Address Resolution Protocol (ARP) is a protocol used to map IP addresses to MAC addresses in a network. It helps when one device wants to communicate with another device in the network.

Working of ARP:

1) In a situation where device 1 wants to communicate to device 2, it first checks whether the MAC address of device 2 is present in the ARP cache of device 1.
2) If it is present then it directly communicates with device 2 using the MAC address of that device.
3) If it is not present then device 1 will broadcast an ARP request message to all the devices in the network. The message will contain device 1's ip address , MAC address and ip address of device 2.
4) All devices will check whether their ip address matches with destination address in the broadcast message. If it does not match they will drop it.
5) When the packet reaches device 2 it will draft an ARP reply message add its ip and MAC address to the message and send it only to device 1.
6) Device 1 will receive the ARP reply message and update its ARP cache accordingly and start communication with device 2.

ARP Spoofing:

In this scenario an attacker sends ARP packets over the local network which contains the Hacker's MAC Address and the target's IP address. This results in other nodes in the network updating their ARP cache. Whenever a node in the network wants to send a message to the target , the packet will be sent to the attacker instead.