Q2) Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.

ARP spoofing is a **Man-in-the-Middle (MITM) attack** where a malicious device sends fake ARP replies to associate its MAC address with the IP address of a legitimate device, such as a gateway or another host. This allows the attacker to intercept, modify, or redirect network traffic. Since ARP is a stateless protocol that does not validate responses, devices accept the forged entries, enabling unauthorized data interception and manipulation.

Effects of ARP Spoofing on Network Devices

When a device receives a malicious ARP response, it updates its ARP table with incorrect MAC-IP mappings. This leads to:

- **Traffic Redirection:** Data meant for a legitimate device is sent to the attacker.
- **Session Hijacking:** Attackers can steal login credentials or sensitive information.
- **Denial of Service (DoS):** If the attacker drops packets instead of forwarding them, communication breaks down.
- **Network Instability:** Continuous ARP spoofing can cause unpredictable network behavior.

Preventing ARP Spoofing

- **Use Dynamic ARP Inspection (DAI)** on managed switches to filter out spoofed ARP packets.
- **Enable port security** on switches to limit allowed MAC addresses per port.
- **Use static ARP entries** on critical devices like routers and servers.
- **Deploy security tools** like ARP spoofing detection systems (`arpwatch` or `XArp`).

ARP spoofing is a dangerous attack that exploits vulnerabilities in the ARP protocol. By simulating this attack in Packet Tracer, we can understand how malicious ARP replies manipulate network behavior and how attackers intercept traffic. Implementing security measures such as **DAI, static ARP mappings, and intrusion detection** can help mitigate these risks. Understanding and analyzing ARP spoofing is essential for securing enterprise networks against **MITM attacks** and **data breaches**.