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

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Hosts on untrusted access interfaces on Ethernet LAN switches send requests for IP addresses in order to access the Internet. The switch forwards or relays these requests to DHCP servers, and the servers send offers for IP address leases in response. Attackers can use these messages to perpetrate address spoofing and starvation.

Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client. The JUNOS software implementation of DHCP option 82 supports RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

This topic covers:

DHCP Option 82 Processing

If DHCP option 82 is enabled on the switch, then when a network device—a DHCP client—that is connected to the switch on an untrusted interface sends a DHCP request, the switch inserts information about the client's network location into the packet header of that request. The switch then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or another parameter for the client. See "Suboption Components of Option 82" on page 2 for details about option 82 information.

You can enable DHCP option 82 on a single VLAN or on all VLANs on the switch. You can also configure it on Layer 3 interfaces (in routed VLAN interfaces, or RVIs) when the switch is functioning as a relay agent.

When option 82 is enabled on the switch, then this sequence of events occurs when a DHCP client sends a DHCP request:

1. The switch receives the request and inserts the option 82 information in the packet header.
2. The switch forwards or relays the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response back to the switch. It does not alter the option 82 information.
4. The switch strips the option 82 information from the response packet.
5. The switch forwards the response packet to the client.

NOTE: To use the DHCP option 82 feature, you must ensure that the DHCP server is configured to accept option 82. If it is not configured to accept option 82, then when it receives requests containing option 82 information, it does not use the information in setting parameters and it does not echo the information in its response message. For detailed information about configuring DHCP services, see the *JUNOS Software System Basics Configuration Guide* at http://www.juniper.net/techpubs/software/junos/junos93/index.html. The configuration for DHCP service on the EX-series switch includes the dhcp statement at the [edit system services] hierarchy level.

Suboption Components of Option 82

Option 82 as implemented on the EX-series switch comprises the suboptions circuit ID, remote ID, and vendor ID. These suboptions are fields in the packet header:

- circuit ID—Identifies the circuit (interface and/or VLAN) on the switch on which the request was received. The circuit ID contains the interface name and/or VLAN name, with the two elements separated by a colon—for example, ge-0/0/10:vlan1, where ge-0/0/10 is the interface name and vlan1 is the VLAN name. If the request packet is received on a Layer 3 interface, the circuit ID is just the interface name—for example, ge-0/0/10.

  Use the prefix option to add an optional prefix to the circuit ID. If you enable the prefix option, the hostname for the switch is used as the prefix; for example, switch1:ge-0/0/10:vlan1, where switch1 is the hostname.

  You can also specify that the interface description be used rather than the interface name and/or that the VLAN ID be used rather than the VLAN name.

- remote ID—Identifies the host. By default, the remote ID is the MAC address of the switch. You can specify that the remote ID be the hostname of the switch, the interface description, or a character string of your choice. You can also add an optional prefix to the remote ID.

- vendor ID—Identifies the vendor of the host. If you specify the vendor-id option but do not enter a value, the default value Juniper is used. To specify a value, you type a character string.

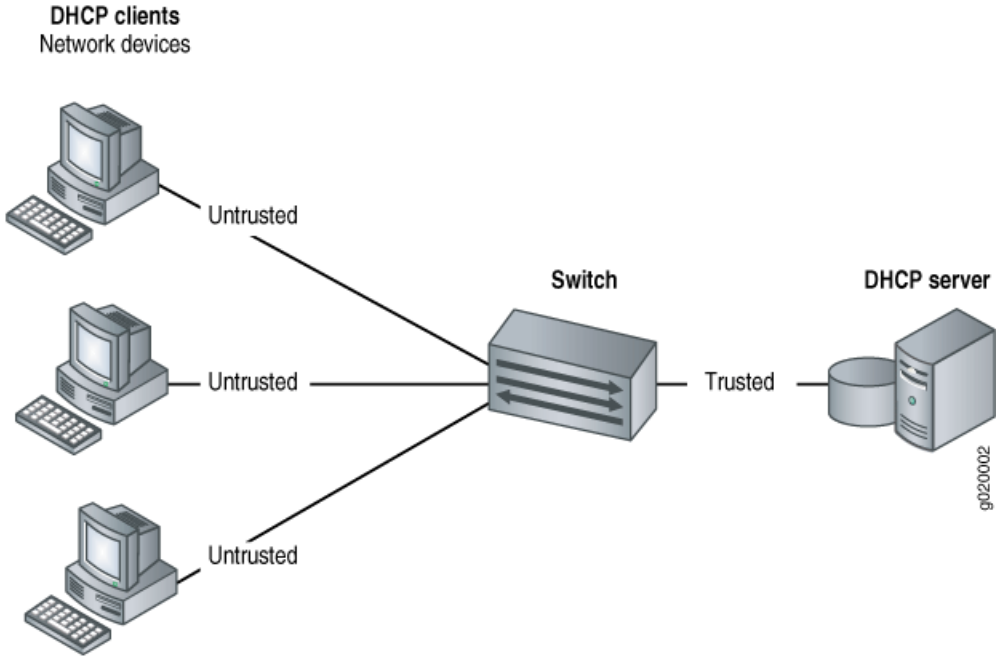
Configurations of the EX-series Switch That Support Option 82

Configurations of the EX-series switch that support option 82 are:

Switch and Clients Are on Same VLAN as DHCP Server

If the DHCP clients, the switch, and the DHCP server are all on the same VLAN, the switch forwards the requests from the clients on untrusted access interfaces to the server on a trusted interface. See Figure 1 on page 3.

Figure 1: DHCP Clients, Switch, and DHCP Server Are All on Same VLAN

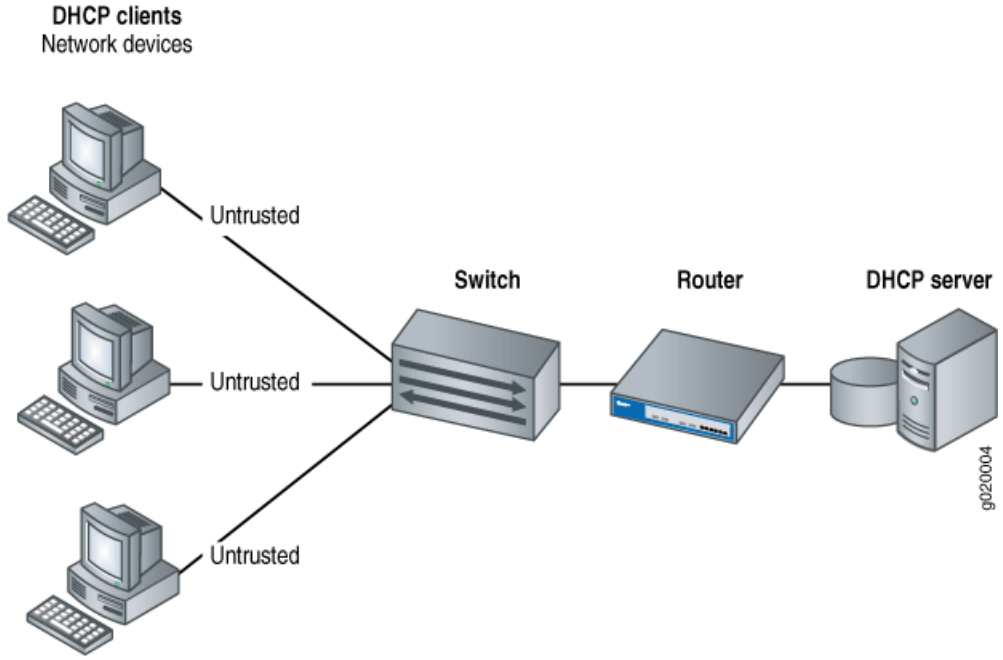


For the configuration shown in Figure 1 on page 3, you set DHCP option 82 at the [edit ethernet-switching-options secure-access-port vlan] hierarchy level.

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. Figure 2 on page 4 illustrates a scenario for the switch-as-relay-agent; in this instance, the switch relays requests through a router to the server.

Figure 2: Switch Relays DHCP Requests to Server



For the configuration shown in Figure 2 on page 4, you set DHCP option 82 at the [edit forwarding-options helpers bootp] hierarchy level.

Related Topics

- Port Security for EX-series Switches Overview
- Example: Setting Up DHCP Option 82 on an EX-series Switch with No Relay Agent Between Clients and DHCP Server
- Example: Setting Up DHCP Option 82 with an EX-series Switch as Relay Agent Between Clients and a DHCP Server
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)