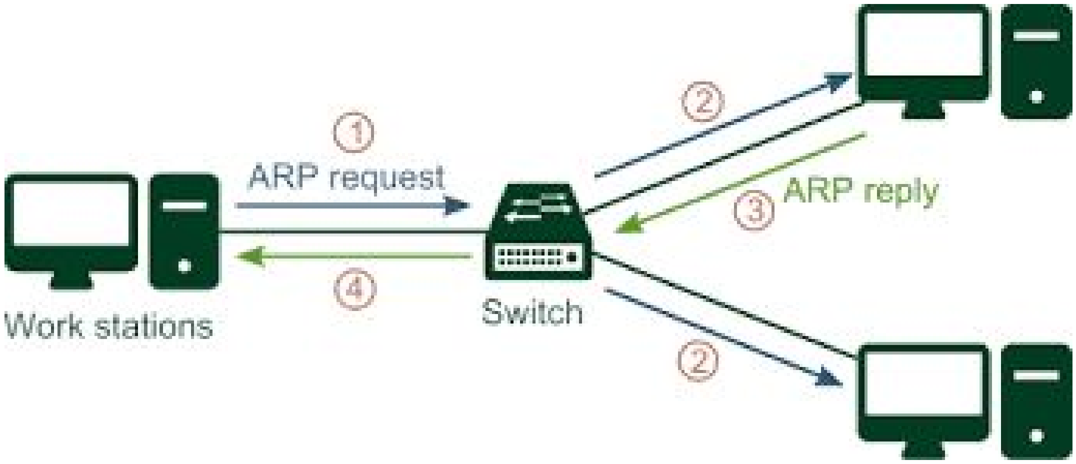
CS3093D Networks Lab

Namburi Soujanya, B180491CS

ASSIGNMENT 2



INTRODUCTION TO ARP:

Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).
An ARP packet is used to find a particular machine's MAC address when the IP address is given. A broadcast is sent to all devices, and then the right device returns its MAC address. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2 (Data link layer) and level 3 (Network layer)
The ARP command manipulates the system's ARP cache.
SYNTAX: arp [-v] [-i if] [-H type] -a [hostname]

There are 2 types of entries in the ARP cache

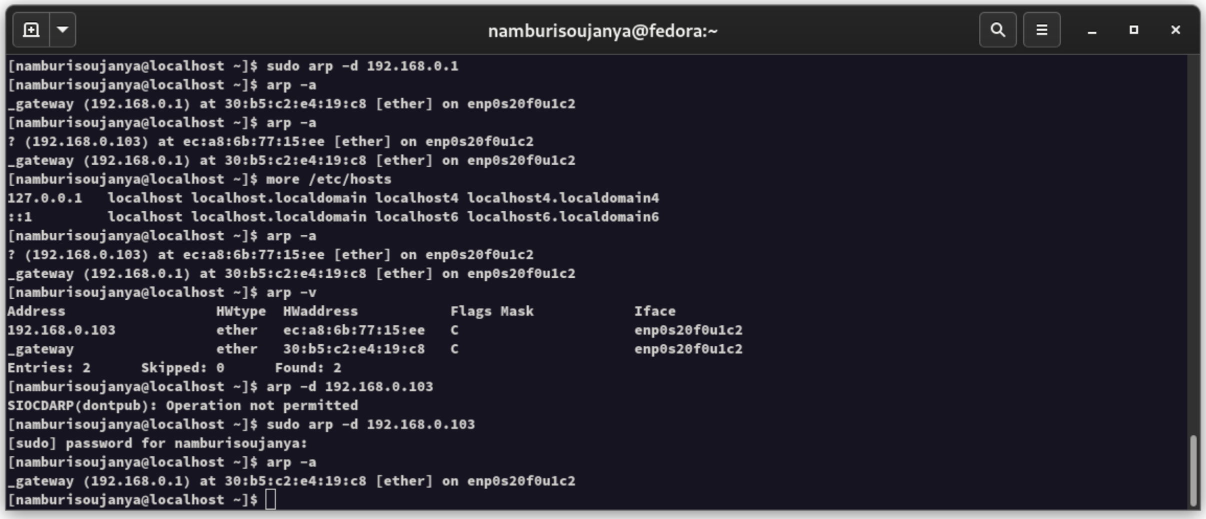
1. Static entries
2. Dynamic entries

Static ones are kept permanently (It can help network managers set up ARP entries to lessen unnecessary ARP broadcast traffic) while the dynamic ones are created and flushed out automatically

This way. To get the ARP traffic on wireshark, we first flush the ARP cache first using

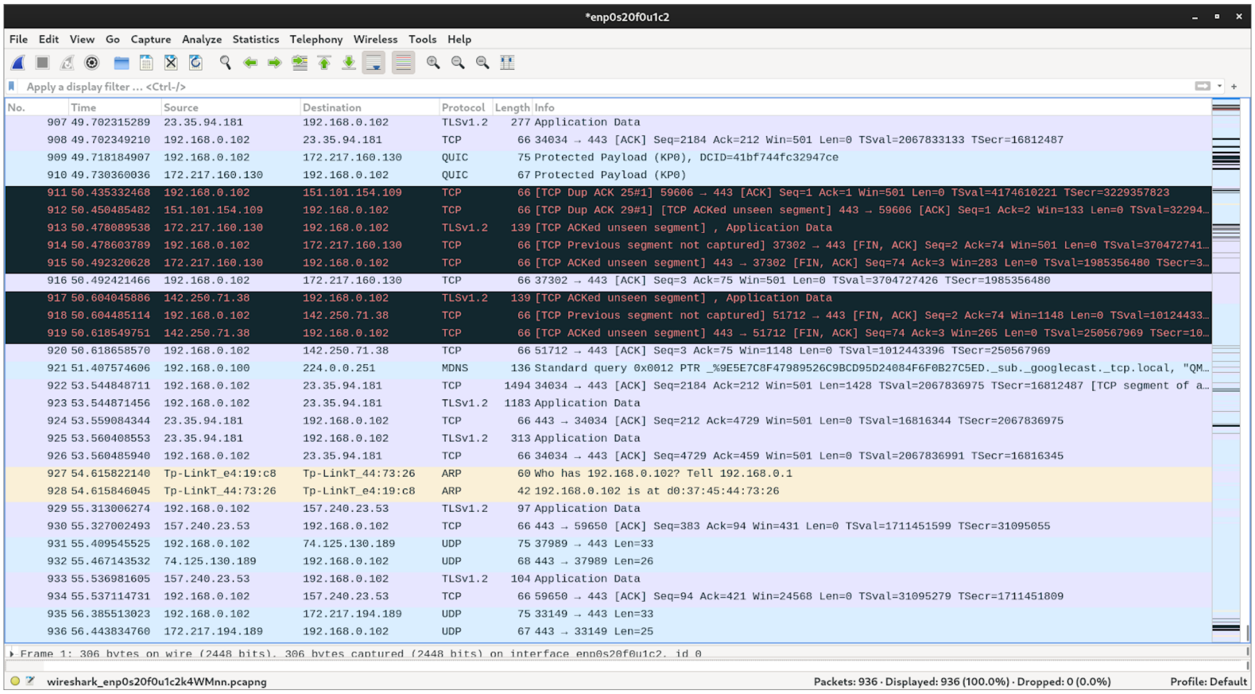
- Sudo arp -d hostname
- -a: Displays current ARP cache tables for all interfaces.
- More /etc/hosts : to display the hosts

This way, I get an ARP packet that is broadcasted and replied to.



```
[namburisoujanya@localhost ~]$ sudo arp -d 192.168.0.1
[namburisoujanya@localhost ~]$ arp -a
_gateway (192.168.0.1) at 30:b5:c2:e4:19:c8 [ether] on enp0s20f0u1c2
[namburisoujanya@localhost ~]$ arp -a
? (192.168.0.103) at ec:a8:6b:77:15:ee [ether] on enp0s20f0u1c2
_gateway (192.168.0.1) at 30:b5:c2:e4:19:c8 [ether] on enp0s20f0u1c2
[namburisoujanya@localhost ~]$ more /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
[namburisoujanya@localhost ~]$ arp -a
? (192.168.0.103) at ec:a8:6b:77:15:ee [ether] on enp0s20f0u1c2
_gateway (192.168.0.1) at 30:b5:c2:e4:19:c8 [ether] on enp0s20f0u1c2
[namburisoujanya@localhost ~]$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.103            ether   ec:a8:6b:77:15:ee   C                     enp0s20f0u1c2
_gateway                 ether   30:b5:c2:e4:19:c8   C                     enp0s20f0u1c2
Entries: 2      Skipped: 0      Found: 2
[namburisoujanya@localhost ~]$ arp -d 192.168.0.103
SIOCDARP(dontpub): Operation not permitted
[namburisoujanya@localhost ~]$ sudo arp -d 192.168.0.103
[sudo] password for namburisoujanya:
[namburisoujanya@localhost ~]$ arp -a
_gateway (192.168.0.1) at 30:b5:c2:e4:19:c8 [ether] on enp0s20f0u1c2
[namburisoujanya@localhost ~]$ 
```

Now, capturing the traffic on wireshark for 5 seconds, we get: ,


*enp0s20f0u1c2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

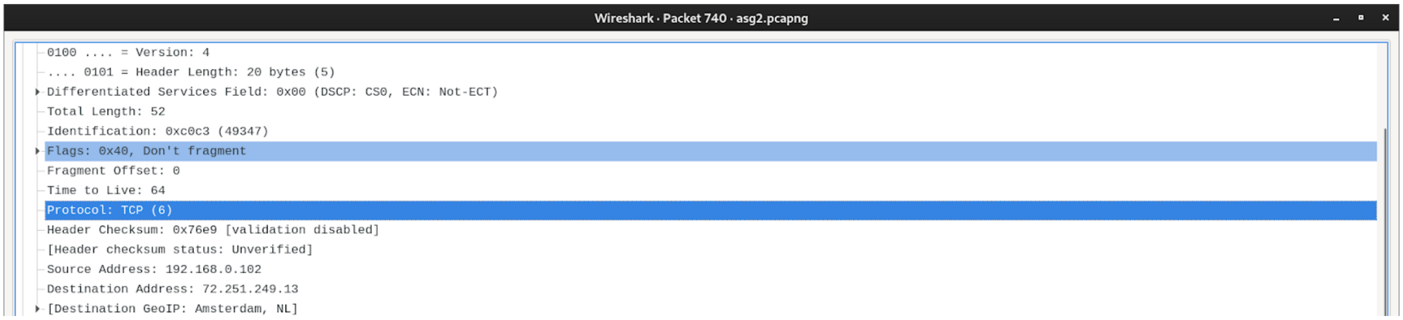
```
No.  Time         Source            Destination       Protocol Length Info
 907 49.702315289 23.35.94.181      192.168.0.102     TLSv1.2   277 Application Data
 908 49.702349210 192.168.0.102     23.35.94.181      TCP        66 34034 → 443 [ACK] Seq=2184 Ack=212 Win=501 Len=0 TSval=2067833133 TSecr=16812487
 909 49.718184907 192.168.0.102     172.217.160.130   QUIC       75 Protected Payload (KP0), DCID=41bf744fc32947ce
 910 49.730360036 172.217.160.130   192.168.0.102     QUIC       67 Protected Payload (KP0)
 911 50.435332468 192.168.0.102     151.101.154.109   TCP        66 [TCP Dup ACK 25#1] 59606 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=4174610221 TSecr=3229357823
 912 50.450485482 151.101.154.109   192.168.0.102     TCP        66 [TCP Dup ACK 29#1] [TCP ACKed unseen segment] 443 → 59606 [ACK] Seq=1 Ack=2 Win=133 Len=0 TSval=32294…
 913 50.478089538 172.217.160.130   192.168.0.102     TLSv1.2   139 [TCP ACKed unseen segment] , Application Data
 914 50.478603789 192.168.0.102     172.217.160.130   TCP        66 [TCP Previous segment not captured] 37302 → 443 [FIN, ACK] Seq=2 Ack=74 Win=501 Len=0 TSval=370472741…
 915 50.492320628 172.217.160.130   192.168.0.102     TCP        66 [TCP ACKed unseen segment] 443 → 37302 [FIN, ACK] Seq=74 Ack=3 Win=283 Len=0 TSval=1985356480 TSecr=3…
 916 50.492421466 192.168.0.102     172.217.160.130   TCP        66 37302 → 443 [ACK] Seq=3 Ack=75 Win=501 Len=0 TSval=3704727426 TSecr=1985356480
 917 50.604045886 142.250.71.38     192.168.0.102     TLSv1.2   139 [TCP ACKed unseen segment] , Application Data
 918 50.604485114 192.168.0.102     142.250.71.38     TCP        66 [TCP Previous segment not captured] 51712 → 443 [FIN, ACK] Seq=2 Ack=74 Win=1148 Len=0 TSval=10124433…
 919 50.618549751 142.250.71.38     192.168.0.102     TCP        66 [TCP ACKed unseen segment] 443 → 51712 [FIN, ACK] Seq=74 Ack=3 Win=265 Len=0 TSval=250567969 TSecr=10…
 920 50.618658570 192.168.0.102     142.250.71.38     TCP        66 51712 → 443 [ACK] Seq=3 Ack=75 Win=1148 Len=0 TSval=1012443396 TSecr=250567969
 921 51.407574606 192.168.0.100     224.0.0.251       MDNS      136 Standard query 0x0012 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local, "QM…
 922 53.544848711 192.168.0.102     23.35.94.181      TCP      1494 34034 → 443 [ACK] Seq=2184 Ack=212 Win=501 Len=1428 TSval=2067836975 TSecr=16812487 [TCP segment of a…
 923 53.544871456 192.168.0.102     23.35.94.181      TLSv1.2  1183 Application Data
 924 53.559084344 23.35.94.181      192.168.0.102     TCP        66 443 → 34034 [ACK] Seq=212 Ack=4729 Win=501 Len=0 TSval=16816344 TSecr=2067836975
 925 53.560408553 23.35.94.181      192.168.0.102     TLSv1.2   313 Application Data
 926 53.560485940 192.168.0.102     23.35.94.181      TCP        66 34034 → 443 [ACK] Seq=4729 Ack=459 Win=501 Len=0 TSval=2067836991 TSecr=16816345
 927 54.615822140 Tp-LinkT_e4:19:c8 Tp-LinkT_44:73:26 ARP        60 Who has 192.168.0.102? Tell 192.168.0.1
 928 54.615846045 Tp-LinkT_44:73:26 Tp-LinkT_e4:19:c8 ARP        42 192.168.0.102 is at d0:37:45:44:73:26
 929 55.313006274 192.168.0.102     157.240.23.53     TLSv1.2    97 Application Data
 930 55.327002493 157.240.23.53     192.168.0.102     TCP        66 443 → 59650 [ACK] Seq=383 Ack=94 Win=431 Len=0 TSval=1711451599 TSecr=31095055
 931 55.409545525 192.168.0.102     74.125.130.189    UDP        75 37989 → 443 Len=33
 932 55.467143532 74.125.130.189    192.168.0.102     UDP        68 443 → 37989 Len=26
 933 55.536981605 157.240.23.53     192.168.0.102     TLSv1.2   104 Application Data
 934 55.537114731 192.168.0.102     157.240.23.53     TCP        66 59650 → 443 [ACK] Seq=94 Ack=421 Win=24568 Len=0 TSval=31095279 TSecr=1711451809
 935 56.385513023 192.168.0.102     172.217.194.189   UDP        75 33149 → 443 Len=33
 936 56.443834760 172.217.194.189   192.168.0.102     UDP        67 443 → 33149 Len=25
▸ Frame 1: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface enp0s20f0u1c2, id 0

wireshark_enp0s20f0u1c2k4WMnn.pcapng    Packets: 936 · Displayed: 936 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

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.

Ans.

The protocol ID is a number embedded in the header of the packet to identify the protocol. It is used for many protocols that are not identified with a port number and it defined only for IP.

For an IP packet:



```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0xc0c3 (49347)
▸ Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x76e9 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.102
Destination Address: 72.251.249.13
▸ [Destination GeoIP: Amsterdam, NL]
```

Here,

The MAC header has:

Src: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)

Dst: Tp-LinkT_e4:19:c8 (30:b5:c2:e4:19:c8)

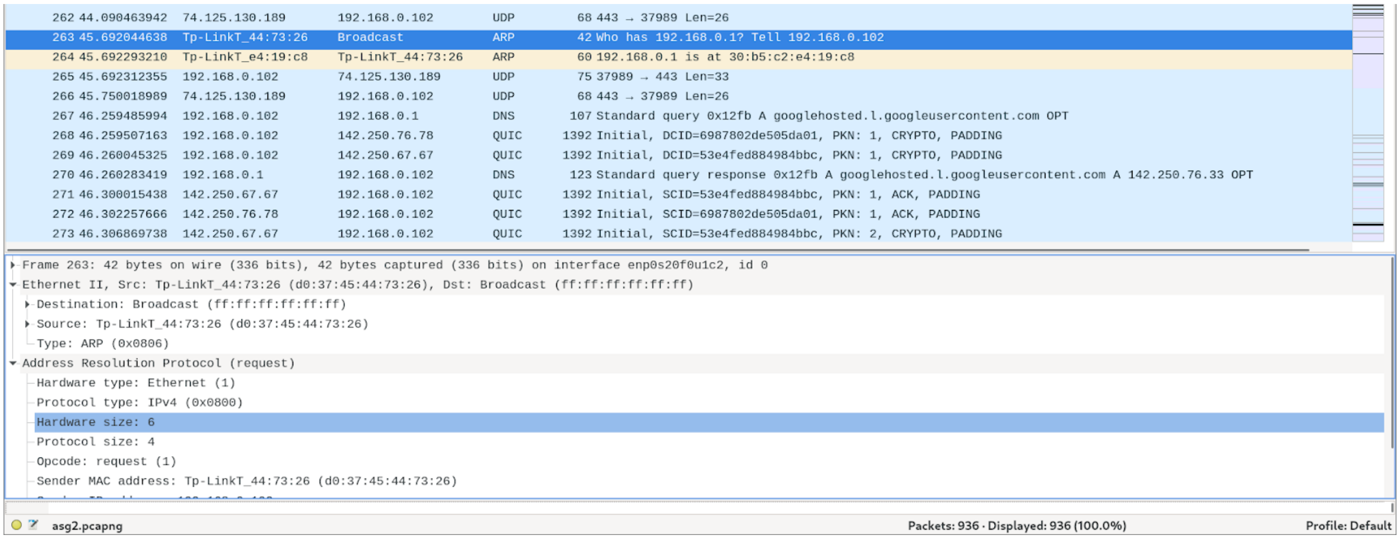
Destination: Tp-LinkT_e4:19:c8 (30:b5:c2:e4:19:c8)

Source: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)

Type: IPv4 (0x0800)

Protocol ID of a TCP packet is 6

For an ARP packet:



```
    262 44.090463942  74.125.130.189     192.168.0.102      UDP        68 443 → 37989 Len=26
    263 45.692044638  Tp-LinkT_44:73:26  Broadcast          ARP        42 Who has 192.168.0.1? Tell 192.168.0.102
    264 45.692293210  Tp-LinkT_e4:19:c8  Tp-LinkT_44:73:26  ARP        60 192.168.0.1 is at 30:b5:c2:e4:19:c8
    265 45.692312355  192.168.0.102      74.125.130.189     UDP        75 37989 → 443 Len=33
    266 45.750018989  74.125.130.189     192.168.0.102      UDP        68 443 → 37989 Len=26
    267 46.259485994  192.168.0.102      192.168.0.1        DNS       107 Standard query 0x12fb A googlehosted.l.googleusercontent.com OPT
    268 46.259507163  192.168.0.102      142.250.76.78      QUIC     1392 Initial, DCID=6987802de505da01, PKN: 1, CRYPTO, PADDING
    269 46.260045325  192.168.0.102      142.250.67.67      QUIC     1392 Initial, DCID=53e4fed884984bbc, PKN: 1, CRYPTO, PADDING
    270 46.260283419  192.168.0.1        192.168.0.102      DNS       123 Standard query response 0x12fb A googlehosted.l.googleusercontent.com A 142.250.76.33 OPT
    271 46.300015438  142.250.67.67      192.168.0.102      QUIC     1392 Initial, SCID=53e4fed884984bbc, PKN: 1, ACK, PADDING
    272 46.302257666  142.250.76.78      192.168.0.102      QUIC     1392 Initial, SCID=6987802de505da01, PKN: 1, ACK, PADDING
    273 46.306869738  142.250.67.67      192.168.0.102      QUIC     1392 Initial, SCID=53e4fed884984bbc, PKN: 2, CRYPTO, PADDING

▸ Frame 263: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s20f0u1c2, id 0
▾ Ethernet II, Src: Tp-LinkT_44:73:26 (d0:37:45:44:73:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)
    Type: ARP (0x0806)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)
```

asg2.pcapng   Packets: 936 · Displayed: 936 (100.0%)   Profile: Default

Ethernet II, Src: Tp-LinkT_44:73:26 (d0:37:45:44:73:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)

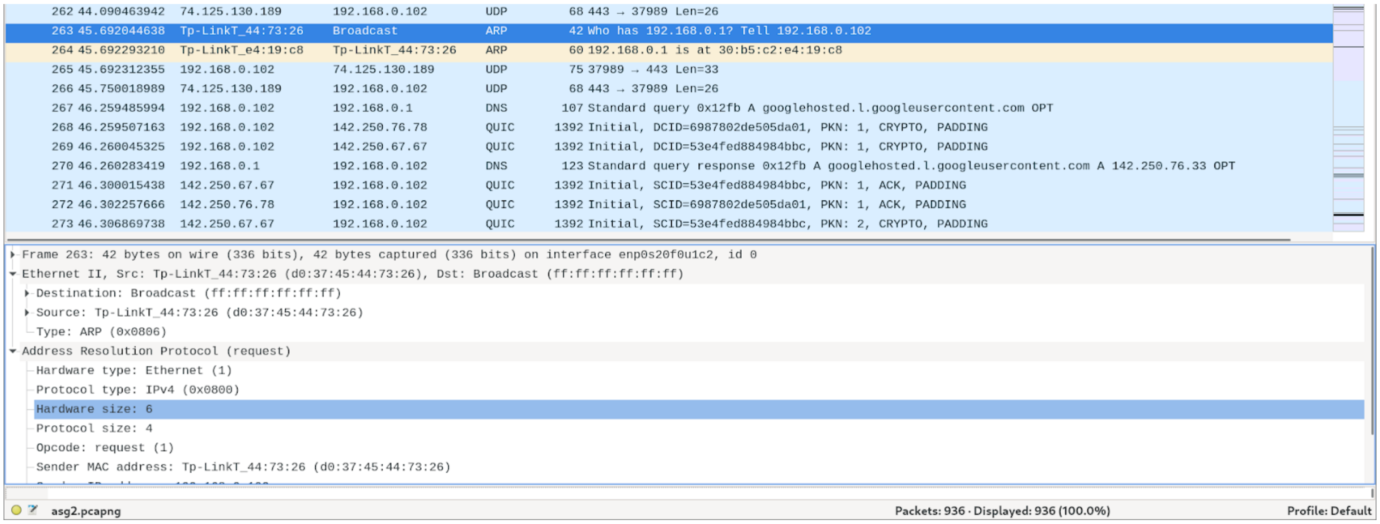
Type: ARP (0x0806)

Protocol ID does not exist for ARP,

The destination MAC address is such as it is first broadcasting to find the right device

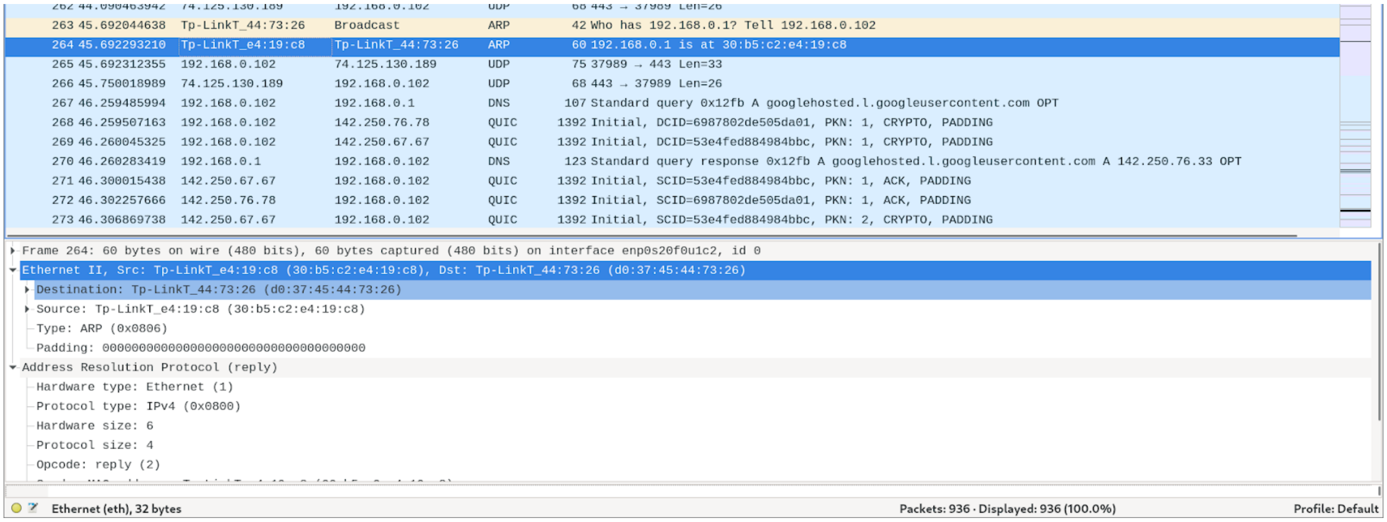
b) Is the destination address of the ARP packet a broadcast address or a unicast address?

Ans: During an ARP request, the destination address is broadcasted to find the machine with the particular IP address and returns its MAC address. Therefore it is “ff:ff:ff:ff:ff:ff”



```
262 44.090463942  74.125.130.189     192.168.0.102      UDP        68 443 → 37989 Len=26
263 45.692044638  Tp-LinkT_44:73:26  Broadcast          ARP        42 Who has 192.168.0.1? Tell 192.168.0.102
264 45.692293210  Tp-LinkT_e4:19:c8  Tp-LinkT_44:73:26  ARP        60 192.168.0.1 is at 30:b5:c2:e4:19:c8
265 45.692312355  192.168.0.102      74.125.130.189     UDP        75 37989 → 443 Len=33
266 45.750018989  74.125.130.189     192.168.0.102      UDP        68 443 → 37989 Len=26
267 46.259485994  192.168.0.102      192.168.0.1        DNS       107 Standard query 0x12fb A googlehosted.l.googleusercontent.com OPT
268 46.259507163  192.168.0.102      142.250.76.78      QUIC     1392 Initial, DCID=6987802de505da01, PKN: 1, CRYPTO, PADDING
269 46.260045325  192.168.0.102      142.250.67.67      QUIC     1392 Initial, DCID=53e4fed884984bbc, PKN: 1, CRYPTO, PADDING
270 46.260283419  192.168.0.1        192.168.0.102      DNS       123 Standard query response 0x12fb A googlehosted.l.googleusercontent.com A 142.250.76.33 OPT
271 46.300015438  142.250.67.67      192.168.0.102      QUIC     1392 Initial, SCID=53e4fed884984bbc, PKN: 1, ACK, PADDING
272 46.302257666  142.250.76.78      192.168.0.102      QUIC     1392 Initial, SCID=6987802de505da01, PKN: 1, ACK, PADDING
273 46.306869738  142.250.67.67      192.168.0.102      QUIC     1392 Initial, SCID=53e4fed884984bbc, PKN: 2, CRYPTO, PADDING

▸ Frame 263: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s20f0u1c2, id 0
▾ Ethernet II, Src: Tp-LinkT_44:73:26 (d0:37:45:44:73:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)
    Type: ARP (0x0806)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)

asg2.pcapng                    Packets: 936 · Displayed: 936 (100.0%)                    Profile: Default
```

During an ARP reply, the destination address becomes unicast as the machine is detected and it contains the details of the machine’s MAC address to the sender of the ARP request.



```
262 44.090463942  74.125.130.189     192.168.0.102      UDP        68 443 → 37989 Len=26
263 45.692044638  Tp-LinkT_44:73:26  Broadcast          ARP        42 Who has 192.168.0.1? Tell 192.168.0.102
264 45.692293210  Tp-LinkT_e4:19:c8  Tp-LinkT_44:73:26  ARP        60 192.168.0.1 is at 30:b5:c2:e4:19:c8
265 45.692312355  192.168.0.102      74.125.130.189     UDP        75 37989 → 443 Len=33
266 45.750018989  74.125.130.189     192.168.0.102      UDP        68 443 → 37989 Len=26
267 46.259485994  192.168.0.102      192.168.0.1        DNS       107 Standard query 0x12fb A googlehosted.l.googleusercontent.com OPT
268 46.259507163  192.168.0.102      142.250.76.78      QUIC     1392 Initial, DCID=6987802de505da01, PKN: 1, CRYPTO, PADDING
269 46.260045325  192.168.0.102      142.250.67.67      QUIC     1392 Initial, DCID=53e4fed884984bbc, PKN: 1, CRYPTO, PADDING
270 46.260283419  192.168.0.1        192.168.0.102      DNS       123 Standard query response 0x12fb A googlehosted.l.googleusercontent.com A 142.250.76.33 OPT
271 46.300015438  142.250.67.67      192.168.0.102      QUIC     1392 Initial, SCID=53e4fed884984bbc, PKN: 1, ACK, PADDING
272 46.302257666  142.250.76.78      192.168.0.102      QUIC     1392 Initial, SCID=6987802de505da01, PKN: 1, ACK, PADDING
273 46.306869738  142.250.67.67      192.168.0.102      QUIC     1392 Initial, SCID=53e4fed884984bbc, PKN: 2, CRYPTO, PADDING

▸ Frame 264: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s20f0u1c2, id 0
▾ Ethernet II, Src: Tp-LinkT_e4:19:c8 (30:b5:c2:e4:19:c8), Dst: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)
  ▸ Destination: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)
  ▸ Source: Tp-LinkT_e4:19:c8 (30:b5:c2:e4:19:c8)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)

Ethernet (eth), 32 bytes       Packets: 936 · Displayed: 936 (100.0%)                    Profile: Default
```

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

Ans. There are 2 types of ARP packets:

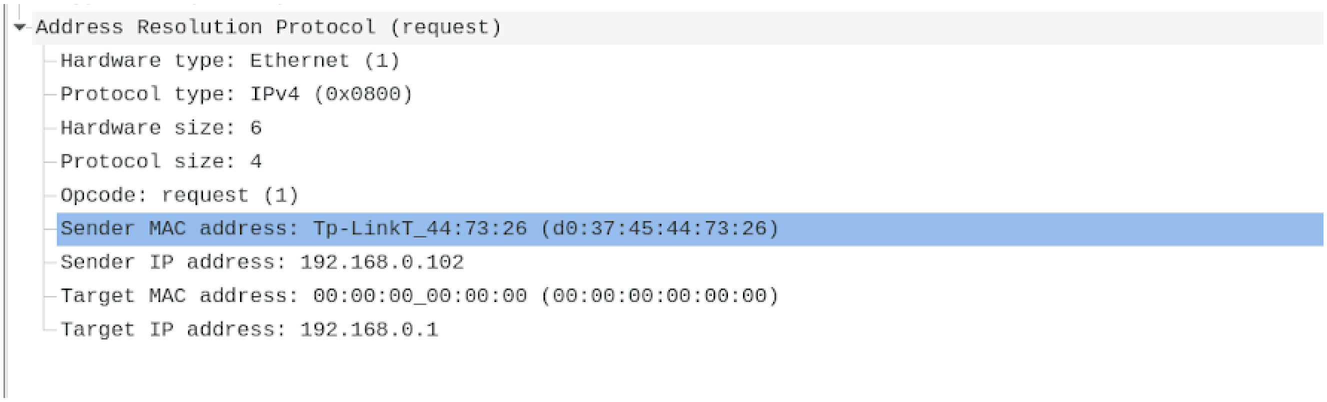
- ARP reply that is unicast to the requesting station alone
- ARP request that is broadcast to all the systems in a LAN segment

Unicast: If the MAC address is present in ARP cache (A table that contains IP address and their corresponding MAC address in the network) for corresponding IP address

Broadcast: If the MAC address is not present in its ARP cache table for corresponding IP address.

The first is a request packet to find the machine having the particular IP address, broadcasted to all devices in the network. Then, the ARP reply packet returns the MAC address of the correct device.

“Who has 192.168.0.1? Tell 192.168.0.102 “ is a request to 192.168.0.1 to return its MAC address



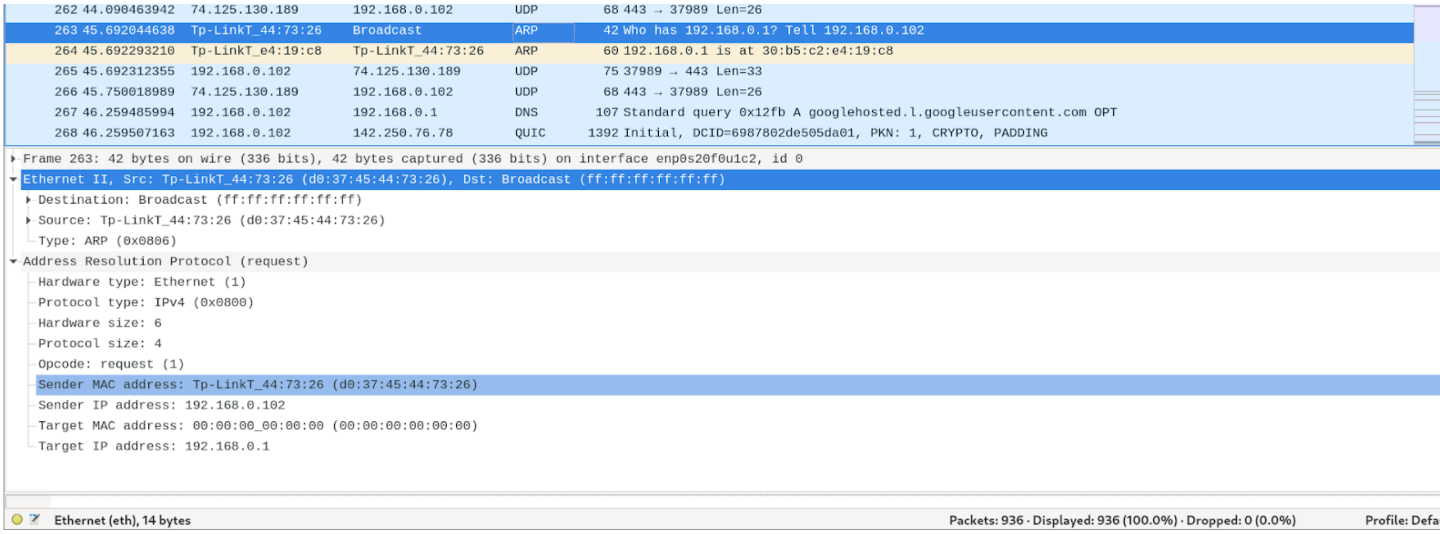
```
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)
    Sender IP address: 192.168.0.102
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.1
```

<u>Opcode there indicates the operation being performed</u> ; reply is 2, request is 1.

d) Examine the payload of the packet.

Ans: The payload of the packet contains the following fields:

1. Hardware type: defines the type of hardware being used to transport the packet
2. Protocol: The protocol that will be used on the Network Layer
3. Hardware size:
4. Protocol size: The size of the addressing scheme in bytes (4 for IPv4)
5. Opcode: The operation being performed using the packet
6. Sender MAC address:
7. Target MAC address
8. Sender IP address
9. Target IP address.

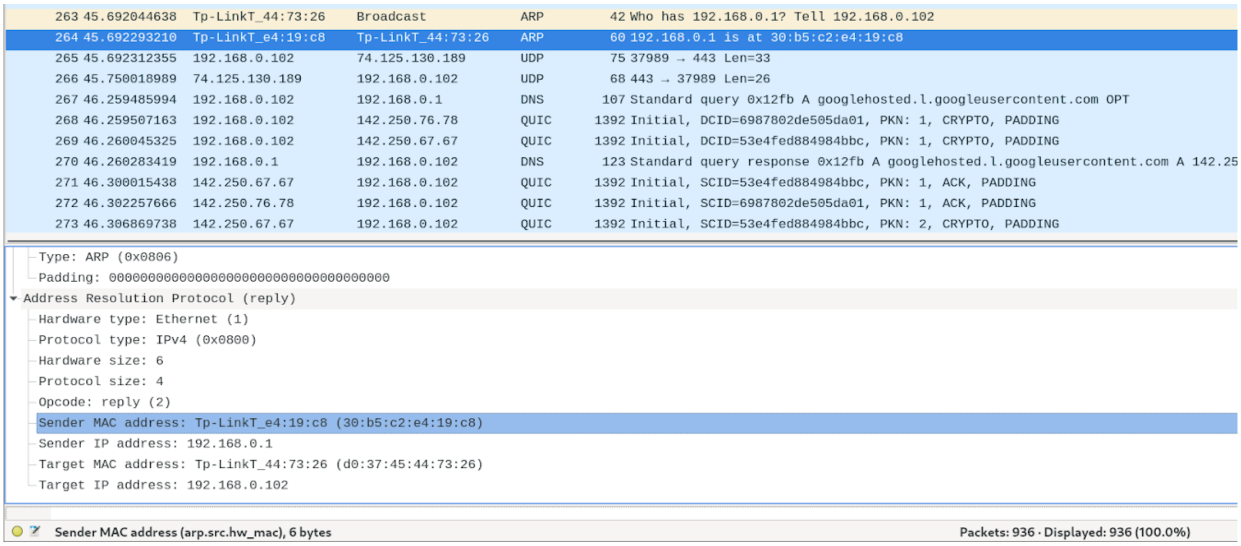


```
    262 44.090463942  74.125.130.189      192.168.0.102       UDP        68 443 → 37989 Len=26
    263 45.692044638  Tp-LinkT_44:73:26   Broadcast           ARP        42 Who has 192.168.0.1? Tell 192.168.0.102
    264 45.692293210  Tp-LinkT_e4:19:c8   Tp-LinkT_44:73:26   ARP        60 192.168.0.1 is at 30:b5:c2:e4:19:c8
    265 45.692312355  192.168.0.102       74.125.130.189      UDP        75 37989 → 443 Len=33
    266 45.750018989  74.125.130.189      192.168.0.102       UDP        68 443 → 37989 Len=26
    267 46.259485994  192.168.0.102       192.168.0.1         DNS       107 Standard query 0x12fb A googlehosted.l.googleusercontent.com OPT
    268 46.259507163  192.168.0.102       142.250.76.78       QUIC     1392 Initial, DCID=6987802de505da01, PKN: 1, CRYPTO, PADDING

▸ Frame 263: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s20f0u1c2, id 0
▾ Ethernet II, Src: Tp-LinkT_44:73:26 (d0:37:45:44:73:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)
    Type: ARP (0x0806)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)
    Sender IP address: 192.168.0.102
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.1

Ethernet (eth), 14 bytes                                  Packets: 936 · Displayed: 936 (100.0%) · Dropped: 0 (0.0%)      Profile: Defa
```

<u>PAYLOAD breakdown of an ARP request packet:</u>

1. **Hardware type:** Ethernet (1)
2. **Protocol**: IPV4
3. **Hardware size:** 6
4. **Protocol size**: 4
5. **Opcode**: 1
6. **Hardware (MAC) Source address:** d0:37:45:44:73:26
7. **Hardware (MAC) Destination address:** 00:00:00:00:00:00 (Since it is broadcasted to find the mac address of the destination)
8. **Protocol (IP) Source Address**: 192.168.0.102
9. **Protocol (IP) Destination Address**: 192.168.0.1

<u>PAYLOAD breakdown of an ARP reply packet:</u>



```
263 45.692044638  Tp-LinkT_44:73:26    Broadcast            ARP         42 Who has 192.168.0.1? Tell 192.168.0.102
264 45.692293210  Tp-LinkT_e4:19:c8    Tp-LinkT_44:73:26    ARP         60 192.168.0.1 is at 30:b5:c2:e4:19:c8
265 45.692312355  192.168.0.102        74.125.130.189       UDP         75 37989 → 443 Len=33
266 45.750018989  74.125.130.189       192.168.0.102        UDP         68 443 → 37989 Len=26
267 46.259485994  192.168.0.102        192.168.0.1          DNS        107 Standard query 0x12fb A googlehosted.l.googleusercontent.com OPT
268 46.259507163  192.168.0.102        142.250.76.78        QUIC      1392 Initial, DCID=6987802de505da01, PKN: 1, CRYPTO, PADDING
269 46.260045325  192.168.0.102        142.250.67.67        QUIC      1392 Initial, DCID=53e4fed884984bbc, PKN: 1, CRYPTO, PADDING
270 46.260283419  192.168.0.1          192.168.0.102        DNS        123 Standard query response 0x12fb A googlehosted.l.googleusercontent.com A 142.25
271 46.300015438  142.250.67.67        192.168.0.102        QUIC      1392 Initial, SCID=53e4fed884984bbc, PKN: 1, ACK, PADDING
272 46.302257666  142.250.76.78        192.168.0.102        QUIC      1392 Initial, SCID=6987802de505da01, PKN: 1, ACK, PADDING
273 46.306869738  142.250.67.67        192.168.0.102        QUIC      1392 Initial, SCID=53e4fed884984bbc, PKN: 2, CRYPTO, PADDING
```

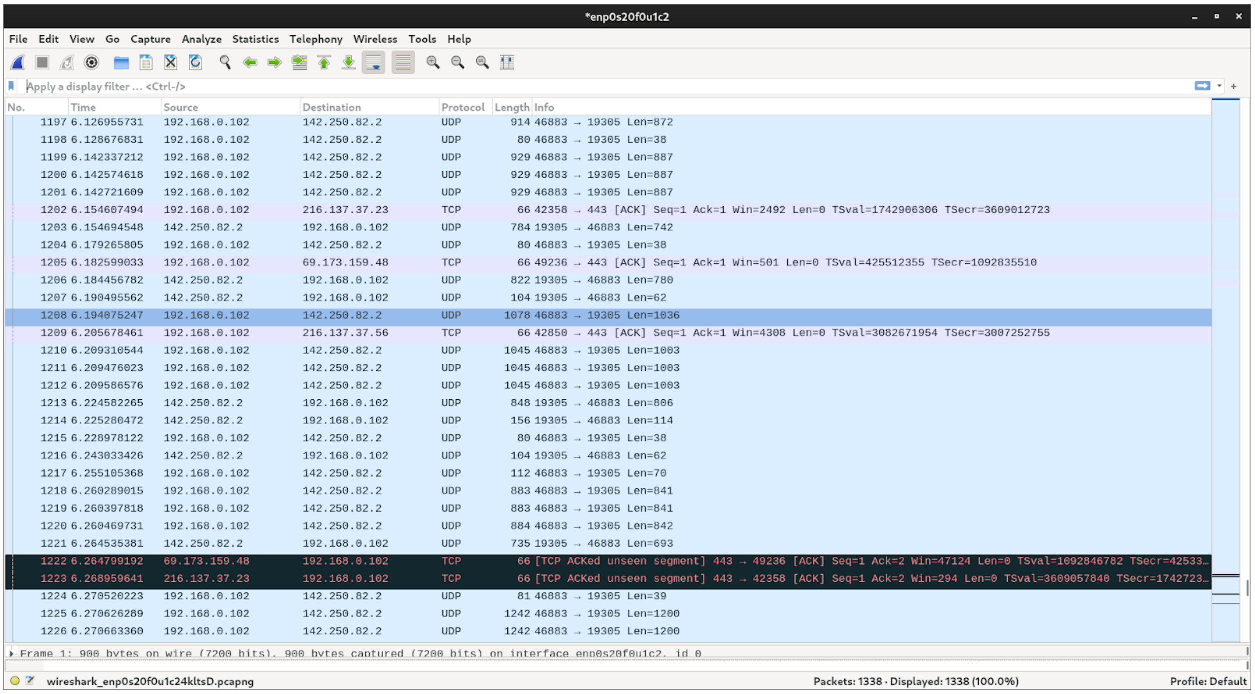
```
  Type: ARP (0x0806)
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Tp-LinkT_e4:19:c8 (30:b5:c2:e4:19:c8)
  Sender IP address: 192.168.0.1
  Target MAC address: Tp-LinkT_44:73:26 (d0:37:45:44:73:26)
  Target IP address: 192.168.0.102
```

```
Sender MAC address (arp.src.hw_mac), 6 bytes                    Packets: 936 · Displayed: 936 (100.0%)
```

1. **Hardware type:** Ethernet (1)
2. **Protocol**: IPV4
3. **Hardware size:** 6
4. **Protocol size**: 4
5. **Opcode**: 2
6. **Hardware (MAC) Source address**: 30:b5:c2:e4:19:c8
7. **Hardware (MAC) Destination address**: d0:37:45:44:73:26
8. **Protocol (IP) Source Address**: 192.168.0.1
9. **Protocol (IP) Destination Address:** 192.168.0.102

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

Ans.


*enp0s20f0u1c2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1197	6.126955731	192.168.0.102	142.250.82.2	UDP	914	46883 → 19305 Len=872
1198	6.128676831	192.168.0.102	142.250.82.2	UDP	80	46883 → 19305 Len=38
1199	6.142337212	192.168.0.102	142.250.82.2	UDP	929	46883 → 19305 Len=887
1200	6.142574618	192.168.0.102	142.250.82.2	UDP	929	46883 → 19305 Len=887
1201	6.142721609	192.168.0.102	142.250.82.2	UDP	929	46883 → 19305 Len=887
1202	6.154607494	192.168.0.102	216.137.37.23	TCP	66	42358 → 443 [ACK] Seq=1 Ack=1 Win=2492 Len=0 TSval=1742906306 TSecr=3609012723
1203	6.154694548	142.250.82.2	192.168.0.102	UDP	784	19305 → 46883 Len=742
1204	6.179265805	192.168.0.102	142.250.82.2	UDP	80	46883 → 19305 Len=38
1205	6.182599033	192.168.0.102	69.173.159.48	TCP	66	49236 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=425512355 TSecr=1092835510
1206	6.184456782	142.250.82.2	192.168.0.102	UDP	822	19305 → 46883 Len=780
1207	6.190495562	142.250.82.2	192.168.0.102	UDP	104	19305 → 46883 Len=62
1208	6.194075247	192.168.0.102	142.250.82.2	UDP	1078	46883 → 19305 Len=1036
1209	6.205678461	192.168.0.102	216.137.37.56	TCP	66	42850 → 443 [ACK] Seq=1 Ack=1 Win=4308 Len=0 TSval=3082671954 TSecr=3007252755
1210	6.209310544	192.168.0.102	142.250.82.2	UDP	1045	46883 → 19305 Len=1003
1211	6.209476023	192.168.0.102	142.250.82.2	UDP	1045	46883 → 19305 Len=1003
1212	6.209586576	192.168.0.102	142.250.82.2	UDP	1045	46883 → 19305 Len=1003
1213	6.224582265	142.250.82.2	192.168.0.102	UDP	848	19305 → 46883 Len=806
1214	6.225280472	142.250.82.2	192.168.0.102	UDP	156	19305 → 46883 Len=114
1215	6.228978122	192.168.0.102	142.250.82.2	UDP	80	46883 → 19305 Len=38
1216	6.243033426	142.250.82.2	192.168.0.102	UDP	104	19305 → 46883 Len=62
1217	6.255105368	192.168.0.102	142.250.82.2	UDP	112	46883 → 19305 Len=70
1218	6.260289015	192.168.0.102	142.250.82.2	UDP	883	46883 → 19305 Len=841
1219	6.260397818	192.168.0.102	142.250.82.2	UDP	883	46883 → 19305 Len=841
1220	6.260469731	192.168.0.102	142.250.82.2	UDP	884	46883 → 19305 Len=842
1221	6.264535381	142.250.82.2	192.168.0.102	UDP	735	19305 → 46883 Len=693
1222	6.264799192	69.173.159.48	192.168.0.102	TCP	66	[TCP ACKed unseen segment] 443 → 49236 [ACK] Seq=1 Ack=2 Win=47124 Len=0 TSval=1092846782 TSecr=42533…
1223	6.268959641	216.137.37.23	192.168.0.102	TCP	66	[TCP ACKed unseen segment] 443 → 42358 [ACK] Seq=1 Ack=2 Win=294 Len=0 TSval=3609057840 TSecr=1742723…
1224	6.270520223	192.168.0.102	142.250.82.2	UDP	81	46883 → 19305 Len=39
1225	6.270626289	192.168.0.102	142.250.82.2	UDP	1242	46883 → 19305 Len=1200
1226	6.270663360	192.168.0.102	142.250.82.2	UDP	1242	46883 → 19305 Len=1200

```
Frame 1: 900 bytes on wire (7200 bits), 900 bytes captured (7200 bits) on interface enp0s20f0u1c2, id 0
```

wireshark_enp0s20f0u1c24kltsD.pcapng   Packets: 1338 · Displayed: 1338 (100.0%)   Profile: Default

This is a screenshot of wireshark during an online video call. As we can see, there are both TCP and UDP packets.

UDP is used for voice and video, as it needs to be fast and not lagging, the reliability is compromised to get rid of the lag since more data is being sent.

TCP is used for sending text messages as it needs to be more reliable and lag is not a huge issue as the size of the data transfer is less

TCP is also used to initiate connection or to bypass some firewalls that block UDP packets