ARP Spoofing

What is the ARP Protocol?

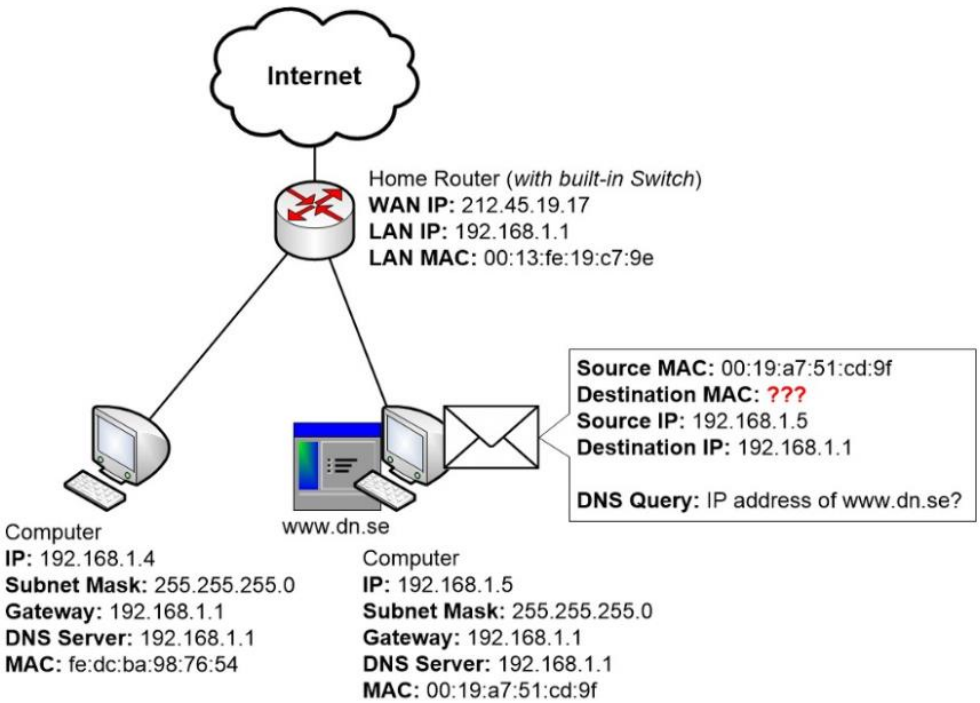
Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.

Hosts maintain an ARP cache, a mapping table between IP addresses and MAC addresses, and use it to connect to destinations on the network. If the host doesn't know the MAC address for a certain IP address, it sends out an ARP request packet, asking other machines on the network for the matching MAC address.

The ARP protocol was not designed for security, so it does not verify that a response to an ARP request really comes from an authorized party. It also lets hosts accept ARP responses even if they never sent out a request. This is a weak point in the ARP protocol, which opens the door to ARP spoofing attacks.

ARP only works with 32-bit IP addresses in the older IPv4 standard. The newer IPv6 protocol uses a different protocol, Neighbor Discovery Protocol (NDP), which is secure and uses cryptographic keys to verify host identities. However, since most of the Internet still uses the older IPv4 protocol, ARP remains in wide use.

Communication on the Internet using ARP



What is ARP Spoofing (ARP Poisoning)?

An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices. The attack works as follows:

1. The attacker gains access to the network and identifies the IP address of at least two devices on the same network.
2. The attacker then uses an ARP spoofing tool in order to send out forged ARP replies on the network which leads to ARP cache poisoning.
3. The fake ARP response convinces both devices that the MAC address of the attacker's system is the right one and thereby both devices end up connecting to that system instead of each other.
4. Once connected, the ARP cache entries are updated for all future communications and the attacker thereby gains access to any and all communications between the two devices.

How to Detect an ARP Cache Poisoning Attack?

Here is a simple way to detect that a specific device's ARP cache has been poisoned, using the command line. Start an operating system shell as an administrator. Use the following command to display the ARP table, on both Windows and Linux:

arp -a

The output will look something like this:

```
Internet Address    Physical Address

192.168.5.1         00-14-22-01-23-45

192.168.5.201       40-d4-48-cr-55-b8

192.168.5.202       00-14-22-01-23-45
```

If the table contains two different IP addresses that have the same MAC address, this indicates an ARP attack is taking place. Because the IP address 192.168.5.1 can be recognized as the router, the attacker's IP is probably 192.168.5.202.

To discover ARP spoofing in a large network and get more information about the type of communication the attacker is carrying out, you can use the open source Wireshark protocol.

ARP Spoofing Prevention

Here are a few best practices that can help you prevent ARP Spoofing on your network:

1. **Use a Virtual Private Network (VPN)—**a VPN allows devices to connect to the Internet through an encrypted tunnel. This makes all communication encrypted, and worthless for an ARP spoofing attacker.

2. **Use static ARP**—the ARP protocol lets you define a static ARP entry for an IP address, and prevent devices from listening on ARP responses for that address. For example, if a workstation always connects to the same router, you can define a static ARP entry for that router, preventing an attack.

3. **Use packet filtering—**packet filtering solutions can identify poisoned ARP packets by seeing that they contain conflicting source information, and stop them before they reach devices on your network.

4. **Run a spoofing attack**—check if your existing defenses are working by mounting a spoofing attack, in coordination with IT and security teams. If the attack succeeds, identify weak points in your defensive measures and remediate them.