Allied Telesis

AlliedWare™ OS

How To | Use DHCP Snooping and ARP Security to Block ARP Poisoning Attacks

Introduction

When you use DHCP servers to allocate IP addresses to clients on a LAN, you can also configure DHCP snooping to bolster the security on the LAN. DHCP snooping only allows clients to access the network if they have specific IP and/or MAC addresses.

With DHCP snooping, you can control access by:

- allowing only known IP addresses on the LAN
- allowing only a specific number of clients to access the LAN on any given port
- providing a record of where on the network any given IP address was in use at any given time

Through a sub-feature known as **ARP security,** DHCP snooping can also impose very strict control over what ARP packets are allowed into the network. This How To Note concentrates on this ARP security aspect of DHCP snooping, and shows how you can use it to guard against certain information-stealing attacks.

Related How To Notes

The following How To Notes give overviews and configuration guides for DHCP snooping:

- *How To Use DHCP Snooping, Option 82 and Filtering on Rapier Series Switches*
- *How To Use DHCP Snooping, Option 82 and Filtering on the x900 Series Switches*
- *How To Use MAC-Forced Forwarding with DHCP Snooping to Create Enhanced Private VLANs*
- *How To Create A Secure Network With Allied Telesis Managed Layer 3 Switches*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

Which products and software version does this apply to?

This configuration applies to the following Allied Telesis switches, running AlliedWare Software Version 2.7.6 or later:

- AT-9900 series
- AT-8948 and x900-48 series
- AT-8800 series
- AT-8600 series
- Rapier and Rapier i series
- AT-8700XL series

ARP cache poisoning

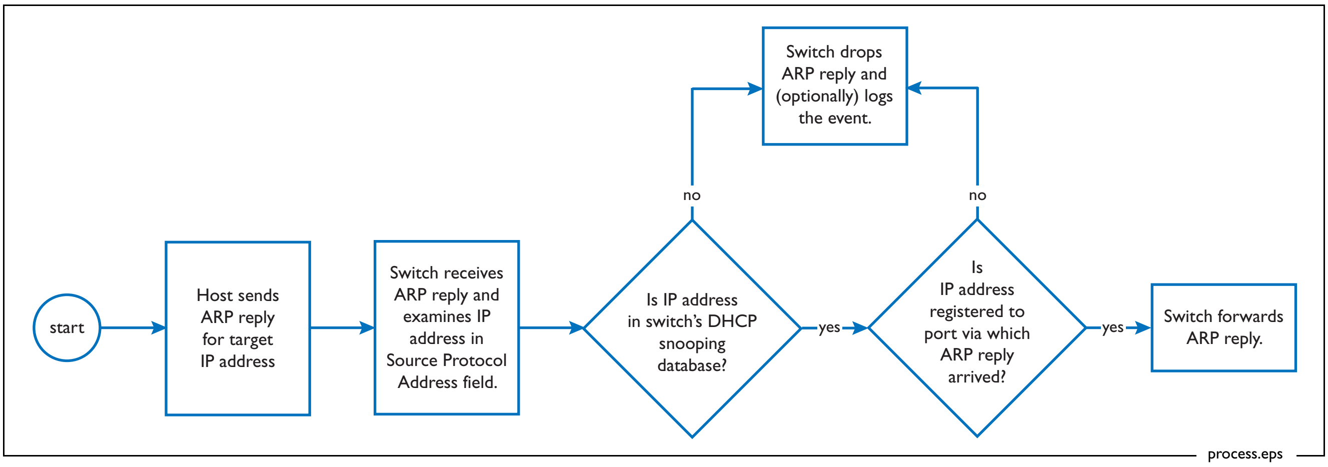
ARP cache poisoning is a tried-and-true method of stealing information on a LAN. In this process, the malicious host uses bogus ARP replies to trick other hosts into sending sensitive information to it (such as passwords).

When a host sends out an ARP request for a server, the malicious host replies to say that it possesses the server IP address that was being ARPed for. The tricked host then sends its packets to the MAC address of the malicious host, instead of sending them to the MAC address of the server. This lets the malicious host learn the usernames and passwords that are in the packets that the tricked hosts send it.

ARP cache poisoning is also called:

IP spoofing
ARP spoofing
ARP poisoning
ARP poison routing (APR)

ARP security prevents this cache poisoning. It does this by determining whether ARP replies contain legitimate IP address information and dropping replies that do not. The following figure shows the process flow.


start
Host sends ARP reply for target IP address
Switch receives ARP reply and examines IP address in Source Protocol Address field.
Is IP address in switch's DHCP snooping database?
no
yes
Switch drops ARP reply and (optionally) logs the event.
Is IP address registered to port via which ARP reply arrived?
no
yes
Switch forwards ARP reply.
process.eps

Therefore, ARP security makes it impossible for a host to poison the ARP caches of other hosts, because the switch only forwards ARP packets that have genuine information in the Source Protocol Address field.

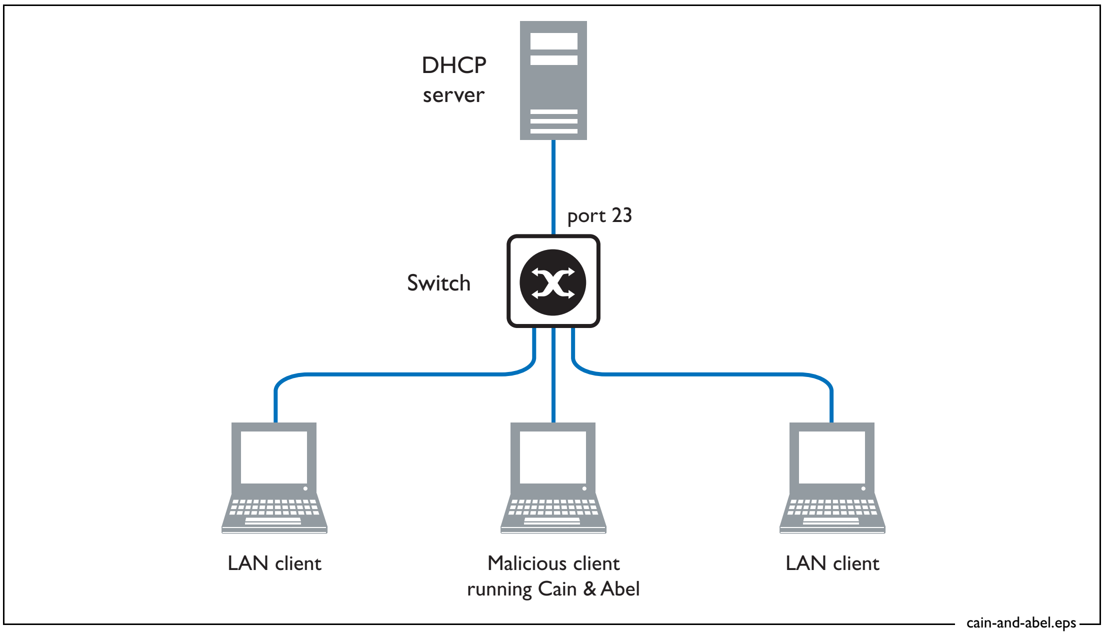
Example: Guarding against ARP poisoning by Cain & Abel

Cain & Abel is a password recovery tool for Microsoft Windows OSs. It uses a variety of methods, ranging from simple dictionary attacks to analysis of routing protocols.

It also includes ARP poison routing, which it uses to direct network traffic to its host. This enables it to sniff on a switched network by hijacking the IP traffic of multiple hosts in the same broadcast domain.

Note that ARP poisoning is only effective in a single broadcast domain, because ARP packets are not routed.

The following figure shows a simple scenario in which the operation of Cain & Abel can be observed and then blocked by ARP security.



In this scenario, the DHCP server is connected to port 23 on an AT-9924 switch, and three clients are also connected to the AT-9924 switch and receive a valid IP address from the DHCP server. Once the clients have received their DHCP leases, successful L3 connectivity can be verified by pinging from the DHCP server to each client on the LAN.

The malicious client then uses Cain & Abel to send out a bogus ARP packet.

If the switch initially has no configuration, so that it just acts as an L2 switch, then the Cain & Abel tool is quite able to go about the business of maliciously directing traffic towards itself.

Then, if the configuration in the following section is configured on the switch, this malicious behaviour is blocked (once the ARP caches on the other clients age out their bogus entries).

Configuration for AT-9900 series, x900-48 series, and AT-8948 switches

1. Configure DHCP snooping and ARP security

Use the commands:

```
enable dhcpsnooping
enable dhcpsnooping arpsecurity
```

Note that you must turn on DHCP snooping and ARP security in separate commands.

Enable logging, to record DHCP violations (see "Logging ARP poisoning attempts" on page 7). Use the command:

```
enable dhcpsnooping log=arpsecurity
```

2. Make port 23 a trusted port because the DHCP server is attached to it

Use the command:

```
set dhcpsnooping port=23 trusted=yes
```

3. Create a flow group to allow traffic that has a valid DHCP snooping address

Use the commands:

```
create classifier=1 protocol=ip ipsaddr=dhcpsn
create qos flow=1 action=forward
```

4. Create a flow group to discard all other IP traffic

Use the commands:

```
create classifier=2 protocol=ip
create qos flow=1001 action=discard
add qos flowgroup=1001 classifier=2
```

5. Create the rest of the QoS hierarchy

Use the commands:

```
create qos trafficclass=1

create qos policy=1

add qos flowgroup=1 classifier=1

add qos trafficclass=1 flowgroup=1,1001

add qos policy=1 trafficclass=1

set qos port=1-22 policy=1
```

6. Create a hardware filter to trap unicast ARP replies from Cain & Abel

When you turn on DHCP snooping, it automatically creates a hardware filter that traps broadcast ARP packets to the CPU for processing. Therefore with the above DHCP snooping and QoS configuration in place, the switch will drop invalid ARP requests broadcasted by the host running Cain & Abel.

However, on AT-8948, AT-9900 and x900-48 series switches, this filter only traps broadcast ARP packets. Cain & Abel uses unicast ARP replies in its attacks. Therefore, you need to capture unicast ARP packets as well. To do this, create the following classifier-based hardware filter:

```
create classifier=3 protocol=arp ethformat=ethii-untagged

add switch hwfilter classifier=3 action=copy,discard
```

This filter forces **all** ARP packets to the CPU (and the “discard” action ensures that they are not hardware switched). Then ARP security examines the packets, and drops any packets whose Source Protocol Address field does not hold an IP address that is currently DHCP-allocated to a client downstream of their ingress port.

Configuration for AT-8800, AT-8600, Rapier, Rapier i, and AT-8700XL series switches

Configuration on these switches is shorter, because the switch automatically creates the QoS hierarchy.

1. Configure DHCP snooping and ARP security

Use the commands:

```
enable dhcpsnooping
enable dhcpsnooping arpsecurity
enable dhcpsnooping log=arpsec
```

Note that you must turn on DHCP snooping and ARP security in separate commands.

2. Make port 23 a trusted port because the DHCP server is attached to it

Use the command:

```
set dhcpsnooping port=23 trusted=yes
```

Logging ARP poisoning attempts

It is very important to block attempted attacks on the network. It is also very useful if network administrators can be informed about the attempted attacks that were blocked. This sort of information alerts administrators to the presence of malicious hosts on their network, and gives them the opportunity to deal with those hosts in an appropriate manner.

To enable this reporting of attempted attacks, ARP security can be configured to send a log message every time it drops an ARP packet. The output of the log message is:

```
ARP Discarded, sender not found in DHCP Snoop DB src
   MAC=<MAC address>
   src IP=<Source Protocol Address found in the ARP packet>
   vlan=<VID>  port=<port that the ARP arrived on>
```

This message tells the administrator the exact location and identity of the malicious host, and the IP address of the host that it was trying to masquerade as.

To enable this logging, use the command:

```
enable dhcpshooping log=arpsecurity
```

Probably the most convenient way to make use of the log output is to send it to a syslog server. To set this up, use the commands:

```
create log output=2 destination=syslog
   server=<syslog server IP address> secure=yes

add log output=2 module=dhcpsn
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

Connecting The IP World

Allied Telesis™