default	The IP-MAC bindings in the DHCP snooping database file are not persistent. If the switch is rebooted, the bindings are lost.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 164 • Understanding DHCP Snooping for Port Security on page 12

dhcp-trusted

Syntax	(dhcp-trusted no-dhcp-trusted);
Hierarchy Level	[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Allow DHCP responses from the specified interfaces (ports) or all interfaces.</p> <ul style="list-style-type: none">• dhcp-trusted—Allow DHCP responses.• no-dhcp-trusted—Deny DHCP responses.
Default	Trusted for trunk ports, untrusted for access ports.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Basic Port Security Features on page 45• Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 56• Enabling a Trusted DHCP Server (CLI Procedure) on page 139• Enabling a Trusted DHCP Server (J-Web Procedure) on page 139

disable-timeout

Syntax	<code>disable-timeout <i>timeout</i>;</code>
Hierarchy Level	[edit ethernet-switching-options port-error-disable],
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches.
Description	Specify how long the Ethernet switching interfaces remain in a disabled state because of MAC limiting, MAC move limiting, or storm control errors.
<div>  <p>NOTE: 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>	
Default	The disable timeout is not enabled.
Options	<p><i>timeout</i>—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>Range: 10 through 3600 seconds</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches</i> • Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 162

encryption (MACsec)

Syntax	encryption;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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 no-encryption configuration statement.</p>
Default	MACsec encryption is disabled when MACsec is configured using static SAK security mode, by default.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on page 118

ethernet-switching-options

```

Syntax ethernet-switching-options {
    analyzer (Port Mirroring) {
        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*

- [Enabling DHCP Snooping \(CLI Procedure\) on page 135](#)
- [Enabling DHCP Snooping \(J-Web Procedure\) on page 138](#)

exclude-protocol

Syntax	<code>exclude-protocol <i>protocol-name</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Default	<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>
Options	<p><i>protocol-name</i>—Specifies the name of the protocol that should not be MACsec-secured. Options include:</p> <ul style="list-style-type: none">• cdp—Cisco Discovery Protocol.• lcp—Link Aggregation Control Protocol.• lldp—Link Level Discovery Protocol.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on page 118

forwarding-class (for DHCP Snooping or DAI Packets)

Syntax	forwarding-class class <i>class-name</i> ;
Hierarchy Level	[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>) (examine-dhcp arp-inspection)]
Release Information	Statement introduced in Junos OS Release 11.2 for EX Series switches. Statement introduced in Junos OS Release 12.1 for the QFX Series.
Description	Assign a user-defined or a predefined forwarding class to the packets that have been checked for DHCP snooping or dynamic ARP inspection (DAI).
<div>  <p>NOTE: 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>	
Default	Disabled.
Options	<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.
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"> • Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 106 • Understanding Junos OS CoS Components for EX Series Switches • Understanding DHCP Snooping for Port Security on page 12 • Understanding DAI for Port Security on page 20

id

Syntax	<pre>id { mac-address <i>mac-address</i>; port-id <i>port-id-number</i>; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	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.
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	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on page 118

include-sci

Syntax	include-sci;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
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	<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>
Default	<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>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on page 118

- [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks on page 56](#)
- [Configuring MAC Limiting \(CLI Procedure\) on page 143](#)
- [Enabling a Trusted DHCP Server \(CLI Procedure\) on page 139](#)
- [Configuring Static IP Addresses for DHCP Bindings on Access Ports \(CLI Procedure\) on page 155](#)

interfaces (MACsec)

Syntax	<code>interfaces <i>interface-name</i> { connectivity-association <i>connectivity-association-name</i>; }</code>
Hierarchy Level	[edit security macsec]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Default	Interfaces are not associated with any connectivity associations, by default.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on page 118

ip-source-guard


Syntax	<code>ip-source-guard;</code>
Hierarchy Level	<ul style="list-style-type: none"> For platforms with ELS: [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] For platforms without ELS: [edit ethernet-switching-options secure-access-port <i>vlan</i> (all <i>vlan-name</i>)]
Release Information	<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>
Description	<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"> ip-source-guard—Enable IP source guard checking. no-ip-source-guard—(Not available in [edit vlans <i>vlan-name</i> forwarding-options dhcp-security]) Disable IP source guard checking. <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"> IP source guard can be configured only for a specific VLAN, not for a list or a range of VLAN IDs. DHCP snooping is automatically enabled. <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 ethernet-switching-options secure-access-port <i>vlan</i> (all <i>vlan-name</i>)] hierarchy level:</p> <ul style="list-style-type: none"> You must enable DHCP snooping on all VLANs if you configure IP source guard on all VLANs. You must enable DHCP snooping for the specific VLAN if you configure IP source guard on that specific VLAN. Otherwise, the default behavior of no DHCP snooping applies to that VLAN. <p>See “Enabling DHCP Snooping (CLI Procedure)” on page 135 for more information about this configuration.</p>



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

Default	Disabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 89 • Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 79 • Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing • Configuring IP Source Guard (CLI Procedure) on page 151 • Configuring IP Source Guard (CLI Procedure)

ipv6-source-guard-sessions

Syntax	<pre>ipv6-source-guard-sessions { max-number <i>max-number</i>; }</pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Specify the maximum number of IPv6 source guard sessions for TCAM space provisioning.
	<div>  <p>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.</p> </div>
Default	Disabled.
Options	max-number <i>max-number</i> —The maximum number of IPv6 source guard sessions. Range: 50 through 300.
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"> • Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing • Configuring IP Source Guard (CLI Procedure)

key (MACsec)

Syntax	<code>key <i>key-string</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name security-association security-association-number]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Default	This statement does not have a default value.
Options	<i>key-string</i> —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.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on page 118

key-server-priority (MACsec)

Syntax	<code>key-server-priority <i>priority-number</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> mka]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Default	The default key server priority number is 16.
Options	<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>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on page 118

location (DHCP Snooping Database)

Syntax	<code>location (<i>local_pathname</i> <i>remote_url</i>); <code>timeout</code> <i>seconds</i>; <code>write-interval</code> <i>seconds</i>; }</code>
Hierarchy Level	[edit <code>ethernet-switching-options secure-access-port dhcp-snooping-file</code>]; [edit <code>ethernet-switching-options secure-access-port dhcpv6-snooping-file</code>]
Release Information	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.
Description	<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>
Options	<p><i>local_pathname</i> <i>remote_url</i></p> <ul style="list-style-type: none">• <i>local_pathname</i>—Use <i>/path</i> to store the database file on the local switch.• <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.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 164• Understanding DHCP Snooping for Port Security on page 12

mac

Syntax	<code>mac mac-address;</code>
Hierarchy Level	<ul style="list-style-type: none"> 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> 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> 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>
Release Information	<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>
Description	Configure the media access control (MAC) address or hardware address of the device connected to the specified interface.
Options	<i>mac-address</i> —Value (in hexadecimal format) of the address assigned to this device.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 155 Configuring Static IP Addresses for DHCP and DHCPv6 Bindings on Access Ports (CLI Procedure) Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers (CLI Procedure)

mac-address (MACsec)

Syntax	<code>mac-address <i>mac-address</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i> id]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<p>Specify a MAC address to enable MACsec using static secure association key (SAK) security mode. The mac-address 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 mac-address.</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 mac-address.</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>
Default	No MAC address is specified in the secure channel, by default.
Options	mac-address —The MAC address, in six groups of two hexadecimal digits.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on page 118

mac-limit (Access Port Security)

Syntax	<code>mac-limit <i>limit</i> action <i>action</i>;</code>
Hierarchy Level	[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)], [edit ethernet-switching-options secure-access-port interface <i>interface-name</i>) vlan <i>vlan-name</i>],
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Set a limit on the number of MAC addresses that can be added to the Ethernet switching table. <ul style="list-style-type: none"> • [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. • [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).



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.

Default	The default action is drop .
Options	action <i>action</i> —(Optional) Action to take when the MAC address limit for an interface or for all interfaces is exceeded: <ul style="list-style-type: none"> • drop—Drop the packet and generate a system log entry. • log—Do not drop the packet but generate a system log entry. • none—No action. • shutdown—Disable the interface and generate a system log entry. If you have configured the switch with the port-error-disable statement, the disabled interface recovers automatically upon expiration of the specified disable timeout. If you have not

configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the **clear ethernet-switching port-error** command.

limit—Maximum number of MAC addresses.

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

Related Documentation

- [allowed-mac on page 180](#)
- *clear ethernet-switching table*
- [Example: Configuring Basic Port Security Features on page 45](#)
- [Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks on page 53](#)
- [Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 60](#)
- [Configuring MAC Limiting \(CLI Procedure\) on page 143](#)
- [Configuring MAC Limiting \(J-Web Procedure\) on page 146](#)
- [Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 162](#)

mac-move-limit

Syntax	<pre>mac-move-limit <i>limit</i> { <action <i>action</i> (drop log none shutdown) packet-action <i>action</i> (drop drop and log log none shutdown vlan-member-shutdown)>; interface <i>interface-name</i> { action-priority <i>value</i>; } }</pre>
Hierarchy Level	<ul style="list-style-type: none"> For platforms with ELS: [edit vlans <i>vlan-name</i> switch-options] For platforms without ELS: [edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>)]
Release Information	<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>
Description	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.
Default	If you do not configure mac-move-limit , the default MAC address move limit is unlimited.
Options	<p><i>limit</i>—Maximum number of moves to a new interface per second.</p> <p>Range: 1 through 4,294,967,295</p> <ul style="list-style-type: none"> action <i>action</i>—(Optional) (Available <i>only</i> under the [edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>) mac-move-limit]) hierarchy level.) Action to take when the MAC address move limit is reached: <ul style="list-style-type: none"> drop—Drop the packet and generate a system log entry. This is the default. log—Do not drop the packet but generate a system log entry. none—No action. shutdown—Disable the interface and generate a system log entry. If you configure the switch with the port-error-disable statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you do not configure the switch for autorecovery from the disabled condition, you can bring up the disabled interfaces by running the clear ethernet-switching port-error operational mode command. packet-action <i>action</i>—(Optional) (Available <i>only</i> under the [edit vlans <i>vlan-name</i> switch-options mac-move-limit] hierarchy level.) Action to take when the MAC address move limit is reached:



NOTE: The **drop** and **drop and log** options are not supported on EX9200 switches.

- **drop**—Drop the packet, but 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**—Forward packets with new source MAC addresses, and learn the new source MAC address.
- **shutdown**—Disable the interface and generate an alarm or an SNMP trap. If you configure the interface with the **recovery-timeout** statement, the disabled interface recovers automatically upon expiration of the specified timeout. If you do not configure the interface for a recovery timeout, you can bring up the disabled interface by running the **clear ethernet-switching recovery-timeout** operational mode command.
- **vlan-member-shutdown**—(EX9200 only) Block the interface on the basis of its membership in a specific VLAN and generate an alarm, an SNMP trap, or a system log entry. If you configure an interface with the **recovery-timeout** statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you do not configure the switch for autorecovery from the disabled condition, the blocked interface will recover automatically after 180 seconds.

Default: There is no default action.

The remaining statements are explained separately.

Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system—control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Basic Port Security Features on page 45 • Configuring MAC Move Limiting (CLI Procedure) on page 148 • Configuring MAC Move Limiting (CLI Procedure) • Configuring Persistent MAC Learning (CLI Procedure) • Configuring MAC Move Limiting (J-Web Procedure) on page 150 • Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 162 • 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 (MACsec);
                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.

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 118](#)

mka

Syntax	<pre>mka { must-secure; key-server-priority <i>priority-number</i>; transmit-interval <i>interval</i>; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15.
Description	Specify parameters for the MACsec Key Agreement (MKA) protocol.
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	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on page 118

must-secure

Syntax	<code>must-secure;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> mka]</code>
Release Information	Statement introduced in Junos OS Release 14.1X53-D10.
Description	<p>Specifies that all traffic travelling on the MACsec-secured link must be MACsec-secured to be forwarded onward.</p> <p>When the must-secure option is enabled, all traffic that is not MACsec-secured that is received on the interface is dropped.</p> <p>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.</p> <p>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.</p>
Default	The must-secure option is disabled.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on page 118

no-allowed-mac-log

Syntax	no-allowed-mac-log;
Hierarchy Level	[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify that the switch does not log messages when it receives packets from invalid MAC addresses on an interface that has been configured for particular (allowed) MAC addresses.
Default	The switch logs messages when it receives packets from invalid MAC addresses on an interface that has been configured for particular (allowed) MAC addresses.
Required Privilege Level	system—To view this statement in the configuration. system—control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• allowed-mac on page 180• Example: Configuring Basic Port Security Features on page 45• Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks on page 68• Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks on page 60• Configuring MAC Limiting (CLI Procedure) on page 143• Configuring MAC Limiting (J-Web Procedure) on page 146

no-encryption (MACsec)

Syntax	no-encryption;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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 encryption configuration statement.</p>
Default	MACsec encryption is enabled if MACsec is enabled using static CAK or dynamic security mode.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on page 118

no-examine-dhcpv6

Syntax	<code>no-examine-dhcpv6 { forwarding-class class-name; }</code>
Hierarchy Level	[edit <code>ethernet-switching-options secure-access-port vlan</code> (all <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	<p>Disable DHCPv6 snooping on all VLANs or on the specified VLAN.</p> <p>The remaining statement is explained separately.</p>
Default	Disabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• examine-dhcpv6 on page 199• Example: Configuring Basic Port Security Features on page 45• Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 71• Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks on page 63• Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic on page 106• Enabling DHCP Snooping (CLI Procedure) on page 135• Enabling DHCP Snooping (J-Web Procedure) on page 138


no-gratuitous-arp-request

Syntax	no-gratuitous-arp-request;
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the switch not to respond to gratuitous ARP requests. You can disable responses to gratuitous ARP requests on 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.)
Default	Gratuitous ARP responses are enabled on all Ethernet switching interfaces, and IRB interfaces or RVIs.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Proxy ARP on an EX Series Switch</i> • <i>Configuring Proxy ARP (CLI Procedure)</i> • <i>Configuring Proxy ARP (CLI Procedure)</i>

no-option-37

Syntax	no-option-37;
Hierarchy Level	[edit ethernet-switching-options secure-access-port vlan <i>vlan-name</i>]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Configure the VLAN <i>not</i> to transmit DHCP option 37 information, even if the VLAN is configured to perform DHCPv6 snooping.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>option-82</i> • Understanding DHCP Option 82 for Port Security on Switching Devices on page 37 • Understanding DHCP Snooping for Port Security on page 12

offset

Syntax	offset (0 30 50);
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>] [edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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 offset in the [edit security macsec connectivity-association <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 offset in the [edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>] hierarchy when you are enabling MACsec using static secure association key (SAK) security mode.</p>
Default	0
Options	<p>0—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>30—Specifies that the first 30 octets of each Ethernet frame are unencrypted.</p>
	<p> NOTE: 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>50—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 118](#)

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 45](#)
- [Configuring Persistent MAC Learning \(CLI Procedure\) on page 162](#)
- [Configuring Persistent MAC Learning \(CLI Procedure\)](#)

port-error-disable

Syntax	<pre>port-error-disable { disable-timeout <i>timeout</i> ; }</pre>
Hierarchy Level	[edit ethernet-switching-options],
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">• If you have enabled MAC limiting with the shutdown option and you enable port-error-disable, the switch disables (rather than shuts down) the interface when the MAC address limit is reached.• If you have enabled MAC move limiting with the shutdown option and you enable port-error-disable, the switch disables (rather than shuts down) the interface when the maximum number of moves to a new interface is reached.• If you have enabled storm control with the action-shutdown option and you enable port-error-disable, the switch disables (rather than shuts down) the interface when applicable traffic exceeds the specified levels. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic.
	<div> NOTE: The port-error-disable configuration does not apply to pre-existing error conditions. It impacts only error conditions that are detected after port-error-disable has been enabled and committed. To clear a pre-existing error condition and restore the interface to service, use the operational command that appears in your CLI:</div> <ul style="list-style-type: none">• clear ethernet-switching port-error
	<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">• <i>action-shutdown</i>• Configuring MAC Move Limiting (CLI Procedure) on page 148

port-id

Syntax	<code>port-id <i>port-id-number</i>;</code>
Hierarchy Level	[edit security <code>macsec connectivity-association connectivity-association-name secure-channel secure-channel-name id</code>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Default	No port ID is specified.
Options	<i>port-id-number</i> —The port ID number.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on page 118

pre-shared-key

Syntax	<pre>pre-shared-key { cak hexadecimal-number; ckn hexadecimal-number; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Default	No pre-shared keys exist, by default.
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	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on page 118

prefix (Circuit ID for Option 82)

Syntax	<pre>prefix { host-name; logical-system-name; routing-instance-name; }</pre>
Hierarchy Level	<ul style="list-style-type: none"> For platforms with enhanced Layer 2 software (ELS): [edit vlans forwarding-options dhcp-security option-82 circuit-id] For platforms without ELS: [edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>) dhcp-option82 circuit-id], [edit forwarding-options helpers bootp dhcp-option82 circuit-id], [edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82 circuit-id] For MX Series platforms: [edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82circuit-id]
Release Information	<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 circuit-id] 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>
Description	Configure an optional prefix for the circuit ID suboption in the DHCP option 82 information that is inserted by the switch or router into the packet header of a DHCP request before it forwards or relays the request to a DHCP server.
Default	If the prefix statement is not explicitly specified, no prefix is prepended to the circuit ID.
Options	<p>host-name—Add router host name to DHCP option 82 circuit ID.</p> <p>logical-system-name—Add logical system name to DHCP option-82 circuit ID. This option is not used for the prefix statement at any of the above hierarchy levels.</p> <p>routing-instance-name—Add routing instance name to DHCP option-82 circuit ID. This option is not used for the prefix statement occurring at the following hierarchy levels:</p> <ul style="list-style-type: none"> [edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82circuit-id] Any of the hierarchy levels for the platforms without ELS

Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 103 • Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server on page 100 • Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 159 • Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 156 • Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure) • RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046.

secure-access-port

```
Syntax  secure-access-port {
        dhcp-snooping-file {
            location local_pathname | remote_URL;
            timeout seconds;
            write-interval seconds;
        }
        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 45](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch on page 71](#)
- [Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 89](#)
- [Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server on page 103](#)
- [Example: Configuring an FCoE Transit Switch](#)

secure-channel

Syntax	<pre> secure-channel <i>secure-channel-name</i> { direction (inbound outbound); encryption (MACsec); 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>; } } </pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Options	The remaining statements are explained separately.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on page 118

security-mode

Syntax	<code>security-mode <i>security-mode</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15. The dynamic security mode option was introduced in Junos OS Release 14.1X53-D10.
Description	<p>Configure the MACsec security mode for the connectivity association.</p> <p>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.</p>
Options	<p>security-mode—Specifies the MACsec security mode. Options include:</p> <ul style="list-style-type: none"> • dynamic—Dynamic mode. <p>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.</p> <ul style="list-style-type: none"> • static-cak—Static connectivity association key (CAK) mode. <p>Static CAK security mode is used to enable MACsec on switch-to-switch Ethernet links. In static-cak 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.</p> <ul style="list-style-type: none"> • static-sak—Static secure association key (SAK) mode. <p>Static SAK security mode is used to enable MACsec on switch-to-switch Ethernet links. In static-sak mode, one of two user-configured security keys is used to secure the point-to-point link. The two security keys are regularly rotated.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on page 118

timeout

Syntax	<code>timeout <i>seconds</i>;</code>
Hierarchy Level	[edit ethernet-switching-options secure-access-port dhcp-snooping-file]; [edit ethernet-switching-options secure-access-port dhcpv6-snooping-file]
Release Information	Statement introduced in Junos OS Release 9.4 for EX Series switches. Support at the [edit ethernet-switching-options secure-access-port dhcpv6-snooping-file] hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Specify 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.
Default	None
Options	<i>seconds</i> —Value in seconds. Range: 10 through 3600.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 164 • Understanding DHCP Snooping for Port Security on page 12

transmit-interval (MACsec)

Syntax	<code>transmit-interval <i>interval</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> mka]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<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>
Default	The default transmit interval is 2000 milliseconds.
Options	<i>interval</i> —Specifies the transmit interval, in milliseconds.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on page 118

- *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>

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

vlan (DHCP Bindings on Access Ports)

Syntax	<code>vlan <i>vlan-name</i>;</code>
Hierarchy Level	[edit <code>ethernet-switching-options secure-access-port interface (all <i>interface-name</i>) static-ip <i>ip-address</i></code>]
Release Information	Statement introduced in Junos OS Release 9.2 for EX Series switches.
Description	Associate the static IP address with the specified VLAN associated with the specified interface.
Options	<i>vlan-name</i> —Name of a specific VLAN associated with the specified interface.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 155

PART 3

Administration

- [Routine Monitoring on page 257](#)
- [Operational Commands on page 271](#)

clear dhcpv6 snooping binding

Syntax	clear dhcpv6 snooping binding <mac (all <i>mac-address</i>)> <vlan (all <i>vlan-name</i>)> <vlan (all <i>vlan-name</i>) mac (all <i>mac-address</i>)>
Release Information	Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Clear the DHCPv6 snooping database information.
Options	<p>mac (all <i>mac-address</i>)—(Optional) Clear DHCPv6 snooping information for the specified MAC address or all MAC addresses.</p> <p>vlan (all <i>vlan-name</i>)—(Optional) Clear DHCPv6 snooping information for the specified VLAN or all VLANs.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show dhcpv6 snooping binding on page 285 • Example: Configuring Basic Port Security Features on page 45 • Verifying That DHCP Snooping Is Working Correctly on page 259
List of Sample Output	clear dhcpv6 snooping binding on page 275
Output Fields	This command produces no output.

Sample Output

clear dhcpv6 snooping binding

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


clear neighbor-discovery-inspection statistics

Syntax	clear neighbor-discovery-inspection statistics <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Clear IPv6 neighbor discovery inspection statistics.
Options	<p>none—Clear neighbor discovery inspection statistics on all interfaces.</p> <p>interface <i>interface-name</i>—(Optional) Clear neighbor discovery inspection statistics on one or more interfaces.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show neighbor-discovery-inspection statistics on page 297 • Example: Configuring Basic Port Security Features on page 45
List of Sample Output	clear neighbor-discovery-inspection statistics on page 279
Output Fields	This command produces no output.

Sample Output

clear neighbor-discovery-inspection statistics

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

clear security mka statistics

Syntax	<code>clear security mka statistics</code> <code><interface <i>interface-name</i>></code>
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	<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 show security mka statistics when you enter this command.</p>
Options	<p>none—Clear all MKA counters for all interfaces on the switch.</p> <p>interface <i>interface-name</i>—(Optional) Clear MKA traffic counters for the specified interface only.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security mka statistics on page 306• show security mka sessions on page 304• Understanding Media Access Control Security (MACsec) on page 26

Sample Output

clear security mka statistics

```
user@switch> clear security mka statistics
```


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


```

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

```


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

