**Q.2 What are potential security issues with ARP?**

Ans- There are mainly two types of security issues with ARP:-

1. ARP Spoofing
2. ARP Poisoning

**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.

**Prevention-**

**ARP spoofing detection software: Utilize** specialized software or intrusion detection systems (IDS) that can monitor ARP traffic and detect anomalies indicative of ARP spoofing attacks. These tools can alert administrators in real-time when suspicious ARP activity is detected.

**Port security:** Implement port security features on network switches to restrict the number of MAC addresses allowed on a port. This prevents attackers from connecting unauthorized devices to the network and launching ARP spoofing attacks.

**Network segmentation:** Divide the network into smaller segments using VLANs (Virtual Local Area Networks) or subnetting. This limits the scope of ARP spoofing attacks by isolating sensitive devices and traffic within separate network segments.

**Network encryption:** Implement encryption protocols such as IPsec (Internet Protocol Security) to encrypt communication between network devices. This prevents attackers from intercepting and tampering with sensitive data transmitted over the network.

**Regular network monitoring:** Continuously monitor network traffic and logs for signs of ARP spoofing activity. Analyze ARP tables, network traffic patterns, and ARP request/response packets for any abnormalities that may indicate an ongoing attack.

**Strong network access controls:** Enforce strong authentication mechanisms, such as IEEE 802.1X authentication, to control access to the network. Require users and devices to authenticate before being granted access, reducing the likelihood of unauthorized devices conducting ARP spoofing attacks.