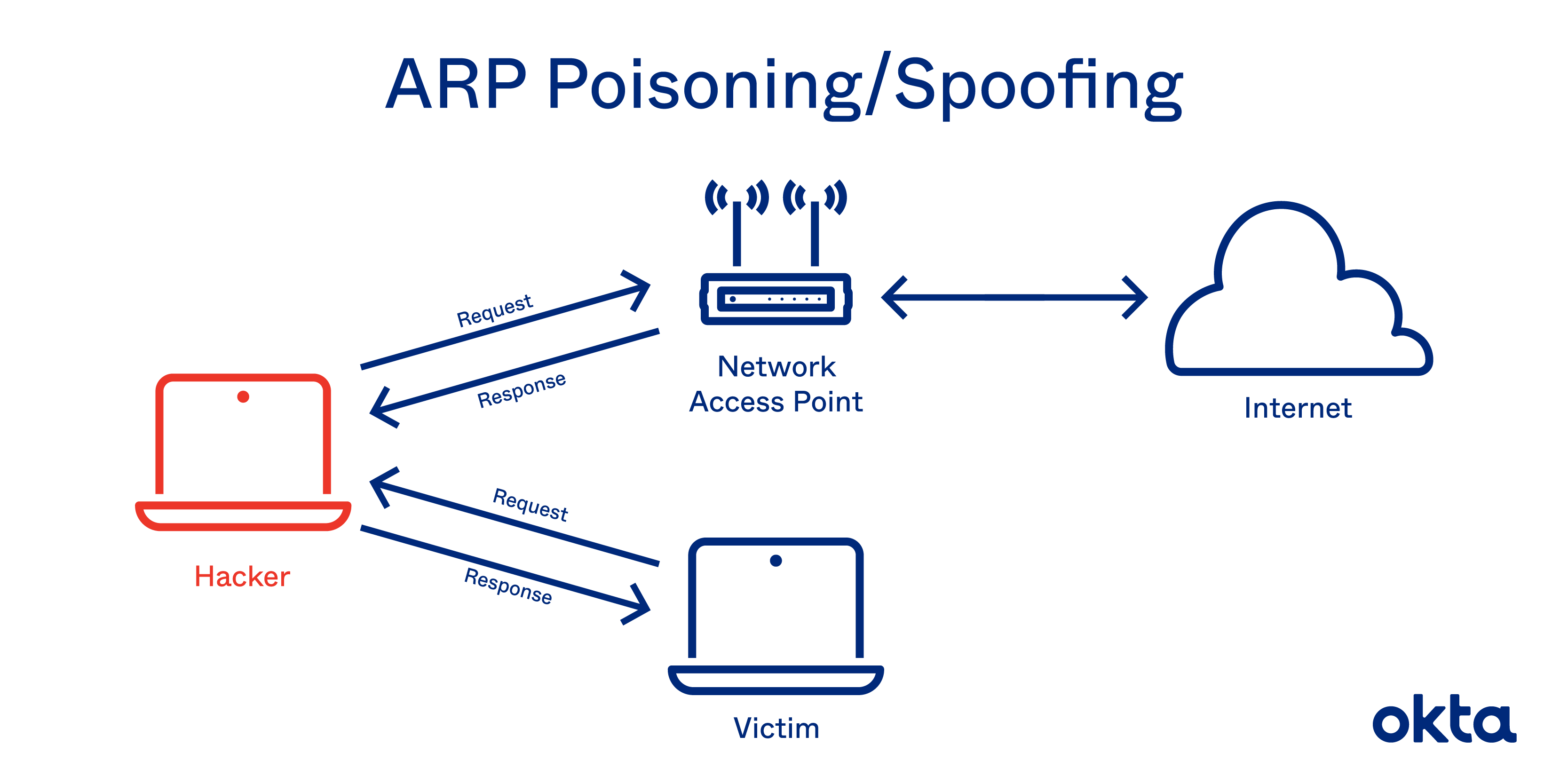
Discuss on the case studies of IP security issues and ARP poisoning attacks.  
  
**Address Resolution Protocol (ARP) spoofing** or **ARP poisoning** is a form of [spoofing attack](https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/) that hackers use to intercept data. A hacker commits an ARP spoofing attack by tricking one device into sending messages to the hacker instead of the intended recipient. This way, the hacker gains access to your device’s communications, including sensitive data such as passwords and credit card information. Luckily, you can protect yourself against these attacks in several ways.

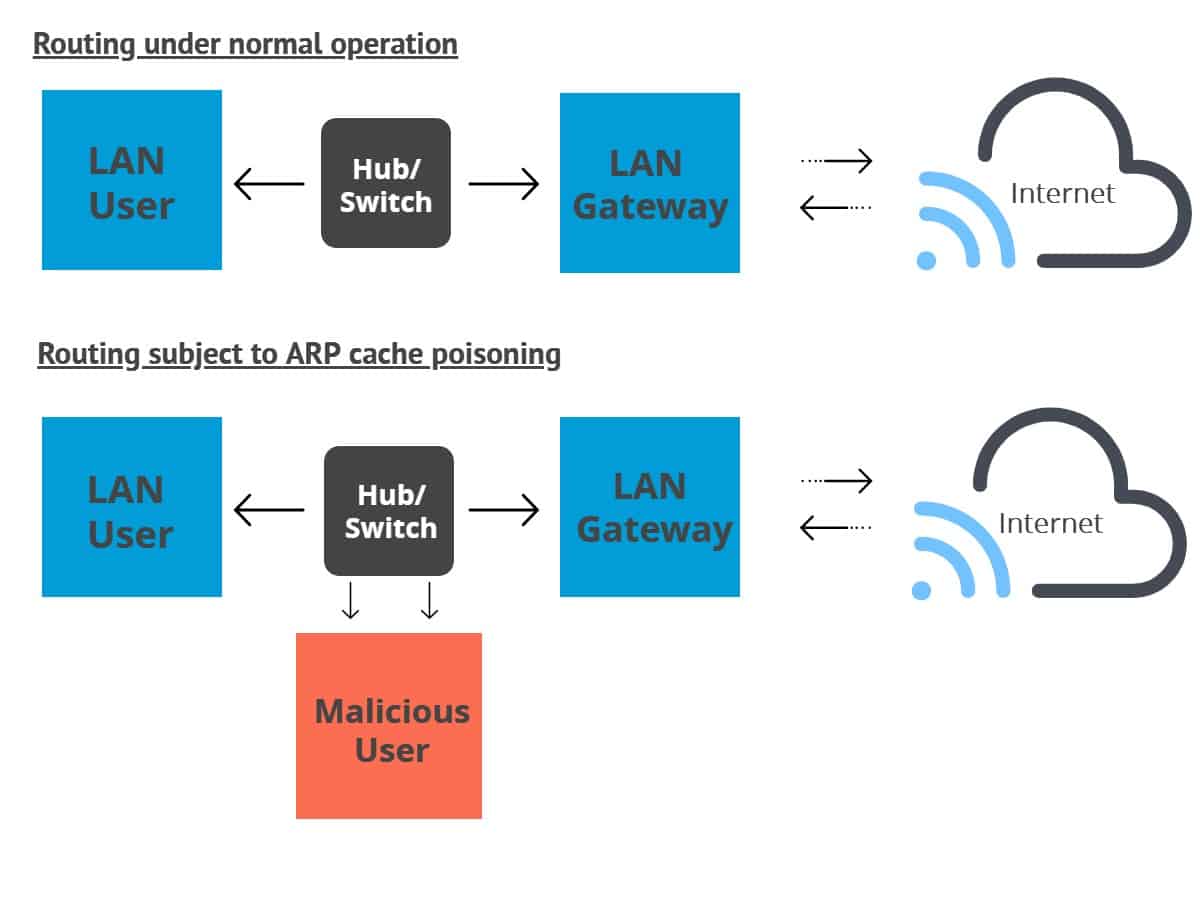


In theory, an ARP should:

* **Accept requests.**A new device asks to join the local area network (LAN), providing an IP address.
* **Translate.**Devices on the LAN don't communicate via IP address. The ARP translates the IP address to a MAC address.
* **Send requests.**If the ARP doesn't know the MAC address to use for an IP address, it sends an ARP packet request, which queries other machines on the network to get what's missing.

Two types of ARP attacks exist.

* **ARP spoofing:**A hacker sends fake ARP packets that link an attacker's MAC address with an IP of a computer already on the LAN.
* **ARP poisoning:**After a successful ARP spoofing, a hacker changes the company's ARP table, so it contains falsified MAC maps. The contagion spreads.



**Purpose of an ARP Spoof Attack**

The goal is to link a hacker's MAC with the LAN. The result means any traffic sent to the compromised LAN will head to the attacker instead.

At the end of a successful ARP attack, a hacker can:

* **Hijack.**Someone may look over everything that heads to the LAN before releasing it.
* **Deny service.**Someone may refuse to release anything from the infected LAN unless some kind of ransom is paid.
* **Sit in the middle.**Someone conducting a [man-in-the-middle attack](https://www.okta.com/video/oktane19-defending-against-identity-attacks-today-and-tomorrow/) can do almost anything, including altering documents before sending them out. These attacks both [threaten confidentiality and reduce user confidence](https://www.internetsociety.org/resources/doc/2020/fact-sheet-man-in-the-middle-attacks/). They are among the most dangerous attacks anyone can perpetrate.
* [**Distributed Denial of Service**](https://www.imperva.com/learn/application-security/denial-of-service/)**(DDoS)**⁠—the attackers can provide the MAC address of a server they wish to attack with DDoS, instead of their own machine. If they do this for a large number of IPs, the target server will be bombarded with traffic.

If a hacker wants to take over an end host, the work must be done quickly. ARP processes expire [within about 60 seconds](https://www.practicalnetworking.net/series/arp/traditional-arp/). But on a network, requests can linger for up to 4 hours. That leaves plenty of time for a hacker to both contemplate and execute an attack.

### **How to Tell if Someone is Spoofing Your ARP**

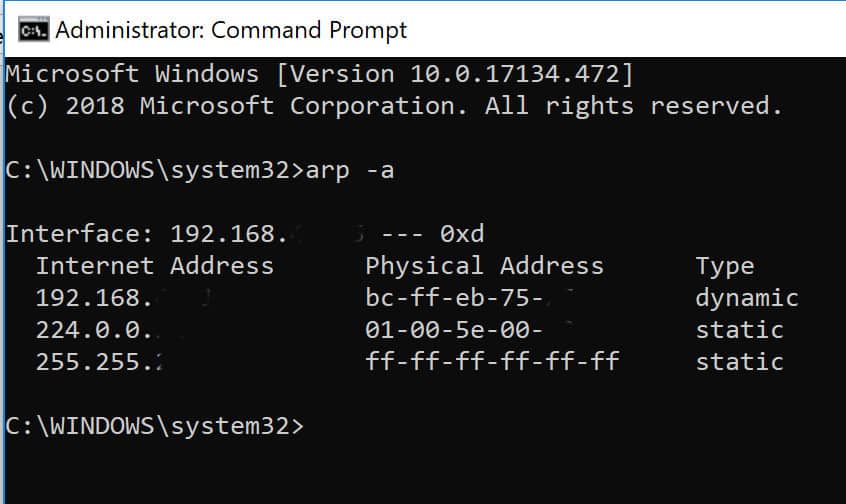
To tell if you’re being spoofed, check your task automation and configuration management program. Here, you will be able to find your ARP cache. If there are two IP addresses with the same MAC address, you might be the victim of an attack. Hackers typically use a spoofing software that sends messages stating that its address is the default gateway’s.

Type in “**cmd**”, then press **Crtl**, **Shift** and **Enter**at the same time.

This will bring up Command Prompt, although you may have to click **Yes** to give the app permission to make changes. In the command line, enter:

**arp -a**

This will give you the ARP table:

[](https://cdn.comparitech.com/wp-content/uploads/2019/01/arp-poisoning-1.jpg)

## ARP Poisoning Attack Prevention

Network administrators can use [two techniques](https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.49) to detect ARP spoofing.

1. **Passive:**Monitor ARP traffic and look for mapping inconsistencies.
2. **Active:**Inject falsified ARP packets into the network. A spoofing attack like this helps you identify weak points in your system. Remediate them quickly, and you could stop an attack in progress.

[Use of a VPN](https://www.okta.com/blog/2018/04/how-secure-is-your-vpn/) could be an exceptional source of protection. Devices connect through an encrypted tunnel, and all communication is immediately encrypted.

Protection Tools to Consider

Plenty of companies provide monitoring programs you can use to both oversee your network and spot ARP problems.

These are common solutions:

* [**Arpwatch**](https://www.tecmint.com/monitor-ethernet-activity-in-linux/)**:**Monitor ethernet activity, including changing IP and MAC addresses, via this Linux tool. Look over the log every day, and access timestamps to understand just when the attack happened.
* [**ARP-GUARD**](https://www.arp-guard.com/download/info/datasheet/arp-guard-datasheet-current.pdf.en)**:**Tap into a graphic overview of your existing network, including illustrations of switches and routers. Allow the program to develop an understanding of what devices are on your network and build rules to control future connections.
* [**XArp**](http://www.xarp.net/)**:**Use this tool to detect attacks happening below your firewall. Get notified as soon as an attack begins, and use the tool to determine what to do next.
* [**Wireshark**](https://www.wireshark.org/)**:**Use this tool to develop a graphic understanding of all the devices on your network. This tool is powerful, but you may need advanced skills to implement it properly.
* **Packet filtering:**Use this firewall technique to manage network access by monitoring incoming and outgoing IP packets. Packets are allowed or stopped based on source and destination IP addresses, ports, and protocols.
* **Static ARP:**These ARPs are added to the cache and retained on a permanent basis. These will serve as permanent mappings between MAC addresses and IP addresses.