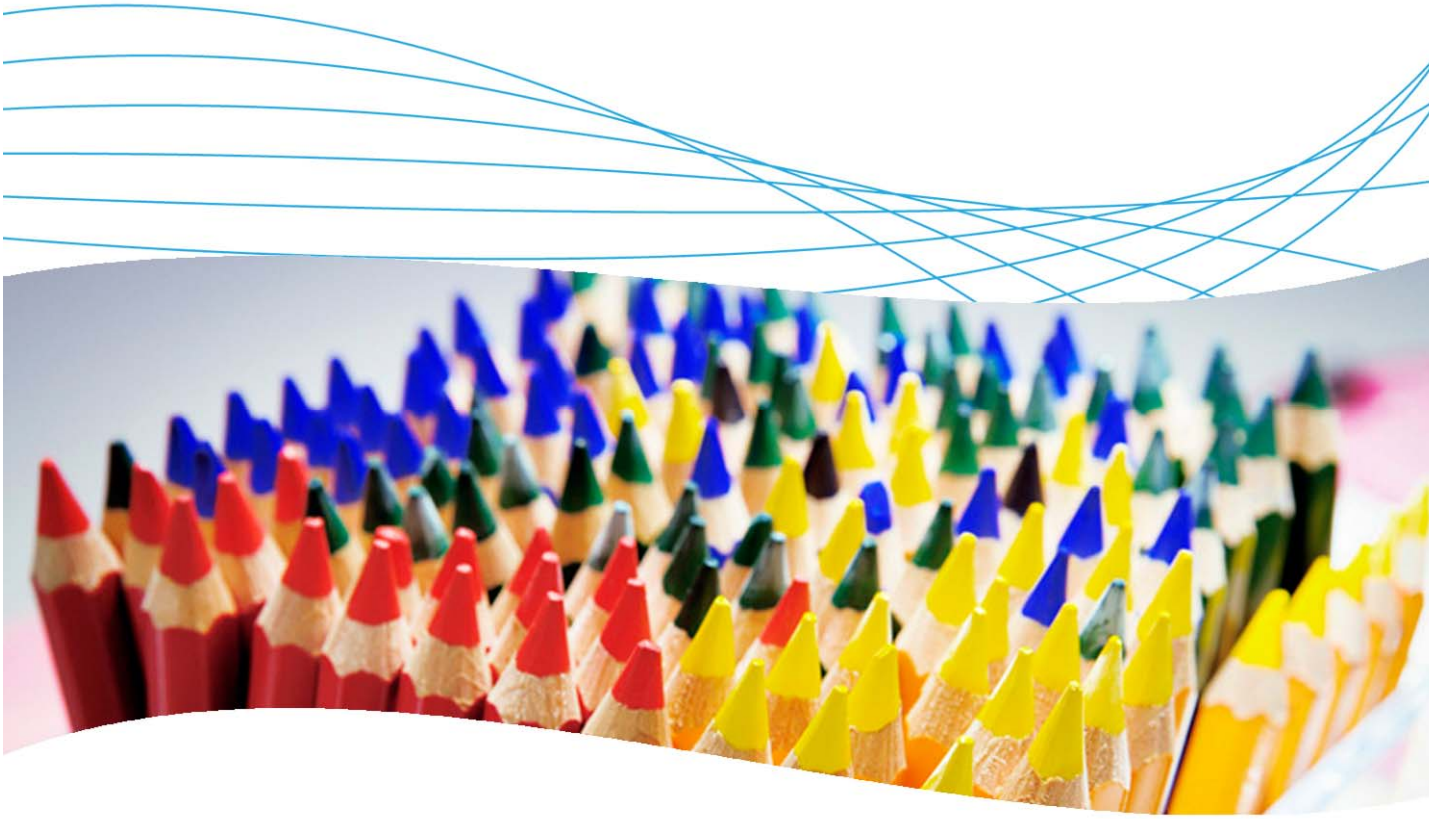
An HP ProCurve Networking Application Note

How to configure dynamic ARP protection on ProCurve switches



Contents

1. Introduction

This application note explains configuration of dynamic ARP protection on ProCurve ProVision switches. This feature protects the network by allowing the switches to verify all ARP packets arriving on untrusted ports, and to block ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data.

2. Prerequisites

You need 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 dynamic ARP protection on a ProCurve switch

4. Configuring dynamic ARP protection

Each client on a network sends ARP packets to inform the network equipment of its MAC address. Each switch maintains a table of bindings between IP addresses, MAC addresses, and ports through which this information was learned. This table of bindings is the ARP table.

4.1 ARP spoofing

When a packet from a client on the subnet is destined for a machine on another system, it is sent to the MAC address of its default gateway. The MAC address is supposed to be unique to each network interface, but in reality it can be modified easily.

An attacker begins by determining the IP address of the default gateway. This is comparatively easy to do—the attacker simply plugs in a laptop on an open port and obtains an IP address from the DHCP server. The attacker then sends to the network an ARP packet with a fake binding between its own MAC address and the IP address of the default gateway. Network switches include this wrong information in their ARP tables and transmit it to clients. Then when a client attempts to reach the default gateway, or any resource located behind it in another subnet or on the Internet, the information is sent to the attacker instead. This type of attack is known as ARP spoofing.

Consequences of ARP spoofing can include:

- Loss of connectivity to other subnets or the Internet, effectively denying service to users on the subnet.
- Compromising of confidential information, such as passwords, which are sent directly to the attacker and stolen.

With the new dynamic ARP protection on ProCurve ProVision switches, you can now configure the switches to verify all ARP packets coming in via untrusted ports, and to drop packets containing bad bindings.

4.2 Configure dynamic ARP protection

To configure dynamic ARP protection on ProCurve ProVision switches:

1. You first enable DHCP snooping.
2. Then you activate dynamic ARP protection globally.
3. You define which VLANs you want to use this feature.
4. You configure trusted ports.
5. Optionally, you can define additional checks (mac-source, mac-destination, ip).

Before configuring dynamic ARP protection, you must first enable DHCP snooping, because ARP protection uses the binding table from DHCP Snooping to determine which bindings are correct.

Here is an example of configuring dynamic ARP protection on a ProCurve Switch 3500yl:

```
3500yl (config)#dhcp-snooping           Enables DHCP snooping, to make its binding table
                                        available for dynamic ARP protection
3500yl (config)#arp-protect vlan 10     Configures ARP protection on VLAN 10
3500yl (config)#arp-protect trust 1     Configures port 1 as a trusted port
```

4.3 How dynamic ARP protection works

Figure 2 shows an example of dynamic ARP protection in action. In the illustration, port 1 on the ProCurve Switch 3500yl has been configured as a trusted port. In dynamic ARP protection, any port that connects to another switch must be defined as a trusted port using the arp-protect trust command. The switch does not check the ARP requests and responses that it receives on the trusted port.

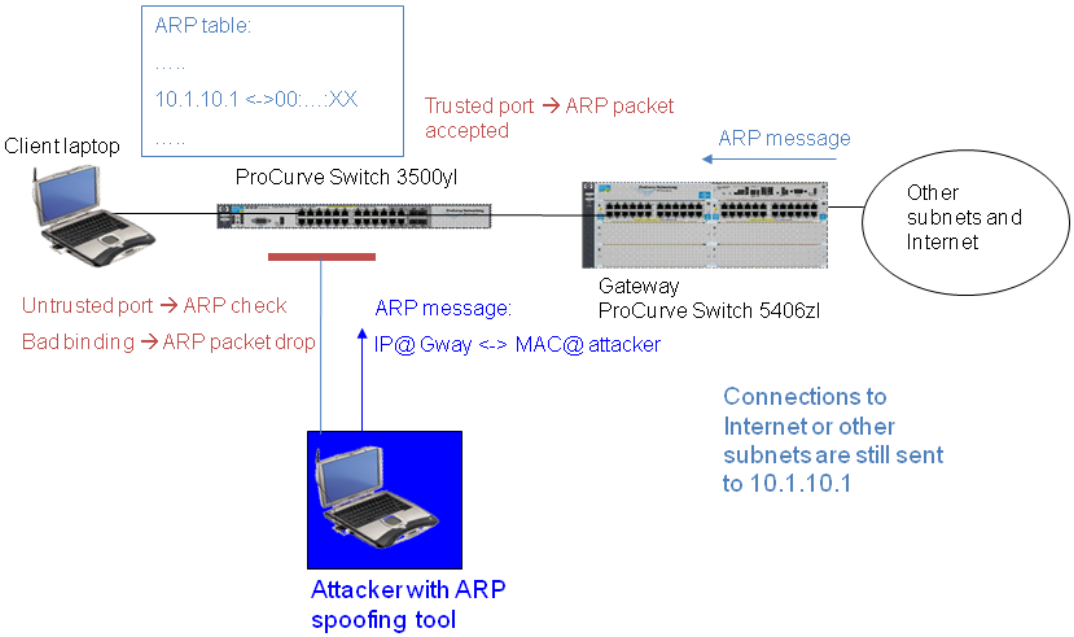


Figure 2. Configuring dynamic ARP protection causes ARP messages from an untrusted port to be checked, and dropped if the binding is bad

Untrusted ports are the ports on which users connect. By default, all ports are untrusted in the context of ARP protection. This means that the switch will check the ARP requests and responses received on all ports that are members of the ARP-protected VLANs.

If a port is untrusted, an intelligent edge switch such as the 3500yl:

- Intercepts all ARP requests and responses received on that port
- Verifies that each of the intercepted packets has a valid IP-to-MAC address binding

The switch verifies the IP-to-MAC address binding by checking the information it has stored in its DHCP snooping table. So typically you will enable DHCP snooping as part of configuring ARP protection.

If you are not using DHCP, you can configure static IP-to-MAC address bindings, and the switch will use this information to verify ARP packets. In fact, even if you are using DHCP snooping, you may want to add static IP-to-MAC address bindings to the DHCP snooping table so that the switch can verify IP-to-MAC bindings for any devices that have been assigned static IP addresses.

Packets from untrusted ports are routed according to the bindings check:

- If the binding is valid, the switch updates its local ARP cache or forwards the packet to the appropriate destination.
- If the binding is invalid, the switch simply drops the packets, preventing other devices from receiving them and being tricked by the faulty information.

In addition to verifying IP-to-MAC address bindings, you can optionally configure the switch to perform three additional checks. The switch can be configured to verify:

- The source MAC address
- The destination MAC address
- The IP address.

4.3 Repelling an attack

In an attack, the attacker sends an ARP message to the switch, supplying it with an ARP entry that resolves the IP address of the default gateway to the MAC address of the attacker. If ARP protection is not configured on the switch, the switch updates its ARP table with this new information, which means that it now has in its ARP table a false ARP entry, and all packets destined to the default gateway IP address (10.1.10.1) will be sent to the MAC address of the attacker. The consequences are that the users trying to access resources on other networks cannot reach them any more, and that the attacker can intercept the packets sent to these resources on other networks.

With dynamic ARP protection configured, however, only those packets that come in via a trusted port, or whose IP-to-MAC bindings are valid, are allowed to continue. All others are dropped. The result is that packets sent to other subnets or the Internet will indeed go out the default gateway and not to the attacker.

Note that in this illustration, you would need to configure dynamic ARP protection separately on both the 3500yl and the 5406zl switches.

5. Reference documents

This concludes the procedure for configuring dynamic ARP protection 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

4AA2-1723EEE, July 2008