CS3009D: NETWORKS LABORATORY
(EXPERIMENT 2)

Name: BHUKYA VASANTH KUMAR Batch: A
Roll Number: B180441CS Date: 31st December 2021

1. Use Wireshark to capture the packets for 5 seconds and answer the following:

INTRODUCTION about ARP:

ARP stands for Address Resolution Protocol. In order for someone to ping an IP address to their local network, the system will need to convert an IP address into a MAC address i.e. ARP maps a network layer protocol (IP address) to a data link layer (MAC address or Ethernet Address).

It means, we have Source IP address,
Source MAC address,
Destination IP address
and we need to find Destination MAC address.

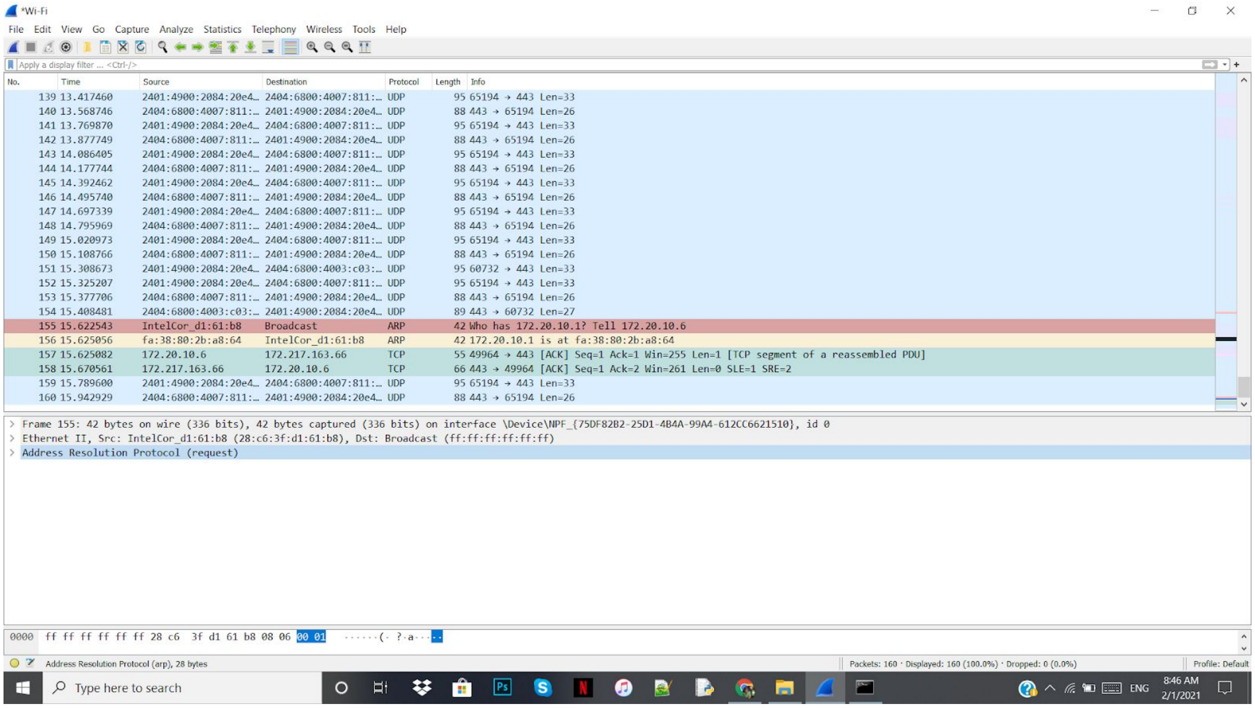
Source and destination are two addresses in the LAN.
In order to do this, the user will need to use ARP to resolve the address.
The system stores information about what IP addresses are associated with MAC addresses in an ARP look-up table/ cache table.

Working of ARP:

When a host has to find the MAC address of the destination (using destination's IP address) ARP program checks its ARP lookup table to see if IP to MAC address translation is already done.

1. If it is done, the ARP packet is displayed in the form of an **ARP REPLY** (which has the MAC address of destination) using the ARP lookup table.
2. If not, it'll send **ARP REQUEST** in the form of a broadcast packet in the network to all the all the devices in the LAN inorder to ask who has the destination IP address and then the destination will send back **ARP REPLY** (by giving the MAC address of the destination) and after giving this reply, it'll store the new MAC address in the ARP lookup table

MAC address: MAC Addresses are unique 48-bit hardware number of a computer, which is embedded into a network card NIC (known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
ENG
8:46 AM
2/1/2021

No.	Time	Source	Destination	Protocol	Length	Info
139	13.417460	2401:4900:2084:20e4…	2404:6800:4007:811:…	UDP	95	65194 → 443 Len=33
140	13.568746	2404:6800:4007:811:…	2401:4900:2084:20e4…	UDP	88	443 → 65194 Len=26
141	13.769870	2401:4900:2084:20e4…	2404:6800:4007:811:…	UDP	95	65194 → 443 Len=33
142	13.877749	2404:6800:4007:811:…	2401:4900:2084:20e4…	UDP	88	443 → 65194 Len=26
143	14.086405	2401:4900:2084:20e4…	2404:6800:4007:811:…	UDP	95	65194 → 443 Len=33
144	14.177744	2404:6800:4007:811:…	2401:4900:2084:20e4…	UDP	88	443 → 65194 Len=26
145	14.392462	2401:4900:2084:20e4…	2404:6800:4007:811:…	UDP	95	65194 → 443 Len=33
146	14.495740	2404:6800:4007:811:…	2401:4900:2084:20e4…	UDP	88	443 → 65194 Len=26
147	14.697339	2401:4900:2084:20e4…	2404:6800:4007:811:…	UDP	95	65194 → 443 Len=33
148	14.795969	2404:6800:4007:811:…	2401:4900:2084:20e4…	UDP	88	443 → 65194 Len=26
149	15.020973	2401:4900:2084:20e4…	2404:6800:4007:811:…	UDP	95	65194 → 443 Len=33
150	15.108766	2404:6800:4007:811:…	2401:4900:2084:20e4…	UDP	88	443 → 65194 Len=26
151	15.308673	2401:4900:2084:20e4…	2404:6800:4003:c03:…	UDP	95	60732 → 443 Len=33
152	15.325207	2401:4900:2084:20e4…	2404:6800:4007:811:…	UDP	95	65194 → 443 Len=33
153	15.377706	2404:6800:4007:811:…	2401:4900:2084:20e4…	UDP	88	443 → 65194 Len=26
154	15.408481	2404:6800:4003:c03:…	2401:4900:2084:20e4…	UDP	89	443 → 60732 Len=27
155	15.622543	IntelCor_d1:61:b8	Broadcast	ARP	42	Who has 172.20.10.1? Tell 172.20.10.6
156	15.625056	fa:38:80:2b:a8:64	IntelCor_d1:61:b8	ARP	42	172.20.10.1 is at fa:38:80:2b:a8:64
157	15.625082	172.20.10.6	172.217.163.66	TCP	55	49964 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
158	15.670561	172.217.163.66	172.20.10.6	TCP	66	443 → 49964 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
159	15.789600	2401:4900:2084:20e4…	2404:6800:4007:811:…	UDP	95	65194 → 443 Len=33
160	15.942929	2404:6800:4007:811:…	2401:4900:2084:20e4…	UDP	88	443 → 65194 Len=26

```
> Frame 155: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{75DF82B2-25D1-4B4A-99A4-612CC6621510}, id 0
> Ethernet II, Src: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 28 c6  3f d1 61 b8 08 06 00 01   ······(· ?·a·····
```

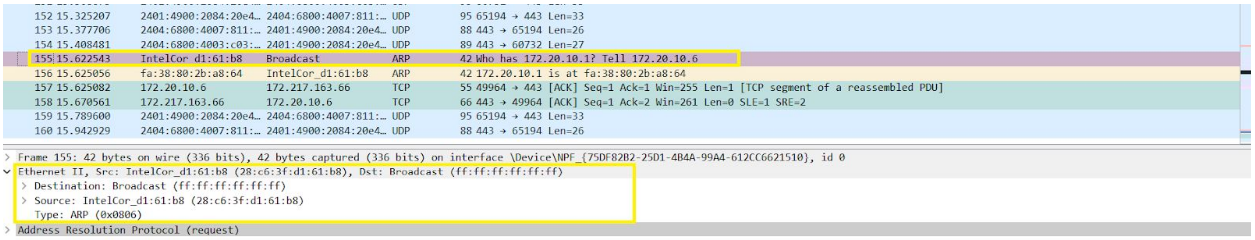
```
Address Resolution Protocol (arp), 28 bytes    Packets: 160 · Displayed: 160 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

WireShark capture for 5 seconds to capture IP and ARP packets

Note: use arp -d to clear cache in command prompt (run as administrator) and use arp -a to broadcast the ARP packets in the same command prompt.

a. For an IP and ARP packet, compare the MAC header of these two packets and find the protocol ID for ARP and IP, if exists.

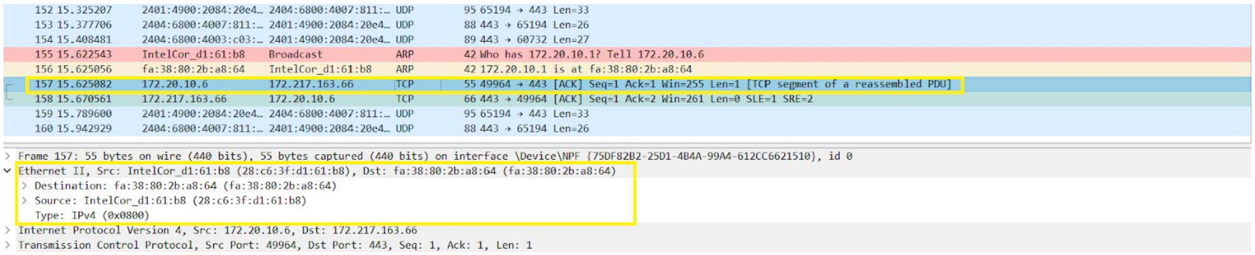
1. ARP Packet



```
152 15.325207   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP   95 65194 → 443 Len=33
153 15.377706   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP   88 443 → 65194 Len=26
154 15.408481   2404:6800:4003:c03:… 2401:4900:2084:20e4… UDP   89 443 → 60732 Len=27
155 15.622543   IntelCor d1:61:b8    Broadcast            ARP   42 Who has 172.20.10.1? Tell 172.20.10.6
156 15.625056   fa:38:80:2b:a8:64    IntelCor_d1:61:b8    ARP   42 172.20.10.1 is at fa:38:80:2b:a8:64
157 15.625082   172.20.10.6          172.217.163.66       TCP   55 49964 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
158 15.670561   172.217.163.66       172.20.10.6          TCP   66 443 → 49964 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
159 15.789600   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP   95 65194 → 443 Len=33
160 15.942929   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP   88 443 → 65194 Len=26

> Frame 155: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{75DF82B2-25D1-4B4A-99A4-612CC6621510}, id 0
v Ethernet II, Src: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
    Type: ARP (0x0806)
> Address Resolution Protocol (request)
```

2. IP Packet



```
152 15.325207   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP   95 65194 → 443 Len=33
153 15.377706   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP   88 443 → 65194 Len=26
154 15.408481   2404:6800:4003:c03:… 2401:4900:2084:20e4… UDP   89 443 → 60732 Len=27
155 15.622543   IntelCor_d1:61:b8    Broadcast            ARP   42 Who has 172.20.10.1? Tell 172.20.10.6
156 15.625056   fa:38:80:2b:a8:64    IntelCor_d1:61:b8    ARP   42 172.20.10.1 is at fa:38:80:2b:a8:64
157 15.625082   172.20.10.6          172.217.163.66       TCP   55 49964 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
158 15.670561   172.217.163.66       172.20.10.6          TCP   66 443 → 49964 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
159 15.789600   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP   95 65194 → 443 Len=33
160 15.942929   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP   88 443 → 65194 Len=26

> Frame 157: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{75DF82B2-25D1-4B4A-99A4-612CC6621510}, id 0
v Ethernet II, Src: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8), Dst: fa:38:80:2b:a8:64 (fa:38:80:2b:a8:64)
  > Destination: fa:38:80:2b:a8:64 (fa:38:80:2b:a8:64)
  > Source: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.10.6, Dst: 172.217.163.66
> Transmission Control Protocol, Src Port: 49964, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

The MAC header will include three fields:

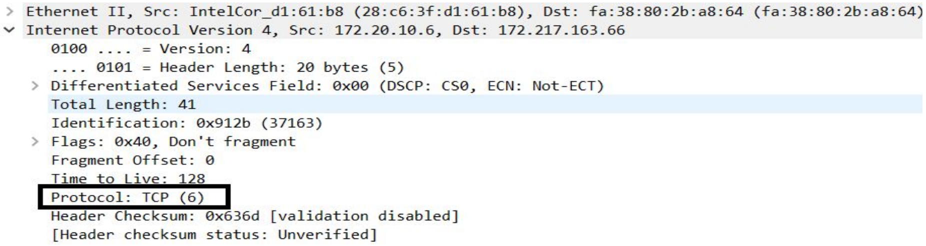
1. Destination MAC address
2. Source MAC address
3. EtherType

For IP Packet

Source address is (28:c6:3f:d1:61:b8) and destination address is (fa:38:80:2b:a4:64) and the EtherType is IPv4 (0x0800) with Protocol ID 6.

For ARP Packet

Source address is (28:c6:3f:d1:61:b8) and destination address is (ff:ff:ff:ff:ff:ff) and the EtherType is ARP (0x0806) and it has no Protocol ID.



```
> Ethernet II, Src: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8), Dst: fa:38:80:2b:a8:64 (fa:38:80:2b:a8:64)
v Internet Protocol Version 4, Src: 172.20.10.6, Dst: 172.217.163.66
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 41
    Identification: 0x912b (37163)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x636d [validation disabled]
    [Header checksum status: Unverified]
```

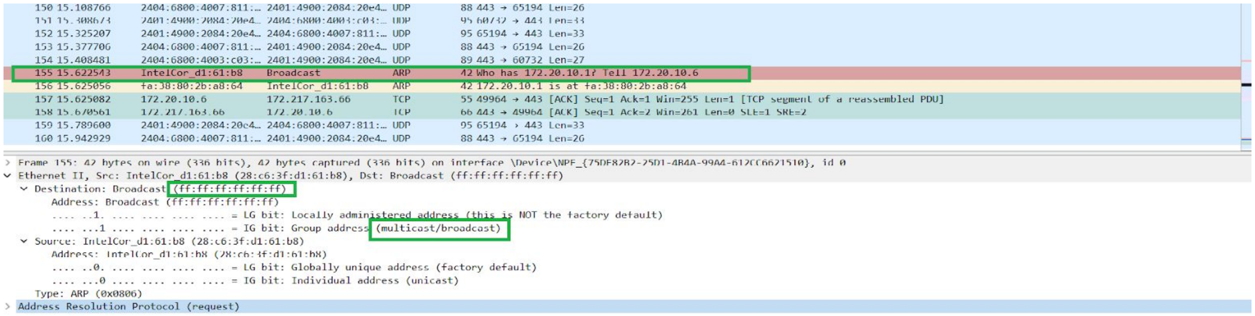
The only change is the EtherType ,the Protocol ID and Destination.

b. Is the destination address of the ARP packet a broadcast address or a unicast address?

The destination address of the ARP packet is of two types

REQUEST PACKET : BROADCAST

Since, the destination's MAC address is not known, an ARP Request of Destination's IP address is sent in the form of broadcast to all the devices in the LAN.

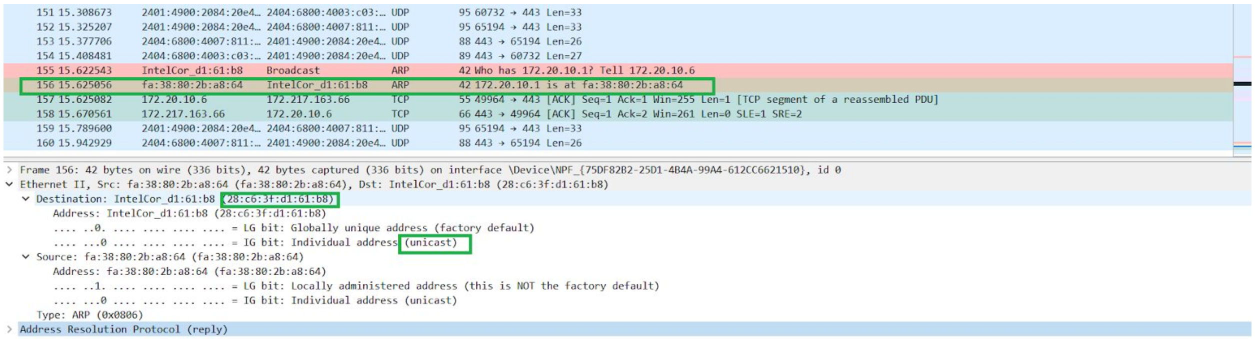


```
150 15.108766   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP     88 443 → 65194 Len=26
151 15.308673   2401:4900:2084:20e4… 2404:6800:4003:c03:… UDP     95 60732 → 443 Len=33
152 15.325207   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP     95 65194 → 443 Len=33
153 15.377706   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP     88 443 → 65194 Len=26
154 15.408481   2404:6800:4003:c03:… 2401:4900:2084:20e4… UDP     89 443 → 60732 Len=27
155 15.622543   IntelCor_d1:61:b8    Broadcast            ARP     42 Who has 172.20.10.1? Tell 172.20.10.6
156 15.625056   fa:38:80:2b:a8:64    IntelCor_d1:61:b8    ARP     42 172.20.10.1 is at fa:38:80:2b:a8:64
157 15.625082   172.20.10.6          172.217.163.66       TCP     55 49964 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
158 15.670561   172.217.163.66       172.20.10.6          TCP     66 443 → 49964 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
159 15.789600   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP     95 65194 → 443 Len=33
160 15.942929   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP     88 443 → 65194 Len=26

> Frame 155: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{75DF82B2-25D1-4B4A-99A4-612CC6621510}, id 0
v Ethernet II, Src: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
      Address: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
> Address Resolution Protocol (request)
```

REPLY PACKET: UNICAST

Since, here the MAC address is sent to Router and we know its IP address and MAC address, and the source is the device, the destination address is unicast.



```
151 15.308673   2401:4900:2084:20e4… 2404:6800:4003:c03:… UDP     95 60732 → 443 Len=33
152 15.325207   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP     95 65194 → 443 Len=33
153 15.377706   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP     88 443 → 65194 Len=26
154 15.408481   2404:6800:4003:c03:… 2401:4900:2084:20e4… UDP     89 443 → 60732 Len=27
155 15.622543   IntelCor_d1:61:b8    Broadcast            ARP     42 Who has 172.20.10.1? Tell 172.20.10.6
156 15.625056   fa:38:80:2b:a8:64    IntelCor_d1:61:b8    ARP     42 172.20.10.1 is at fa:38:80:2b:a8:64
157 15.625082   172.20.10.6          172.217.163.66       TCP     55 49964 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
158 15.670561   172.217.163.66       172.20.10.6          TCP     66 443 → 49964 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
159 15.789600   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP     95 65194 → 443 Len=33
160 15.942929   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP     88 443 → 65194 Len=26

> Frame 156: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{75DF82B2-25D1-4B4A-99A4-612CC6621510}, id 0
v Ethernet II, Src: fa:38:80:2b:a8:64 (fa:38:80:2b:a8:64), Dst: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
  v Destination: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
      Address: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: fa:38:80:2b:a8:64 (fa:38:80:2b:a8:64)
      Address: fa:38:80:2b:a8:64 (fa:38:80:2b:a8:64)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
> Address Resolution Protocol (reply)
```

c. Is the ARP packet a request or reply packet? Justify.

An ARP packet is either a request packet or reply packet.

An ARP request packet can be differentiated from an ARP reply packet using the OPERATION field i.e. opcode in the ARP packet.

For ARP Request, it is 1.
For ARP Reply, it is 2.

d. Examine the payload of the packet

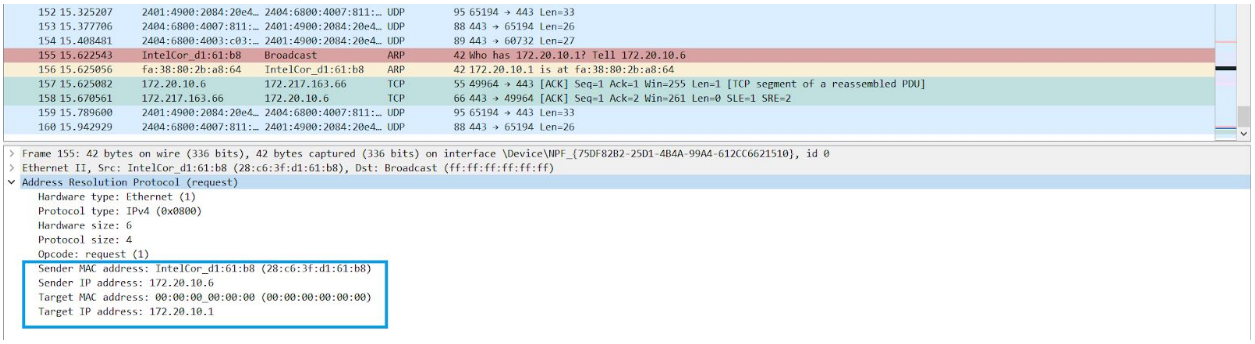
The payload of the packet contains the following:

1. *Sender Hardware Address:* Specifies the physical address of the sender.
2. *Sender Protocol Address:* specifies logical address of the sender i.e. IPv4 address.
3. *Receiver Hardware Address*: Specifies physical address of the target. For ARP REQUEST PACKET, this field contains all zeros, because the sender doesn't know MAC or physical address.
4. *Receiver Protocol address:* Specifies logical address of the target.

It also has the other following attributes :

1. *Hardware Type and Hardware size*
2. *Protocol Type and Protocol size*
3. *Opcode:* Specifies if the packet is ARP request or ARP reply.

ARP REQUEST - PAYLOAD

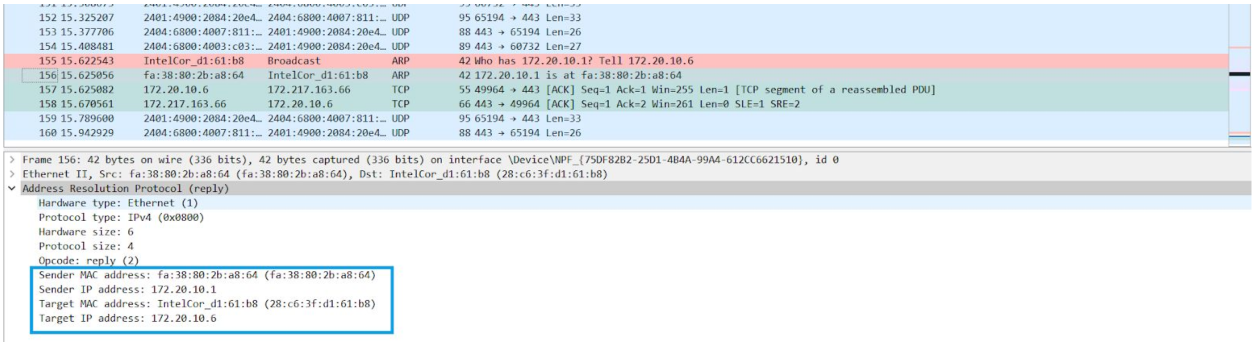


```
    152 15.325207     2401:4900:2084:20e4… 2404:6800:4007:811:… UDP          95 65194 → 443 Len=33
    153 15.377706     2404:6800:4007:811:… 2401:4900:2084:20e4… UDP          88 443 → 65194 Len=26
    154 15.408481     2404:6800:4003:c03:… 2401:4900:2084:20e4… UDP          89 443 → 60732 Len=27
    155 15.622543     IntelCor_d1:61:b8    Broadcast            ARP          42 Who has 172.20.10.1? Tell 172.20.10.6
    156 15.625056     fa:38:80:2b:a8:64    IntelCor_d1:61:b8    ARP          42 172.20.10.1 is at fa:38:80:2b:a8:64
    157 15.625082     172.20.10.6          172.217.163.66       TCP          55 49964 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
    158 15.670561     172.217.163.66       172.20.10.6          TCP          66 443 → 49964 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
    159 15.789600     2401:4900:2084:20e4… 2404:6800:4007:811:… UDP          95 65194 → 443 Len=33
    160 15.942929     2404:6800:4007:811:… 2401:4900:2084:20e4… UDP          88 443 → 65194 Len=26

> Frame 155: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{75DF82B2-25D1-4B4A-99A4-612CC6621510}, id 0
> Ethernet II, Src: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
    Sender IP address: 172.20.10.6
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.20.10.1
```

Hardware (MAC) Source Address: 28:c6:3f:d1:61:b8
Hardware (MAC) Destination Address: 00:00:00:00:00:00 (Since We don’t know the MAC address of destination)
Protocol (IP) Source Address: 172.20.10.6
Protocol (IP) Destination Address: 172.20.10.1 (This is the default gateway IP address of the router)
Opcode: 1
Hardware type: Ethernet
Hardware Size: 4
Protocol type: IPv4
Protocol Size: 6

ARP REPLY - PAYLOAD



```
152 15.325207   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP   95 65194 → 443 Len=33
153 15.377706   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP   88 443 → 65194 Len=26
154 15.408481   2404:6800:4003:c03:… 2401:4900:2084:20e4… UDP   89 443 → 60732 Len=27
155 15.622543   IntelCor_d1:61:b8    Broadcast            ARP   42 Who has 172.20.10.1? Tell 172.20.10.6
156 15.625056   fa:38:80:2b:a8:64    IntelCor_d1:61:b8    ARP   42 172.20.10.1 is at fa:38:80:2b:a8:64
157 15.625082   172.20.10.6          172.217.163.66       TCP   55 49964 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
158 15.670561   172.217.163.66       172.20.10.6          TCP   66 443 → 49964 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
159 15.789600   2401:4900:2084:20e4… 2404:6800:4007:811:… UDP   95 65194 → 443 Len=33
160 15.942929   2404:6800:4007:811:… 2401:4900:2084:20e4… UDP   88 443 → 65194 Len=26

> Frame 156: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{75DF82B2-25D1-4B4A-99A4-612CC6621510}, id 0
> Ethernet II, Src: fa:38:80:2b:a8:64 (fa:38:80:2b:a8:64), Dst: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: fa:38:80:2b:a8:64 (fa:38:80:2b:a8:64)
    Sender IP address: 172.20.10.1
    Target MAC address: IntelCor_d1:61:b8 (28:c6:3f:d1:61:b8)
    Target IP address: 172.20.10.6
```

Hardware (MAC) Source Address: fa:38:80:2b:a4:64
Hardware (MAC) Destination Address: 28:c6:3f:d1:61:b8
Protocol (IP) Source Address: 172.20.10.1
Protocol (IP) Destination Address: 172.20.10.6 (This is the default gateway IP address of the router)
Opcode: 2
Hardware type: Ethernet
Hardware Size: 4
Protocol type: IPv4
Protocol Size: 6

e. **What transport layer protocols are used in Skype and Zoom.**

Skype and uses both transport layer protocols, UDP and TCP.

Ex: It sends audio/video over UDP and then uses TCP to send text messages and also to initiate connections or to bypass some firewalls which would block UDP packets.

Basically, any client-server communication will usually happen over HTTP/HTTPS channels. In case, if the communication is bidirectional, we will be using WEB SOCKET PROTOCOLS. Here, the connection is made after a <u>THREE-WAY TCP HANDSHAKE</u> i.e. client sends a connection request to server, the server responds with some sort of acknowledgment and the client responds back with an acknowledgement and now a connection is formed. This 3 step process is called a <u>THREE-WAY TCP HANDSHAKE</u>.

So, *TCP is a lossless protocol* i.e. data packets can never go missing. TCP ensures this by receiving an acknowledgement from the receiver for every data packet it receives. Until the sender receives the acknowledgment for a data packet it will keep sending the data packet again and again. Also, TCP does confession control i.e. every time the network gets choked due to high traffic, it will delay sending some data packets so as to not affect the network. Thus, kind of delay and lots of overhead is involved in TCP.

UDP is a lossy protocol, i.e. it doesn’t need a connection to send data packets. If the devices know each other’s IP address, with P2P (Peer to Peer) connection, the sender can send packets, but only once. If the packets don’t reach the receiver, the sender won’t send it again. UDP is faster and can avoid overhead, traffic but data reaching will not be perfect.

Therefore, Skype and Zoom will be using the combination of both TCP and UDP. All API calls, communication will happen over TCP but video transfer will be over UDP.