ARP

* What is the purpose of ARP ?

The purpose of ARP, which stands for Address Resolution Protocol, is to map an IP address to a physical hardware address (usually a MAC address) on a local network. ARP is primarily used in Ethernet and other local area networks where devices need to communicate with each other.

Although, ARP plays a crucial role in local network communication by allowing devices to discover each other's MAC addresses when they know each other's IP addresses. This enables the correct routing of data packets within a local network, facilitating effective and efficient communication between devices.

* What are the ARP Request Packet's Source and destination IP addresses?

The source IP address in an ARP request packet is the IP address of the sender, while the destination IP address is the IP address that the sender wants to resolve to a MAC address. The ARP request packet is broadcast to all devices on the local network because the sender doesn't yet know the MAC address of the target device.

* What is the Destination MAC Address of the ARP Request Packet? Who’s MAC – Address is it?

The destination MAC address of an ARP request packet is a special value called a broadcast MAC address, which is typically represented as all ones in hexadecimal format (FF:FF:FF:FF:FF:FF). This broadcast MAC address is used to ensure that the ARP request packet is received by all devices on the local network.

it's not tied to any particular MAC address; rather, it's a way to request information from the entire local network so that the appropriate device with the matching IP address can respond with its MAC address. The MAC address that ultimately responds to the ARP request will be the one associated with the IP address being queried.

* What is the Source MAC – Address of the ARP reply packet? Who’s MAC - Address is it?

When a device sends an ARP request to discover the MAC address associated with a particular IP address, the device that has that IP address responds with an ARP reply packet.

The source MAC address in the ARP reply packet will be the MAC address of the responding device, which corresponds to the IP address in question.

* How can you identify whether it is an ARP request or a Reply packet? Specify for both types.

We can identify whether a packet is an ARP request or an ARP reply by checking the value in the "Opcode" field within the ARP packet:

**ARP Request Packet :** The Opcode field has a value of 1 (or 0x0001 in hexadecimal).

**ARP Reply Packet :** The Opcode field has a value of 2 (or 0x0002 in hexadecimal).

The Opcode field is the key indicator of the packet type, making it easy to differentiate between ARP requests and ARP replies.

* How can you identify whether the ARP is a Gratuitous ARP?

To identify a Gratuitous ARP:

* Check that the Opcode field has a value of 2.
* Verify that the sender and target IP addresses are the same.
* Observe that the sender and target MAC addresses may be the same.

Gratuitous ARPs are often used to announce changes in network configurations or to update ARP caches on other devices, making them a useful tool in certain network scenarios.

* Which field indicates this is an ARP Packet?

The field that indicates that a packet is an ARP (Address Resolution Protocol) packet is the "Ether Type" field in the Ethernet frame header. The Ether Type field is a 2-byte (16-bit) field that specifies the type of protocol encapsulated within the Ethernet frame.

* What is the size of the Hardware Address and Protocol (Network) Address?

**Hardware Address:** The Hardware Address, which is typically the Media Access Control (MAC) address, is 48 bits or 6 bytes in size. MAC addresses are unique identifiers assigned to network interface cards (NICs) and are used at the data link layer of the OSI model.

**Protocol (Network) Address:** The Protocol Address, which is the IP address in the context of most ARP implementations, is 32 bits or 4 bytes in size. IP addresses are used to identify devices on a network and operate at the network layer (Layer 3) of the OSI model.

ICMP

* What is the IP address of your host? What is the IP address of the destination host?

IP address of my host: 192.168.6.7

IP address of the destination host: 104.114.93.189

* Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers?

The ICMP type is 8, and the code number is 0

* What other fields does this ICMP packet have?

The ICMP packet also has checksum, identifier, sequence number, and data fields.

* Identify the checksum, sequence number, and identifier fields of the captured ICMP packet if present.

