**ARP Spoofing**

**Other names: ARP cache poisoning, or ARP poison routing, ARP poisoning**

**Description 1**

**ARP spoofing** is a technique by which an attacker sends ([spoofed](https://en.wikipedia.org/wiki/Spoofing_attack)) [Address Resolution Protocol](https://en.wikipedia.org/wiki/Address_Resolution_Protocol) (ARP) messages onto a [local area network](https://en.wikipedia.org/wiki/Local_area_network). Generally, the aim is to associate the attacker's [MAC address](https://en.wikipedia.org/wiki/MAC_address) with the [IP address](https://en.wikipedia.org/wiki/IP_address) of another [host](https://en.wikipedia.org/wiki/Host_(network)), such as the [default gateway](https://en.wikipedia.org/wiki/Default_gateway), causing any traffic meant for that IP address to be sent to the attacker instead. ARP spoofing may allow an attacker to intercept [data frames](https://en.wikipedia.org/wiki/Data_frame) on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as [denial of service](https://en.wikipedia.org/wiki/Denial_of_service), [man in the middle](https://en.wikipedia.org/wiki/Man-in-the-middle_attack), or [session hijacking](https://en.wikipedia.org/wiki/Session_hijacking) attacks. [1][3]

**Description 2**

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker’s MAC address with the IP address of a legitimate computer or server on the network. Once the attacker’s MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. **ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit**. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

In their most basic application, ARP spoofing attacks are used **to steal sensitive information**. Beyond this, ARP spoofing attacks are often used **to facilitate other attacks such as**:

* Denial-of-service attacks: DoS attacks often leverage ARP spoofing to link multiple IP addresses with a single target’s MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target’s MAC address, overloading the target with traffic.
* Session hijacking: Session hijacking attacks can use ARP spoofing to steal session IDs, granting attackers access to private systems and data.
* Man-in-the-middle attacks: MITM attacks can rely on ARP spoofing to intercept and modify traffic between victims. [2]

**More About consequences**

Consequences of ARP spoofing are similar to MAC and IP spoofing and DNS poisoning.

**Description 3**

**Other names: ARP Poisoning, Man In the Middle Attack**

A Man-In-The-Middle (MITM) attack is achieved when an attacker poisons the ARP cache of two devices with the (48-bit) MAC address of their Ethernet NIC (Network Interface Card). Once the ARP cache has been successfully poisoned, each of the victim devices send all their packets to the attacker when communicating to the other device. This puts the attacker in the middle of the communications path between the two victim devices; hence the name Man-In-The-Middle (MITM) attack. **It allows an attacker to easily monitor all communication between victim devices.** **The objective of this this attack is to take over a session. The intent is to intercept and view the information being passed between the two victim devices. [4]**

**Reference**

[1] Ramachandran, Vivek, and Sukumar Nandi. "Detecting ARP spoofing: An active technique." *International Conference on Information Systems Security*. Springer Berlin Heidelberg, 2005.

[2] <https://www.veracode.com/security/arp-spoofing>

[3] <https://en.wikipedia.org/wiki/ARP_spoofing>

[4] http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white\_paper\_c11\_603839.html