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

In a DHCP starvation attack, an attacker floods an Ethernet LAN with DHCP requests from spoofed (counterfeit) MAC addresses. The switch's trusted DHCP server or servers cannot keep up with the requests and can no longer assign IP addresses and lease times to legitimate DHCP clients on the switch. Requests from those clients are either dropped or directed to a rogue DHCP server set up by the attacker.

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

Requirements

This example uses the following hardware and software components:

- One EX 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 MAC limiting, a port security feature, to mitigate DHCP starvation attacks, be sure you have:

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

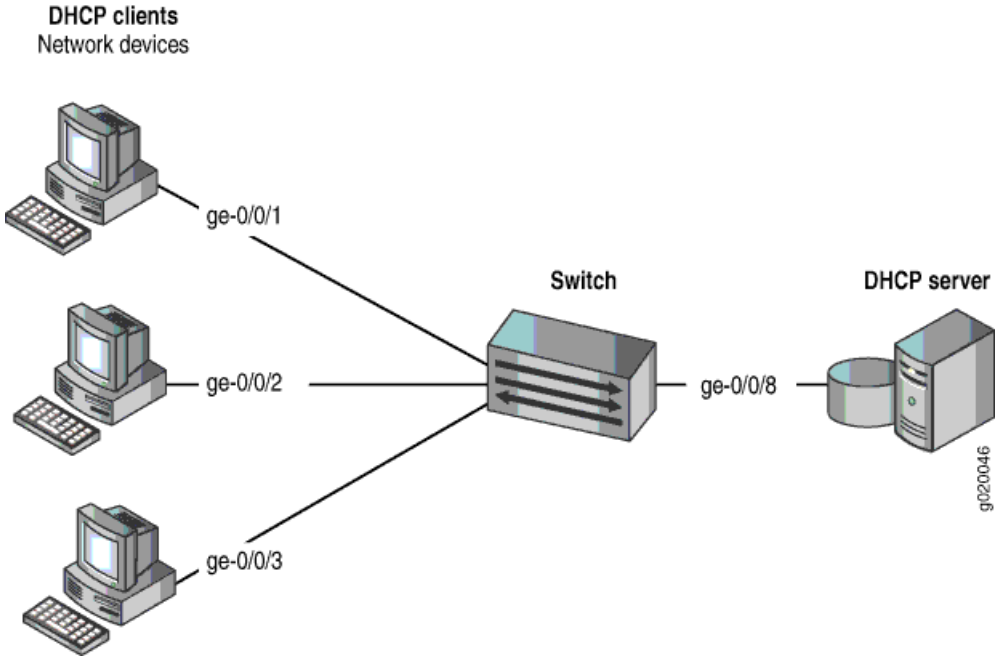
Overview and Topology

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

This example shows how to configure port security features on an EX 3200-24P switch that is connected to a DHCP server.

The setup for this example includes the VLAN employee-vlan on the switch. The procedure for creating that VLAN is described in the topic Example: Setting Up Bridging with Multiple VLANs for EX-series Switches. That procedure is not repeated here. Figure 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	default
Interfaces in employee-vlan	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface for DHCP server	ge-0/0/8

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

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

Configuration

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

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

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

Step-by-Step Procedure Configure MAC limiting:

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

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

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

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

Results Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That MAC Limiting Is Working Correctly on the Switch on page 3

Verifying That MAC Limiting Is Working Correctly on the Switch

Purpose Verify that MAC limiting is working on the switch.

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

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

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

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

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

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

Related 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)