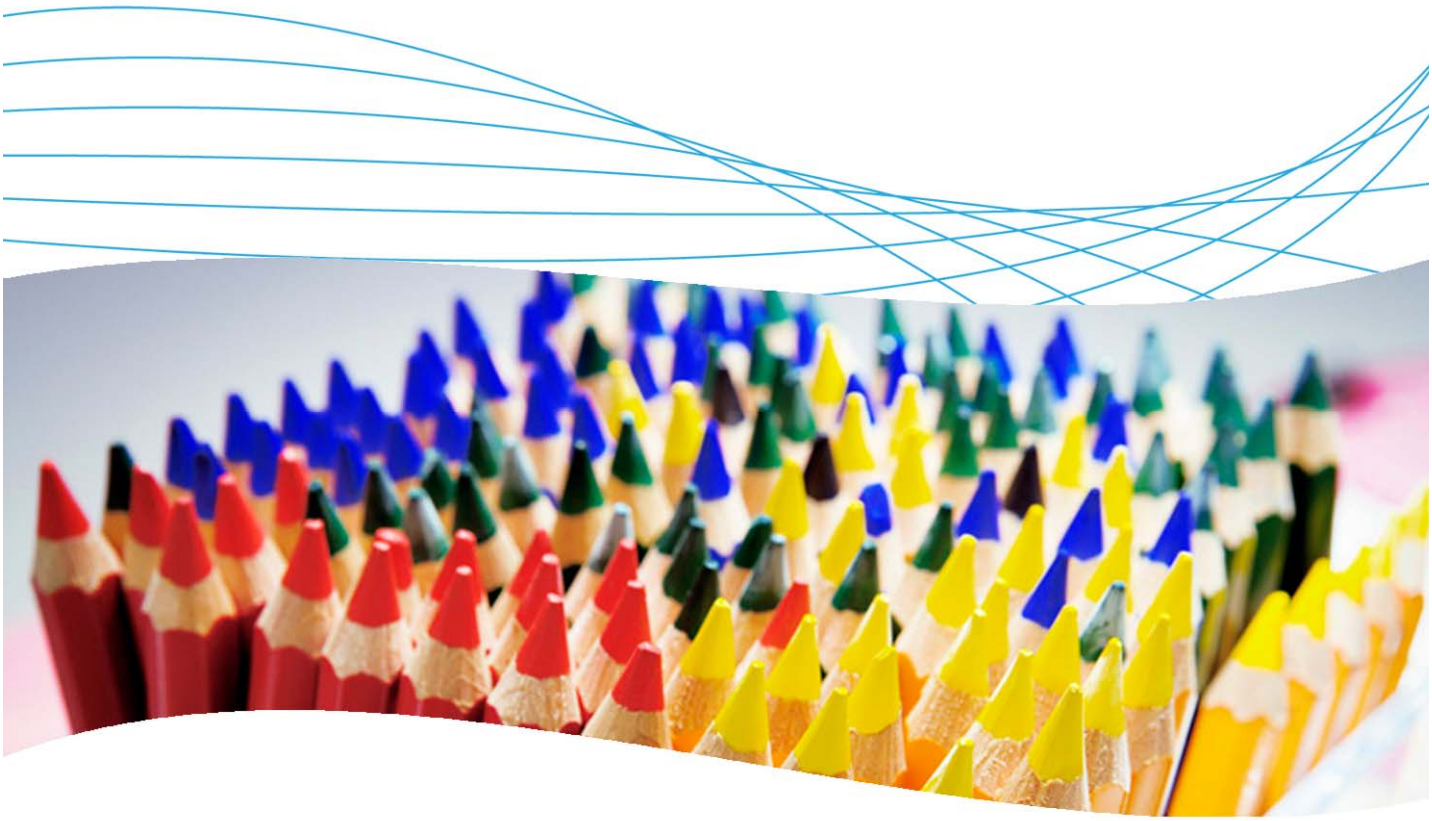
An HP ProCurve Networking Application Note

How to configure DHCP Snooping on ProCurve switches



Contents

1. Introduction

This application note explains configuration of DHCP Snooping on ProCurve ProVision switches. This feature protects the network by allowing the switches to accept DHCP responses only from authorized servers connected to trusted ports.

2. Prerequisites

You need a DHCP server, and a ProCurve ProVision switch, such as the ProCurve Switch 5400zl.

3. Network diagram

Figure 1 details the hardware configuration referenced in this application note.

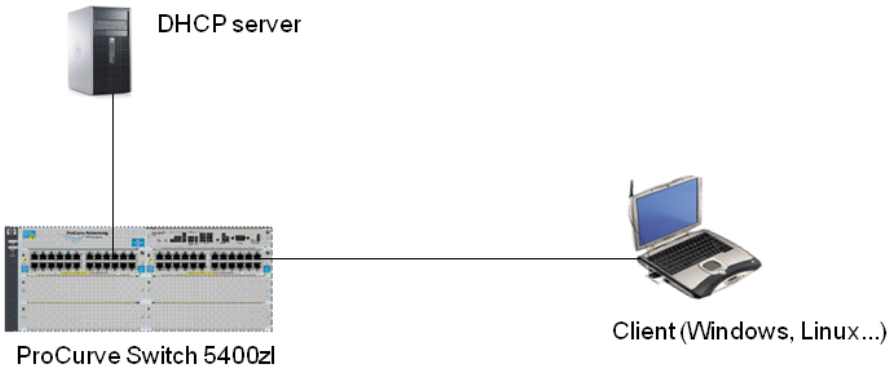


Figure 1. Setup for configuring DHCP snooping on a ProCurve switch

4. Configuring DHCP Snooping

When a DHCP client connects to the network, a DHCP broadcast request is sent across its VLAN. If a DHCP server is present on this VLAN, the server responds and allocates an IP address to the client. If there is no DHCP server on the VLAN, the switches can be configured with an ip helper-address command to relay DHCP requests to a DHCP server located in another VLAN.

But if multiple DHCP servers are present on the VLAN, you cannot control which server will answer first. Furthermore, each time the client connects, it will first try to renew its IP address from the same DHCP.

4.1 Rogue DHCP servers

The danger is that an attacker can place a “rogue” DHCP server on the network. Another possible source of false DHCP information is when a DHCP server is installed on an employee’s machine for testing purposes, and the employee forgets to disable the server before connecting the machine to the network.

If the rogue server answers DHCP requests more quickly than the corporate server, it will allocate a false address to all DHCP clients in the subnet. Clients on that subnet will either be unable to reach resources on the network, or worse, can be configured with an IP address in the correct subnet but with the wrong default gateway, so that any traffic directed to the gateway will be redirected to an attacker machine.

4.2. Configure DHCP Snooping

The DHCP Snooping feature on ProCurve ProVision switches allows you to configure switches to accept DHCP responses only from authorized servers that are connected to trusted ports.

The dhcp-snooping command configures DHCP Snooping. With this command, there are four steps to configuring DHCP Snooping on a ProCurve switch:

1. First, define a list of authorized DHCP servers (up to 20).

   Example: Define a DHCP server with IP address 10.1.1.10 as trusted:

```
5400(config)# dhcp-snooping authorized-server 10.1.1.10    Trust the DHCP server
                                                           at this address
```

2. Configure trusted ports.

   Example: Define ports 4,5,6 and 7 as trusted.

```
5400(config)# dhcp-snooping trust 4, 5, 6, 7        Trust traffic coming from
                                                     interfaces (ports) 4, 5,
                                                     6, and 7
```

3. Specify the VLAN(s) on which you want to use this feature.

   Example: Activate DHCP snooping on VLAN1, VLAN2, and VLAN3:

```
5400(config)# dhcp-snooping vlan 1-3   Activate DHCP snooping for VLAN 1, VLAN 2,
                                       and VLAN 3
```

4. Finally, activate DHCP Snooping globally.

```
5400(config)# dhcp-snooping     Activate DHCP snooping globally
```

Remember that when you have multiple switches, you must configure all of them in the same way: Trust the DHCP server, trust the port from which the DHCP offer will come, and activate DHCP snooping on the correct VLANs. Finally activate DHCP snooping globally.

As illustrated in Figure 2, with DHCP Snooping enabled on the switches, the rogue DHCP server is unauthorized and cannot send any IP addresses to the clients. The process is:

1. A laptop is plugged into the network.
2. The laptop tries to renew its “rogue” IP address but the rogue DHCP server is not trusted and cannot respond.
3. The laptop receives a reply from the Corporate DHCP server.

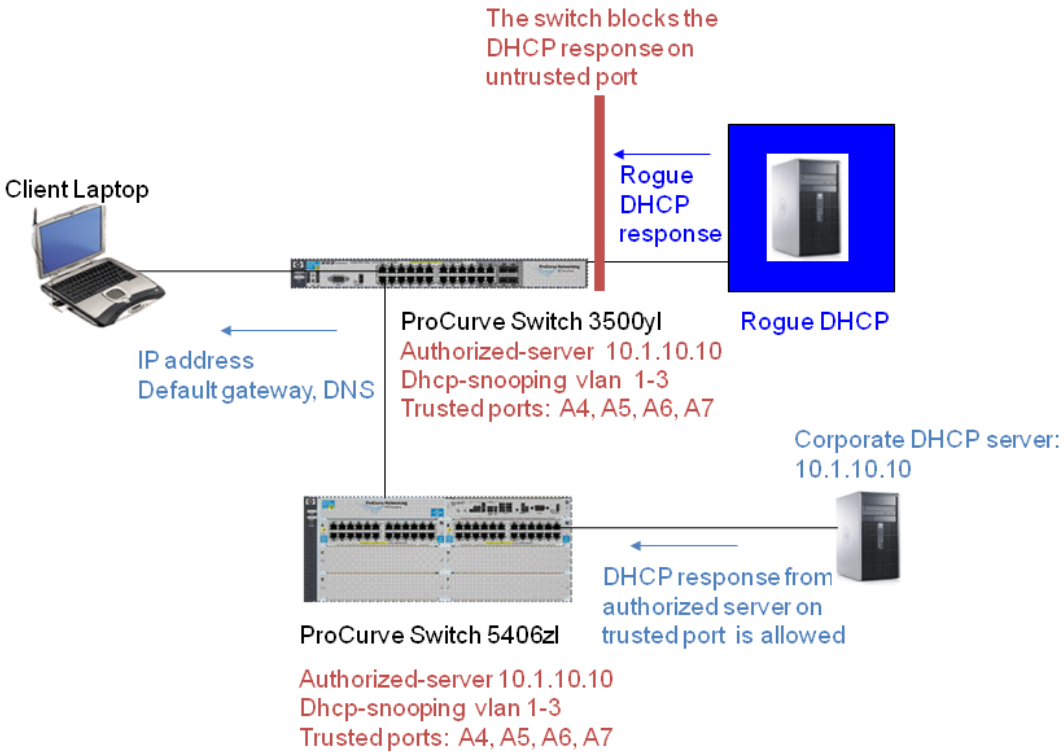


Figure 2. Using DHCP snooping to protect against rogue DHCP servers

5. Reference documents

This concludes the procedure for configuring DHCP Snooping on ProCurve switches.

For further information about how to configure ProCurve switches to support security, please refer to the following links:

- For PCM+ and IDM manuals:
  http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm
  http://www.hp.com/rnd/support/manuals/IDM.htm

- For user manuals for ProCurve 3500yl-5400zl-8212zl switches:
  http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm

- For ProCurve Switch 2610 series manuals:
  http://www.hp.com/rnd/support/manuals/2610.htm

For further information, please visit www.procurve.eu

4AA2-1720EEE, July 2008