Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks

In a rogue DHCP server attack, an attacker has introduced a rogue server into the network, allowing it to give IP address leases to the network's DHCP clients and to assign itself as the gateway device.

This example describes how to configure a DHCP server interface as untrusted to protect the switch from a rogue DHCP server:

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 an untrusted DHCP server interface to mitigate rogue DHCP server attacks, be sure you have:

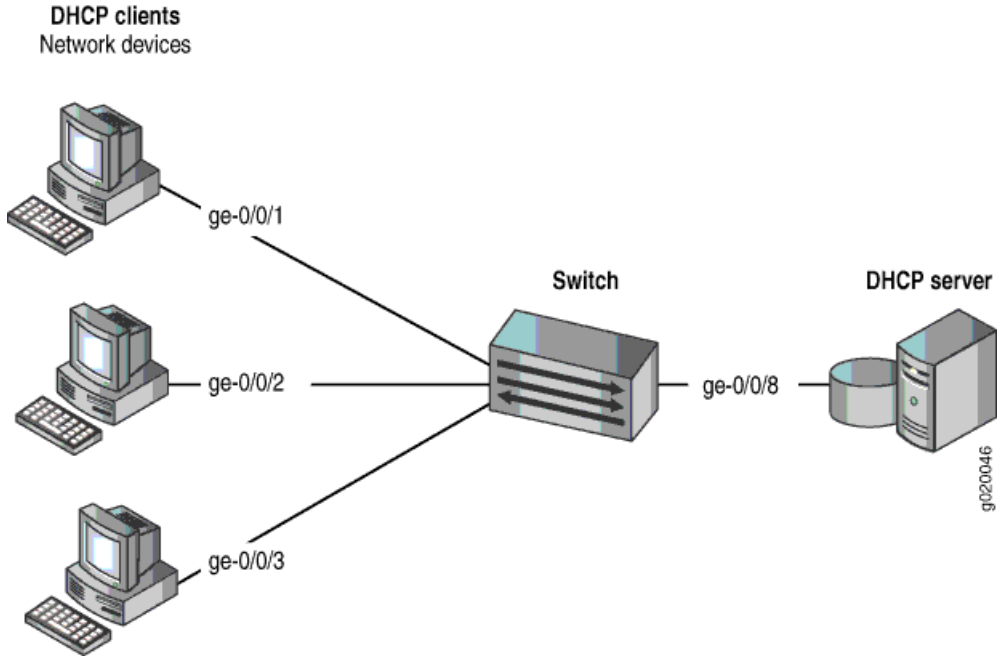
- Connected the DHCP server to the switch.
- Enabled DHCP snooping on the VLAN.
- Configured the VLAN employee-vlan on the switch. See Example: Setting Up Bridging with Multiple VLANs for EX-series Switches.

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 rogue DHCP server attacks.

This example shows how to explicitly configure an untrusted interface on an EX 3200-24P switch. 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 the 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.
- The interface (port) where the rogue DHCP server has connected to the switch is currently trusted.

Configuration

To configure the DHCP server interface as untrusted because the interface is being used by a rogue DHCP server:

CLI Quick Configuration To quickly set the rogue DHCP server interface as untrusted, copy the following command and paste it into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/8 no-dhcp-trusted
```

Step-by-Step Procedure To set the DHCP server interface as untrusted:Specify the interface (port) from which DHCP responses are not allowed:[edit ethernet-switching-options secure-access-port]user@switch# set interface ge-0/0/8 no–dhcp-trusted

Results Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/8.0 {
    no-dhcp-trusted;
}
```

Verification

To confirm that the configuration is working properly:

- Verifying That the DHCP Server Interface Is Untrusted on page 3

Verifying That the DHCP Server Interface Is Untrusted

Purpose Verify that DHCP snooping is working on the switch. See what happens when the DHCP server is untrusted.

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

Display the DHCP snooping information when the port on which the DHCP server connects to the switch is not trusted. The following output results when requests are sent from the MAC addresses but no server has provided 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      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
```

Meaning In the sample output from 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).

Related Topics

- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX-series Switch
- Enabling a Trusted DHCP Server (CLI Procedure)
- Enabling a Trusted DHCP Server (J-Web Procedure)