

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

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

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

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

Requirements

This example uses the following hardware and software components:

- One EX 3200-24P 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 specific port security features to mitigate common access-interface attacks, be sure you have:

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

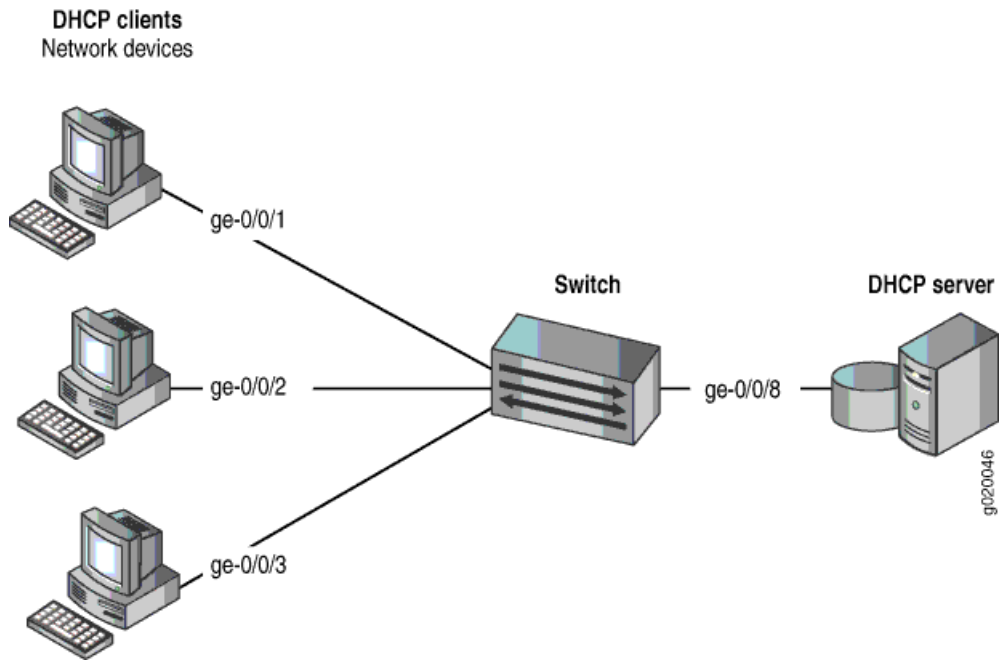
Overview and Topology

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

This example shows how to configure port security features on an EX 3200-24P 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 EX 3200-24P, 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, use the MAC limit feature to control the total number of MAC addresses that can be added to the Ethernet switching table for the specified interface. Use the allowed MAC addresses feature to ensure that the addresses of network devices whose network access is critical are guaranteed to be included in the Ethernet switching table.

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

- Secure port access is activated on the switch.
- No MAC limit is set on any of the interfaces.

- All access interfaces are untrusted, which is the default setting.

Configuration

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

CLI Quick Configuration To quickly configure MAC limiting and some allowed MAC addresses, copy the following commands and paste them into the switch terminal window:

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

Step-by-Step Procedure Configure MAC limiting and some allowed MAC addresses:

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

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

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

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

Results Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That MAC Limiting Is Working Correctly on the Switch on page 4

Verifying That MAC Limiting Is Working Correctly on the Switch

Purpose Verify that MAC limiting is working on the switch.

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

```
user@switch> show ethernet-switching table
Ethernet-switching table: 5 entries, 4 learned
  VLAN          MAC address      Type      Age   Interfaces
  -----
employee-vlan  00:05:85:3A:82:71 Learn     0    ge-0/0/1.0
employee-vlan  00:05:85:3A:82:74 Learn     0    ge-0/0/1.0
employee-vlan  00:05:85:3A:82:77 Learn     0    ge-0/0/1.0
employee-vlan  00:05:85:3A:82:79 Learn     0    ge-0/0/1.0
employee-vlan  *                Flood     0    ge-0/0/1.0
employee-vlan  00:05:85:3A:82:80 Learn     0    ge-0/0/2.0
employee-vlan  00:05:85:3A:82:81 Learn     0    ge-0/0/2.0
employee-vlan  00:05:85:3A:82:83 Learn     0    ge-0/0/2.0
employee-vlan  00:05:85:3A:82:85 Learn     0    ge-0/0/2.0
employee-vlan  *                Flood     -    ge-0/0/2.0
```

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

- Related Topics**
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX Series Switch
 - Configuring MAC Limiting (CLI Procedure)
 - Configuring MAC Limiting (J-Web Procedure)

Published: 2009-08-29