Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks

In one type of attack on the DHCP snooping database, an intruder introduces a DHCP client on an untrusted access interface with a MAC address identical to that of a client on another untrusted interface. The intruder then acquires the DHCP lease of that other client, thus changing the entries in the DHCP snooping table. Subsequently, what would have been valid ARP requests from the legitimate client are blocked.

This example describes how to configure allowed MAC addresses, a port security feature, to protect the switch from DHCP snooping database alteration attacks:

- Requirements on page 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-inteface 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.

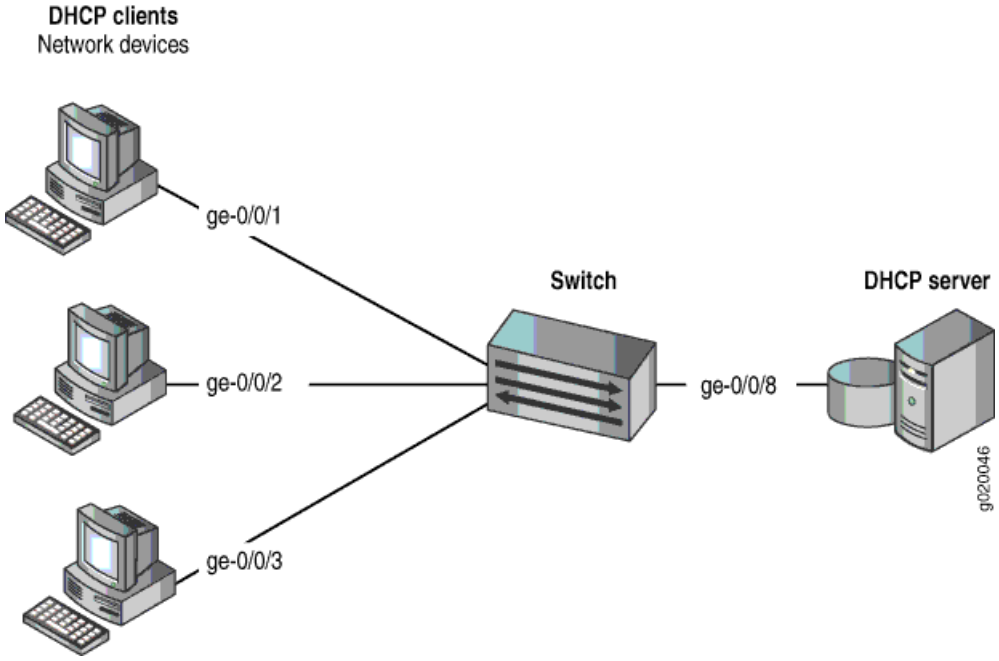
Overview and Topology

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 DHCP snooping database that alters the MAC addresses assigned to some clients.

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 on page 2 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 on page 2.

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, the switch has already been configured as follows:

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

Configuration

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

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

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

Step-by-Step Procedure To configure some allowed MAC addresses on an interface:Configure the five allowed MAC addresses on an interface:[edit ethernet-switching-options secure-access-port]user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88

Results Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 3

Verifying That Allowed MAC Addresses Are Working Correctly on the Switch

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

Action Display the MAC cache information:

```
user@switch> show ethernet-switching table
Ethernet-switching table:  6 entries, 5 learned
  VLAN                MAC address         Type         Age    Interfaces

  employee-vlan       00:05:85:3A:82:80   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:81   Learn          0    ge-0/0/2.0
  employee-vlan       00:05:85:3A:82:83   Learn          0    ge-0/0/2.0
```

```
employee-vlan       00:05:85:3A:82:85   Learn          0    ge-0/0/2.0
employee-vlan       00:05:85:3A:82:88   Learn          0    ge-0/0/2.0
employee-vlan       *                   Flood          -    ge-0/0/2.0
```

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

Related 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)