

## Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX Series Switch

---

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

This example describes how to configure basic port security features—DHCP snooping, DAI, MAC limiting, and MAC move limiting, as well as a trusted DHCP server and allowed MAC addresses—on a switch. The DHCP server and its clients are all members of a single VLAN on the switch.

- Requirements on page 1
- Overview and Topology on page 1
- Configuration on page 3
- Verification on page 4

### Requirements

This example uses the following hardware and software components:

- One EX3200-24P switch
- JUNOS Release 9.0 or later for EX Series switches
- A DHCP server to provide IP addresses to network devices on the switch

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

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

### Overview and Topology

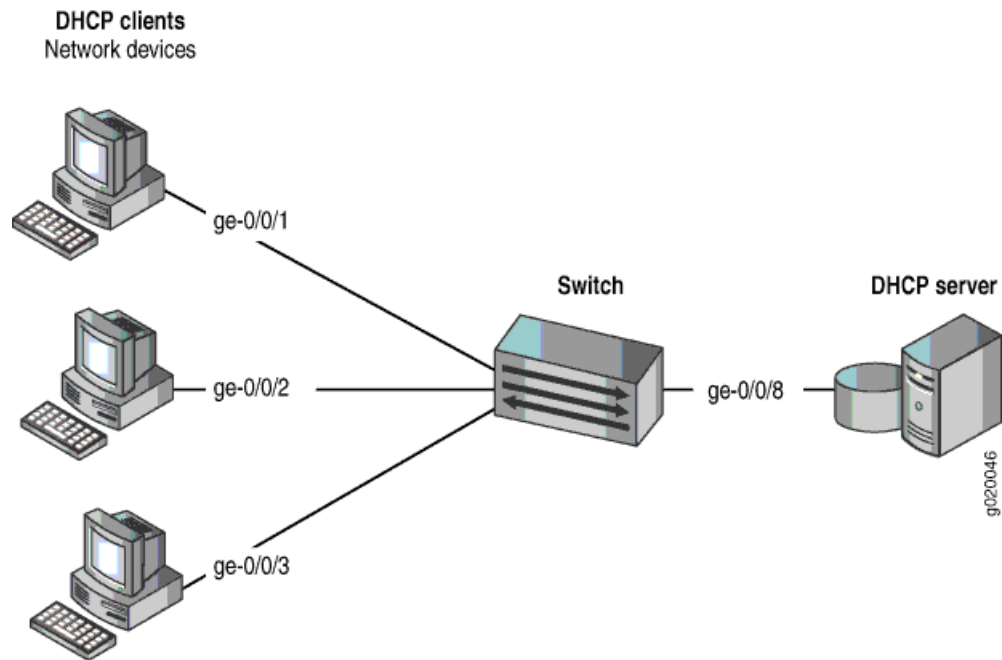
Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. To protect the devices from such attacks, you can configure DHCP snooping to validate DHCP server messages, DAI to protect against MAC spoofing, and MAC cache limiting to constrain the number of MAC addresses the switch adds to its MAC address cache. You can also configure MAC move limiting to help prevent MAC spoofing.

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

The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic Example: Setting Up

Bridging with Multiple VLANs for EX Series Switches. That procedure is not repeated here. Figure 1 illustrates the topology for this example.

**Figure 1: Network Topology for Basic Port Security**



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

**Table 1: Components of the Port Security Topology**

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

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

- 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, which is the default setting.

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

## Configuration

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

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

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

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

1. Enable DHCP snooping on the VLAN:

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

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

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

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

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

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

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

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

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

6. Configure the allowed MAC addresses:

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

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

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

## Verification

To confirm that the configuration is working properly:

- Verifying That DHCP Snooping Is Working Correctly on the Switch on page 5
- Verifying That DAI Is Working Correctly on the Switch on page 5
- Verifying That MAC Limiting and MAC Move Limiting Are Working Correctly on the Switch on page 6
- Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 7

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

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

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

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

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

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

If the DHCP server had been configured as untrusted, the output would look like this:

```
user@switch> show dhcp snooping binding
DHCP Snooping Information:
MAC Address      IP Address      Lease      Type      VLAN      Interface
-----
00:05:85:3A:82:77 0.0.0.0         -          dynamic  employee-vlan ge-0/0/1.0
00:05:85:3A:82:79 0.0.0.0         -          dynamic  employee-vlan ge-0/0/1.0
00:05:85:3A:82:80 0.0.0.0         -          dynamic  employee-vlan ge-0/0/2.0
00:05:85:3A:82:81 0.0.0.0         -          dynamic  employee-vlan ge-0/0/2.0
00:05:85:3A:82:83 0.0.0.0         -          dynamic  employee-vlan ge-0/0/2.0
00:05:85:27:32:88 0.0.0.0         -          dynamic  employee-vlan ge-0/0/2.0
```

In the preceding output sample, IP addresses and lease times are not assigned because the DHCP clients do not have a trusted server to which they can send requests. In the database, the clients' MAC addresses are shown with no assigned IP addresses (hence the 0.0.0.0 content in the IP Address column) and no leases (the lease time is shown as a dash – in the Lease column).

## Verifying That DAI Is Working Correctly on the Switch

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

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

Display the DAI information:

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

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

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

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

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

Display the MAC addresses learned:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 7 entries, 6 learned
VLAN          MAC address          Type      Age      Interfaces
-----
employee-vlan  *                    Flood     -        ge-0/0/2.0
employee-vlan  00:05:85:3A:82:77    Learn     0        ge-0/0/1.0
employee-vlan  00:05:85:3A:82:79    Learn     0        ge-0/0/1.0
employee-vlan  00:05:85:3A:82:80    Learn     0        ge-0/0/2.0
employee-vlan  00:05:85:3A:82:81    Learn     0        ge-0/0/2.0
employee-vlan  00:05:85:3A:82:83    Learn     0        ge-0/0/2.0
employee-vlan  00:05:85:3A:82:85    Learn     0        ge-0/0/2.0
```

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

Display the MAC addresses in the table:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 7 entries, 4 learned
VLAN          MAC address          Type      Age      Interfaces
-----
employee-vlan  *                    Flood     -        ge-0/0/2.0
employee-vlan  00:05:85:3A:82:77    Learn     0        ge-0/0/1.0
employee-vlan  00:05:85:3A:82:79    Learn     0        ge-0/0/1.0
employee-vlan  00:05:85:3A:82:80    Learn     0        ge-0/0/2.0
```

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

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

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

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

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

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

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

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

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