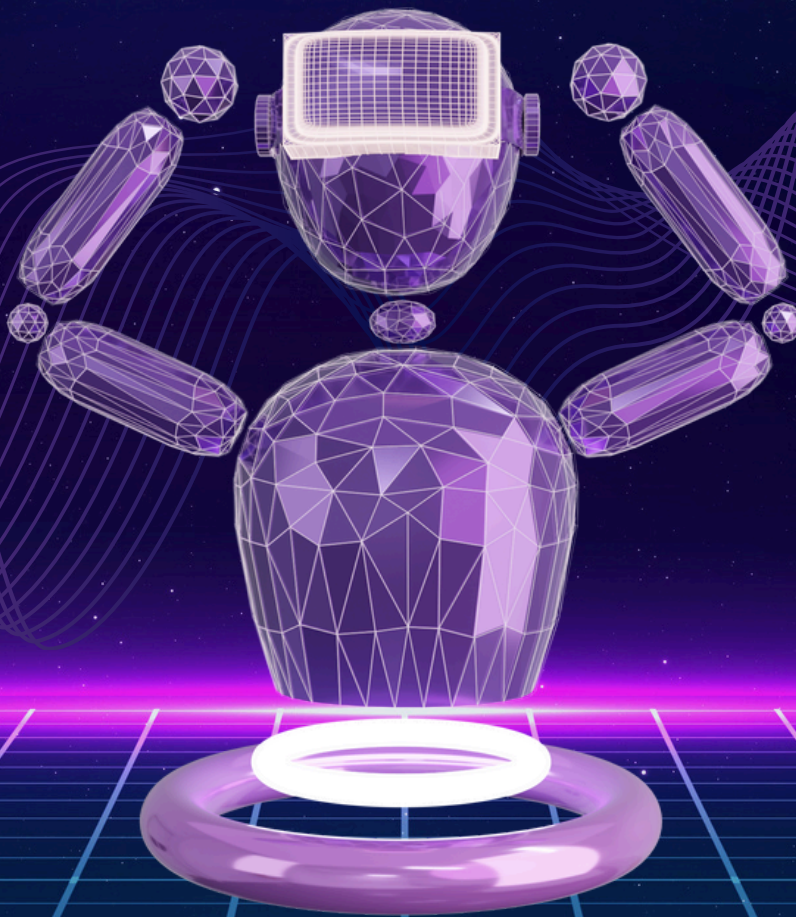




ARP

(ADDRESS RESOLUTION PROTOCOL)



www.pmnetworking.in

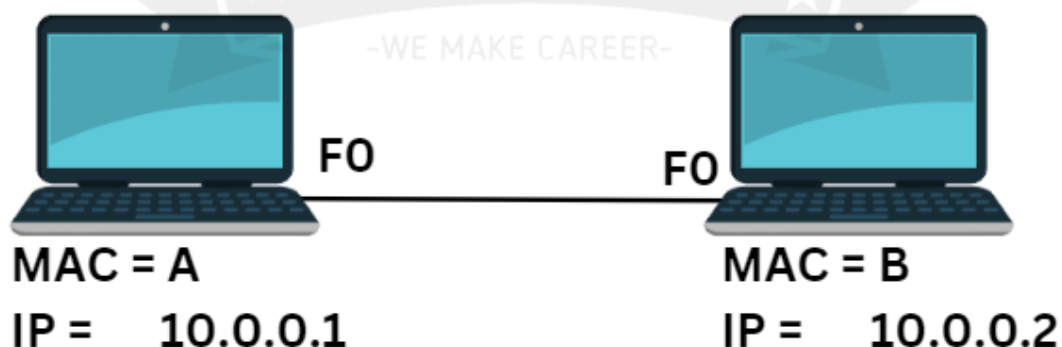
ARP (Address Resolution Protocol)

The Address Resolution Protocol (ARP) is a communication protocol that maps the Internet Protocol (IP) address to the Media Access Control (MAC) address.

- ARP is a Layer-2 protocol which is use to resolve MAC Address from IP Address.
- As you know, for basic communication four things are required.
 1. Source IP
 2. Destination IP
 3. Source MAC
 4. Destination MAC

So, whenever a device needs to find MAC Address from an IP Address, It will use ARP.

- Suppose Computer Whose IP Address is 10.0.0.1 and MAC Address is A needs to Send an ICMP Request to Computer whose IP Address is 10.0.0.2, But Problem is Computer A don't know the MAC Address of 10.0.0.2, To check MAC Address from IP Address Computer will look up their ARP Table.

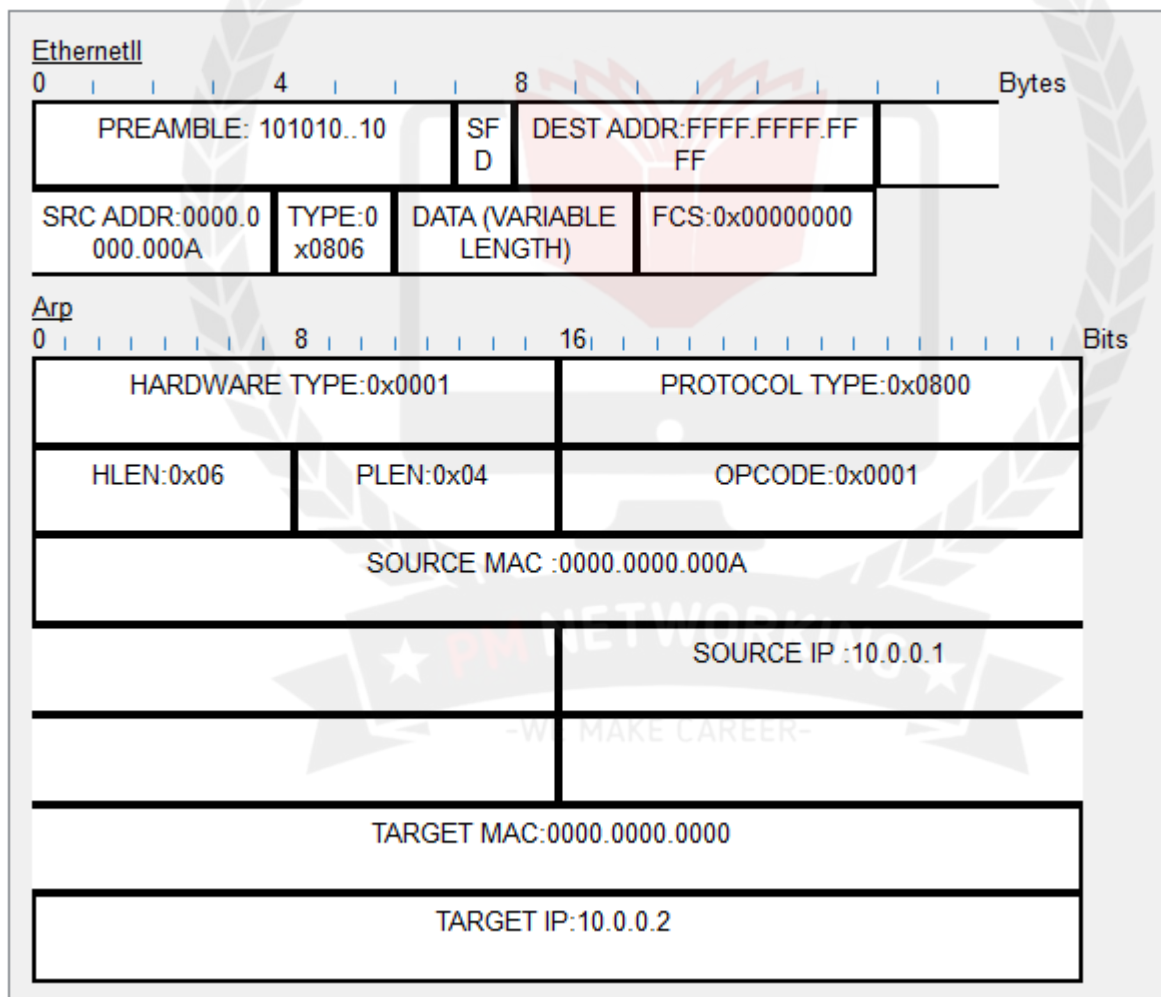


#Ping 10.0.0.2 (Source IP=10.0.0.1, Destination IP=10.0.0.2, Source MAC=A, Destination MAC=? Unknown)

ARP Table of Computer A:

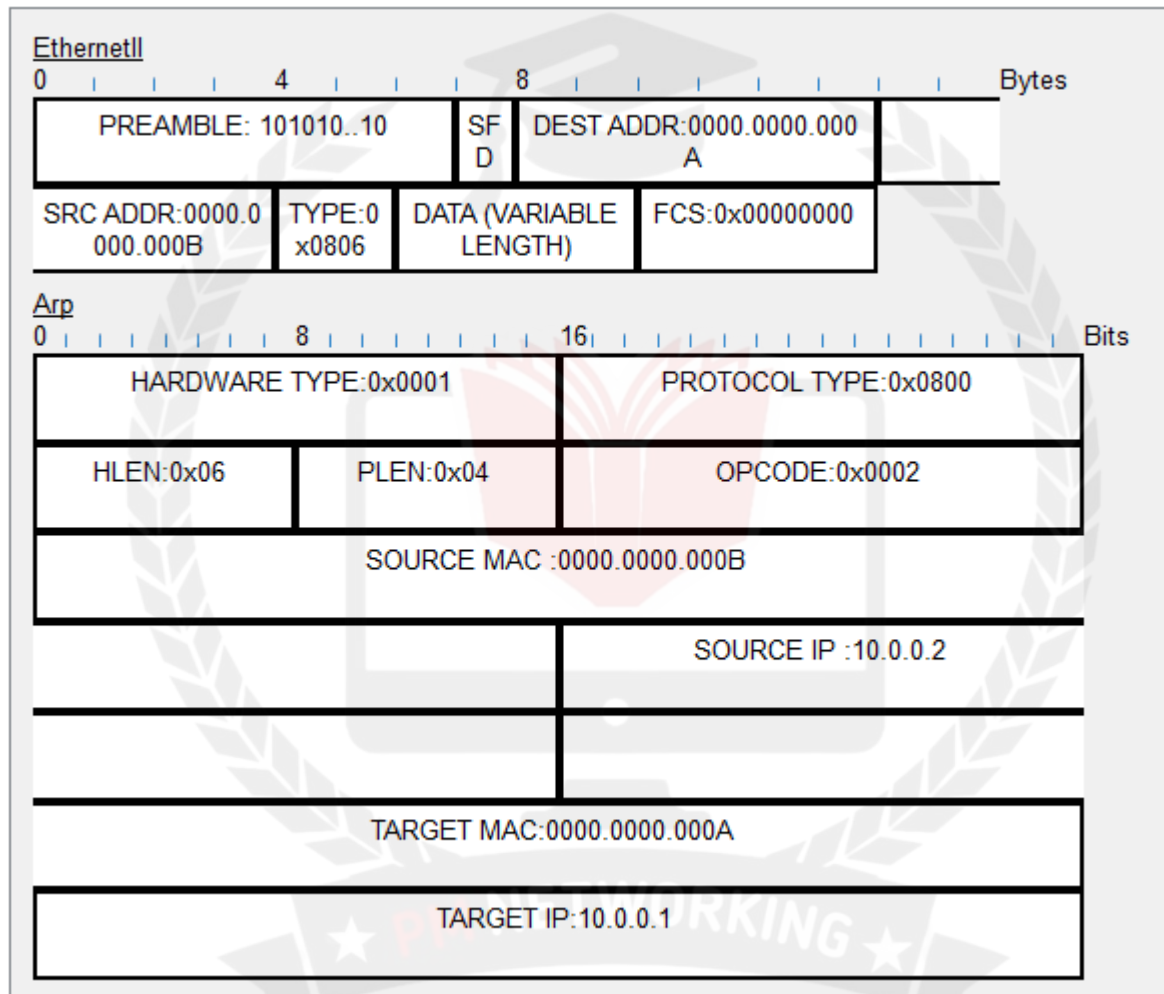
```
C:\>
C:\>
C:\>arp -a
No ARP Entries Found
C:\>
C:\>
```

Step 1: Computer A will generate ARP Request



As you can see, Target IP in the ARP Request is 10.0.0.2 that means This ARP Request is for the device whose IP Address is 10.0.0.2, So Computer B will generate Reply.

Step 2: Computer 2 will generate ARP Reply



Once Computer A will receive ARP Reply, It will update their ARP Table.


```
C:\>
C:\>
C:\>arp -a
    Internet Address      Physical Address      Type
    10.0.0.2              0000.0000.000b       dynamic

C:\>
C:\>
```

Now Computer A has all information which required for basic communication.

- Now, Computer A will Encapsulate ICMP Request Packet into Frame at layer-2.

Essentially, without ARP, a host would not be able to figure out the hardware address of another host.

How to explain in Interview:

“When a source device wants to send an IPv4 packet to another device, ARP performs two important tasks. First, the ARP program checks the ARP cache table, which consists of IPv4 address to MAC address mappings.

The second task starts if the ARP cache lookup does not provide a matching MAC address. In this case, the source server forms an ARP message, which is broadcast on the local area network”

Types of ARP

There are four types of Address Resolution Protocol:

1. Proxy ARP
2. Gratuitous ARP

3. Reverse ARP

4. Inverse ARP

Proxy ARP

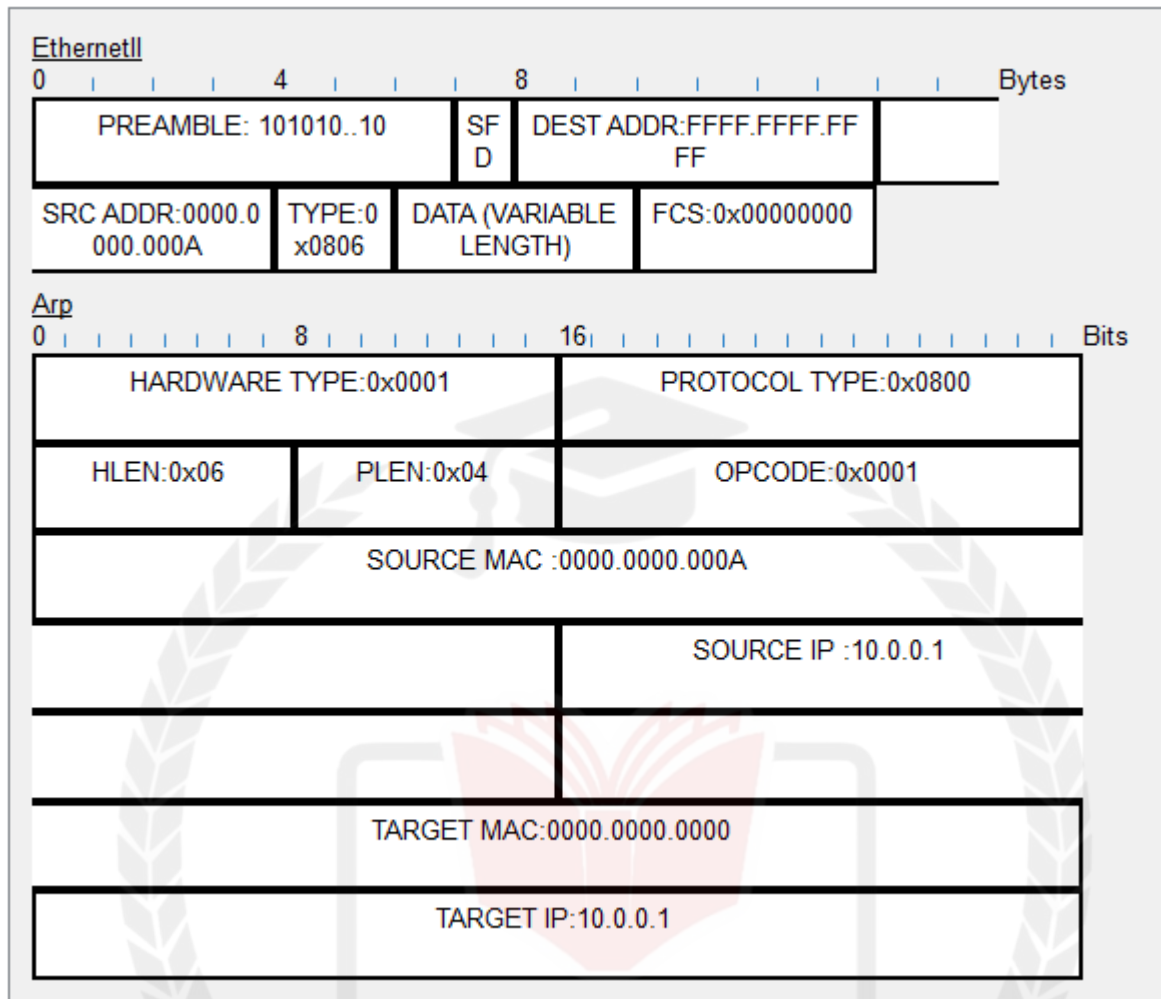
A Proxy ARP protocol handles requests coming from IP addresses that are not on the local area network. When the request packet comes from a system outside the host's network, the protocol configured router responds to the ARP request packet.

```
Router#show ip int f0/0
FastEthernet0/0 is up, line protocol is up (connected)
Internet address is 10.0.0.1/8
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
```

However, instead of providing a MAC address of the target host, the router responds by pretending to be the destination and delivers its own MAC address instead.

Gratuitous ARP

A Gratuitous ARP works as an ARP response that is not evoked by an ARP request, It is used to check duplicate IP Address.



Reverse ARP

A Reverse Address Resolution Protocol (RARP) requests IPv4 addresses from the ARP gateway router table. New systems or machines that don't have the memory to store their own IP addresses tend to use this type of ARP.

The requesting device broadcasts a Reverse ARP packet with its own MAC address in the address field of both the sender and the receiver hardware. The RARP server installed in the local network responds to the request. The server then locates a mapping table entry in the IP to MAC address. If the matching

is successful, the server sends the response packet with the IP address of the requesting computer.

Inverse ARP

An Inverse ARP does the opposite of what a traditional ARP does – it maps IP addresses using the associated hardware addresses

