Address Resolution Protocol(ARP)

When a device sends a frame(in layer 2), its header contains two address fields: destination MAC and source MAC addresses. When multiple host devices are connected in a local network, they have to use each other's MAC addresses to communicate. End devices use the ARP to translate IP addresses to MAC addresses. Moreover, ARP makes a table of IPv4 to MAC address mappings. When transmitting data in the same network, the device will look up the MAC address in its own ARP table, but when transmitting it in another network, the device will search for it in the default gateway’s ARP table. The ARP request header contains the Destination MAC address, which is the broadcast MAC address(FF-FF-FF-FF-FF-FF), the source MAC address, and the type, which indicates that the frame has to pass the ARP process. Only one of the devices in the network will match the IP address with its own; others will drop the frame. And that device will generate an ARP reply message, which will contain the destination MAC address, source MAC address (the one we have been looking for), and the type field. The MAC addresses will be saved in the ARP tables of both requesting and replying devices, and there will be no need to send a broadcast message to find the MAC addresses of those devices. This will lower the traffic in the network.

Though ARP is a crucial protocol, it has a few drawbacks. One is that ARP requests are broadcast; when a large number of devices are booted at the same time, it can reduce the performance of the network. In addition, threat actors can use ARP spoofing and perform ARP poisoning attacks. They reply to the ARP request and pretend to be the default gateway. The ARP function is in layer 2 of the OSI model.