Understanding DHCP Snooping for Port Security on EX-series Switches

DHCP snooping allows the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. When DHCP snooping is enabled, the system builds and maintains a database of valid IP-address/MAC-address (IP-MAC) bindings called the DHCP snooping database.

DHCP Snooping Basics

Dynamic Host Configuration Protocol (DHCP) allocates IP addresses dynamically, “leasing” addresses to devices so that the addresses can be reused when no longer needed. Hosts and end devices that require IP addresses obtained through DHCP must communicate with a DHCP server across the LAN. JUNOS software for EX-series switches provides the option to apply all access-port security features by VLAN or by port (interface).

DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server (the server is connected to a trusted network port).

DHCP snooping reads the lease information from the switch (which is a DHCP client) and from this information creates the DHCP snooping database. This database is a mapping between IP address and VLAN–MAC-address pair. For each VLAN–MAC-address pair, the database stores the corresponding IP address.

When a DHCP client releases an IP address (sends a DHCPRELEASE message), the associated mapping entry is deleted from the database.

You can configure the switch to snoop DHCP server responses only from particular VLANs. Doing this prevents spoofing of DHCP server messages.

By default, all trunk ports on the switch are trusted and all access ports are untrusted for DHCP snooping. You can modify these defaults on each of the switch's interfaces.

You configure DHCP snooping for each VLAN, not for each interface (port). By default, DHCP snooping is disabled for all VLANs.

If you move a network device from one VLAN to another, typically the device has to acquire a new IP address, so its entry in the database, including the VLAN ID, is updated.

The Ethernet switching process, ESWD, maintains the timeout (lease time) value for each IP-MAC binding in its database. The lease time is assigned by the DHCP server.

The software reads the DHCP messages to obtain the lease time and deletes the associated entry from the database when the lease time expires.

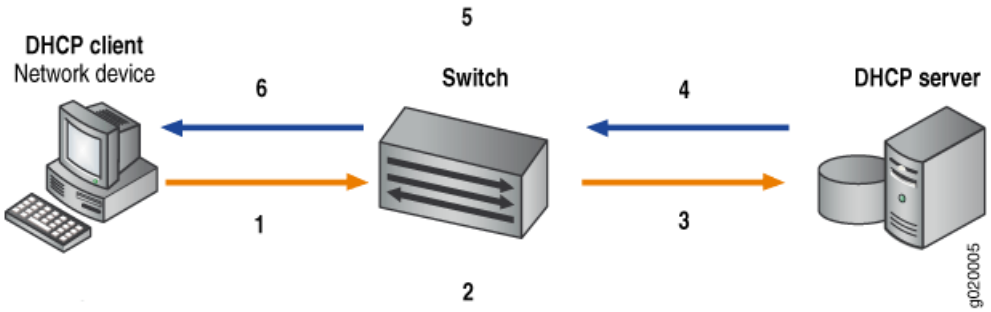
Persistence of IP-MAC Bindings

By default, the IP-MAC bindings are lost when the switch is rebooted. The DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the dhcp-snooping-file statement to store the database file either locally or remotely. See dhcp-snooping-file.

DHCP Snooping Process

The basic process of DHCP snooping is shown in Figure 1 on page 2.

Figure 1: DHCP Snooping



1. Device sends DHCPDISCOVER to request IP address or DHCPREQUEST to accept IP address and lease.
2. Switch snoops packet. Adds IP-MAC placeholder binding to database.
3. Switch forwards DHCPDISCOVER or DHCPREQUEST.
4. Server sends DHCPOFFER to offer address, DHCPACK to assign one, or DHCPNAK to deny address request.
5. Switch snoops packet. If placeholder exists, replaces it with IP-MAC binding on receipt of DHCPACK.
6. Switch forwards DHCPOFFER, DHCPACK, or DHCPNAK.

.

For general information about the messages that the DHCP client and DHCP server exchange during the assignment of an IP address for the client, see the *JUNOS Software System Basics Configuration Guide* at http://www.juniper.net/techpubs/software/junos/junos94/index.html..

DHCP Server Access

Switch access to the DHCP server can be configured in three ways:

- Switch, DHCP Clients, and DHCP Server Are All on the Same VLAN on page 3
- Switch Acts as DHCP Server on page 4
- Switch Acts as Relay Agent on page 5

Switch, DHCP Clients, and DHCP Server Are All on the Same VLAN

When the switch, DHCP clients, and DHCP server are all members of the same VLAN, the DHCP server can be connected to the switch in one of two ways:

- The server is directly connected to the same switch as the one connected to the DHCP clients (the hosts, or network devices, that are requesting IP addresses from the server). You must configure the port that connects the server to the switch as a trusted port. See Figure 2 on page 3.
- The server is directly connected to a switch that is itself directly connected through a trunk port to the switch that the DHCP clients are connected to. The trunk port is configured by default as a trusted port. The switch that the DHCP server is connected to is not configured for DHCP snooping. See Figure 3 on page 4—in the figure, ge-0/0/11 is a trusted trunk port.

Figure 2: DHCP Server Connected Directly to Switch

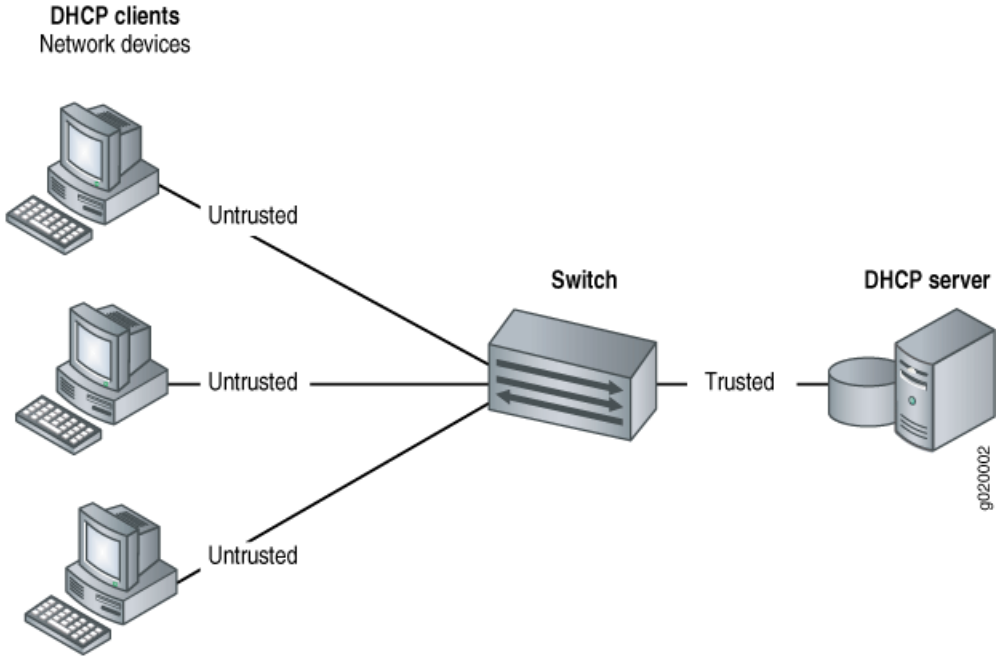
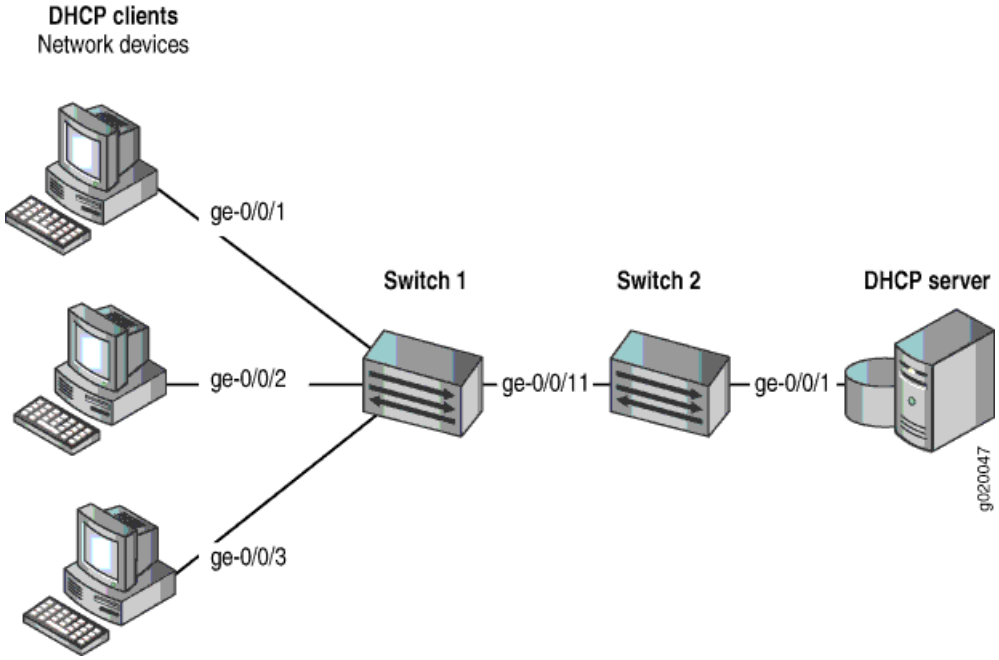


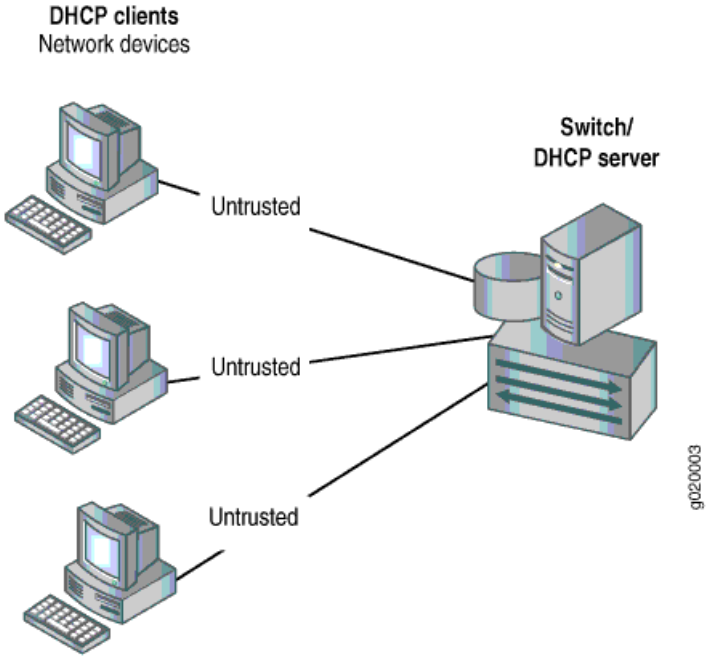
Figure 3: DHCP Server Connected Directly to Switch 2, with Switch 2 Connected to Switch 1 Through a Trusted Trunk Port



Switch Acts as DHCP Server

The switch itself is configured as a DHCP server; this is known as a “local” configuration. See Figure 4 on page 5.

Figure 4: Switch Is the DHCP Server



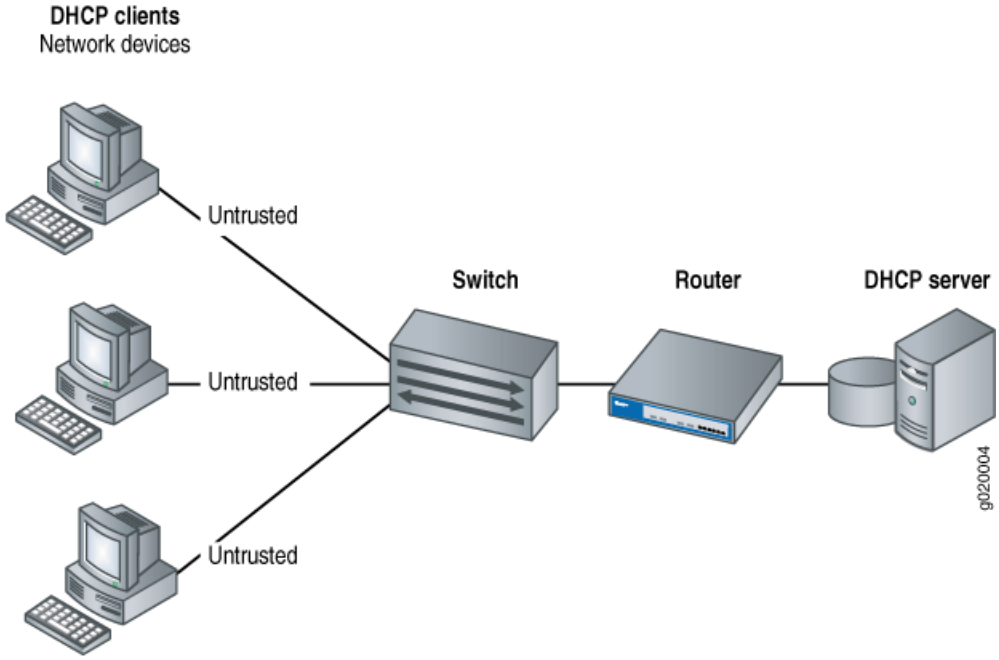
Switch Acts as Relay Agent

The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface (on the switch, these interfaces are configured as routed VLAN interfaces, or RVIs). These trunk interfaces are trusted by default.

These two scenarios illustrate the switch acting as a relay agent:

- The DHCP server and clients are in different VLANs.
- The switch is connected to a router that is in turn connected to the DHCP server. See Figure 5 on page 6.

Figure 5: Switch Acting as Relay Agent Through Router to DHCP Server



DHCP Snooping Table

The software creates a DHCP snooping information table that displays the content of the DHCP snooping database. The table shows current IP-MAC bindings, as well as lease time, type of binding, names of associated VLANs, and associated interface. To view the table, type show dhcp snooping binding at the operational mode prompt:

```
user@switch> show dhcp snooping binding
DHCP Snooping Information:
MAC address        IP address   Lease (seconds)  Type     VLAN      Interface
00:05:85:3A:82:77  192.0.2.17   600              dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:79  192.0.2.18   653              dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:80  192.0.2.19   720              dynamic  employee  ge-0/0/2.0
```

Static IP Address Additions to the DHCP Snooping Database

You can add specific static IP addresses to the database as well as have the addresses dynamically assigned through DHCP snooping. To add static IP addresses, you supply the IP address, the MAC address of the device, the interface on which the device is connected, and the VLAN with which the interface is associated. No lease time is assigned to the entry. The statically configured entry never expires.

Related Topics

- Port Security for EX-series Switches Overview
- Understanding Trusted DHCP Servers for Port Security on EX-series Switches
- Understanding DHCP Option 82 for Port Security on EX-series Switches

- DHCP Services for EX-series Switches Overview
- DHCP/BOOTP Relay for EX-series Switches Overview
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX-series Switch
- Enabling DHCP Snooping (CLI Procedure) and Enabling DHCP Snooping (J-Web Procedure)