

Forum:[Hack Forums](#)

Thread: [\[Sui Generis\] The Address Resolution Protocol \(ARP\) Explained](#)

Toast - June 26, 2019, 4:20 pm

Every device with an IP address (Layer 3 address) also has a MAC address (Layer 2 address). When a device sends an Ethernet frame, it contains two addresses: Destination MAC address and Source MAC Address. Destination Mac Address, which will be either the MAC address of the final destination device or the router.

Source MAC Address, which will be the MAC address of the sender's Ethernet NIC

To determine the destination MAC address, the device uses ARP, which provides two basic functions: Resolving IP addresses to MAC addresses

Maintaining a table of mappings

When a packet is sent to the data link layer to be encapsulated into an Ethernet frame, the device refers to a table in its memory to find the MAC address that is associated with the IPv4 address. This table is called the ARP table or the ARP cache. It is stored in the RAM of the device.

The sending device will search inside its ARP table for the destination IPv4 address and a corresponding MAC address. If the packet's destination IPv4 address is on the same network as the source IPv4 address, it will search the table for the destination IPv4 address, and the MAC address associated with it.

If the packet's destination IPv4 address is not on the same network as the source IPv4 address, then it will search the table for the IPv4 address of the default gateway, and the MAC address associated with it.

Each entry of the table binds an IPv4 address and a corresponding MAC address. The ARP table temporarily caches the mapping for the devices on the LAN.

If the device can find an entry for the IPv4 address, then it uses the MAC address associated with it as the destination MAC address. If not, then the device sends an ARP request

ARP messages are encapsulated directly in an Ethernet frame, without an IPv4 header. An ARP request includes the Target IPv4 address and the Target MAC Address. The target IPv4 address is the IPv4 address that requires a corresponding MAC address.

The target MAC address is the unknown MAC address, and it will be empty in the ARP request message.

The Ethernet frame in which the ARP request is encapsulated uses the following header information: Destination MAC Address, which is set to the broadcast address (FF:FF:FF:FF:FF:FF)

Source MAC Address, which is the MAC address of the sending device

Type, which is set to 0x806. This informs the receiving NIC that the data portion of the frame needs to be passed to the ARP process

Since ARP requests are broadcast, they are sent out all ports of the switch, except for the one it came through. All Ethernet NICs on the LAN will process the ARP request to check if the target IPv4 address matches their own, and only one device will have the IPv4 address that matches the Target IPv4 address, so only one device will reply. (Routers will not forward broadcasts out other

interfaces)

The device that has the matching IPv4 will then send an ARP reply, which includes: Sender's IPv4 address, which is the IPv4 address of the sender (the device whose MAC was requested)

Sender's MAC Address, which is the MAC address of the sender (the MAC address needed by the sender of the ARP request)

The ARP reply is also encapsulated in an Ethernet frame with the following header information: Destination MAC Address, which is the MAC address of the sender of the ARP request

Source MAC address, which is the MAC address of the sender of the ARP reply

Type, which is once again set to 0x806 .

Note that the ARP reply is not a broadcast, like the ARP request. It is a unicast, which means only the device that sent the ARP request will receive the ARP reply.

Once the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table. Now, packets destined for that IPv4 address can be encapsulated in frames using its corresponding MAC address.

If no device responds to the ARP request, then the packet is dropped, because a frame cannot be created.

Each entry in an ARP table is time stamped. If a device does not receive a frame from a device inside the ARP table by the time the time stamp expires, the entry for that device is removed from the ARP table.

Static map entries, which do not expire in time and need to be manually removed, can be entered in the ARP table, but that is rarely done.

If the packet's destination IPv4 address is not in the same network, then the source device needs to send the frame to its default gateway, which is the interface of the local router. When a device has a packet with the destination in another network, it encapsulates that packet in a frame, using the destination MAC address of the router interface.

The device checks its ARP table for the MAC address of the default gateway. If it finds it, then the frame headers are set to the required information, and the packet is sent to the router to be forwarded out the correct interface. If it does not find a match in its routing table, then it sends an ARP request, and waits for an ARP reply to complete the header information on the frame.

The application of this in a hacking scenario is called ARP cache poisoning / ARP spoofing / Man In The Middle (MITM).

To pull this off, an attacker will reply to an ARP request for the IPv4 address that belongs to the default gateway. The attacker sends an ARP reply with its own MAC address, and the receiver of the ARP reply will add the wrong MAC address to its ARP table, and send packets to the attacker.

virus - June 26, 2019, 4:22 pm

Well written thread Toast. More is coming from Sui Generis. ?

Mad76e. - June 27, 2019, 3:13 pm

Very nice! I liked this one a lot :)