# ARP Poisoning

# ARP Poisoning

ARP spoofing is a type of attack in which a malicious attacker 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.

# Attacks

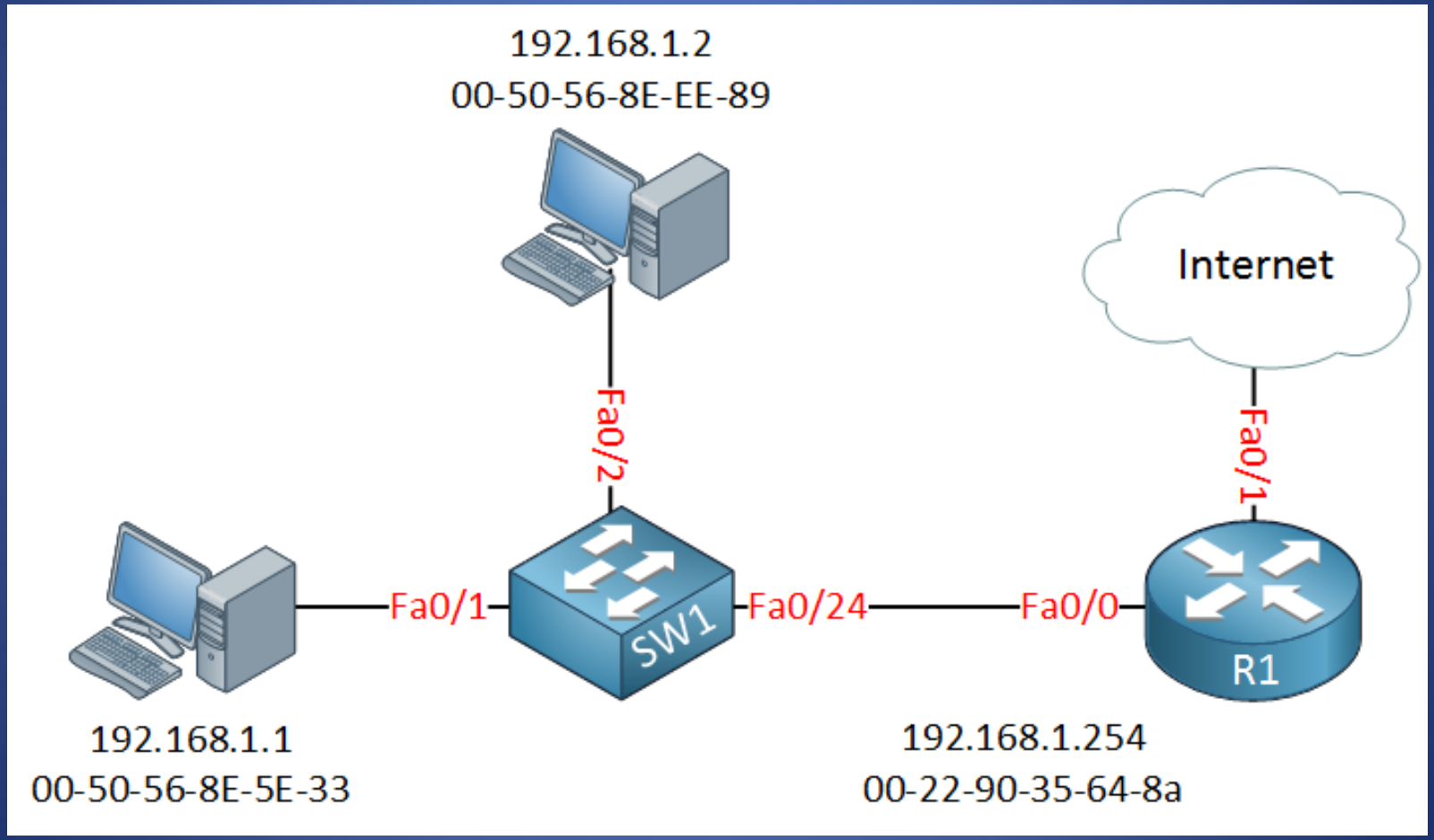
- Denial-of-service attacks: DoS attacks often leverage ARP spoofing to link multiple IP addresses with a single target's MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target's MAC address, overloading the target with traffic.
- Session hijacking: 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.

# Example

An attacker may want to see the traffic between victim computer, 192.168.1.1, and the internet router 192.168.1.254. The attacker begins by sending malicious ARP reply to the router, associating his/her MAC address with 192.168.1.1. The router confuses attacker's computer with the victim's computer.

Then the attacker sends a malicious ARP reply to the computer, associating his/her MAC address with 192.168.1.254. The victim's machine thinks the attacker's computer is the router. Finally attacker enables operating system feature called IP forwarding to forward any network traffic it receives from victim's computer to router.

# Example


192.168.1.2
00-50-56-8E-EE-89
Internet
Fa0/2
Fa0/1
Fa0/1
SW1
Fa0/24
Fa0/0
R1
192.168.1.1
00-50-56-8E-5E-33
192.168.1.254
00-22-90-35-64-8a