

# NETWORKS LAB ASSIGNMENT

Arjun Syam

B180031CS

## A. Comparing ARP packets and IP packets (MAC Headers)

The MAC address Header contains :

1. Destination MAC address
2. Source MAC Address
3. Type of Protocol

The TCP packets have an IPv4 type while the ARP packets have ARP type. The ARP packet is used to find the MAC address by the packet. You would notice the protocol ID for IP packet (TCP) is 6. For an ARP packet there is no protocol ID. but a type of packet as 0x0800

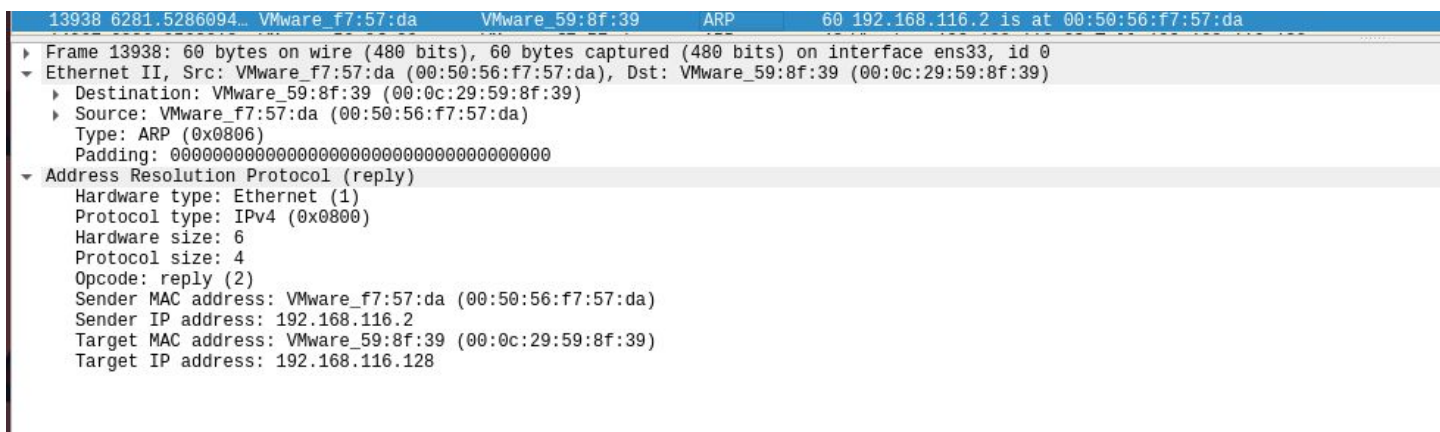


FIGURE : ARP PACKET

6169	74.264000110	202.88.235.13	192.168.116.128	TCP	2974 443 → 56374	[PSH, ACK]	Seq=1940544 Ack=2050
6170	74.264016888	192.168.116.128	202.88.235.13	TCP	54 56374 → 443	[ACK]	Seq=2050 Ack=1943464 Win=
6171	74.267399392	202.88.235.13	192.168.116.128	TCP	1514 443 → 56374	[PSH, ACK]	Seq=1943464 Ack=2050
6172	74.271086693	202.88.235.13	192.168.116.128	TCP	2974 443 → 56374	[PSH, ACK]	Seq=1944924 Ack=2050
6173	74.271101732	192.168.116.128	202.88.235.13	TCP	54 56374 → 443	[ACK]	Seq=2050 Ack=1947844 Win=
6174	74.277847968	202.88.235.13	192.168.116.128	TCP	1514 443 → 56374	[PSH, ACK]	Seq=1947844 Ack=2050
6175	74.281424085	202.88.235.13	192.168.116.128	TCP	1514 443 → 56374	[PSH, ACK]	Seq=1949304 Ack=2050
6176	74.281437603	192.168.116.128	202.88.235.13	TCP	54 56374 → 443	[ACK]	Seq=2050 Ack=1950764 Win=
6177	74.284549956	202.88.235.13	192.168.116.128	TCP	2974 443 → 56374	[PSH, ACK]	Seq=1950764 Ack=2050
6178	74.284693718	192.168.116.128	202.88.235.13	TCP	54 56374 → 443	[ACK]	Seq=2050 Ack=1953684 Win=
6179	74.288340511	202.88.235.13	192.168.116.128	TCP	1514 443 → 56374	[PSH, ACK]	Seq=1953684 Ack=2050
6180	74.291692190	202.88.235.13	192.168.116.128	TLSv1.3	1514 Application Data	[TCP segment of a reassemb	

- ▶ Frame 6170: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface ens33, id 0
- ▼ Ethernet II, Src: VMware\_59:8f:39 (00:0c:29:59:8f:39), Dst: VMware\_f7:57:da (00:50:56:f7:57:da)
  - ▶ Destination: VMware\_f7:57:da (00:50:56:f7:57:da)
  - ▶ Source: VMware\_59:8f:39 (00:0c:29:59:8f:39)
  - Type: IPv4 (0x0800)
- ▼ Internet Protocol Version 4, Src: 192.168.116.128, Dst: 202.88.235.13
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 40
  - Identification: 0xc319 (49945)
  - ▶ Flags: 0x4000, Don't fragment
  - Fragment offset: 0
  - Time to live: 64
  - Protocol: TCP (6)
  - Header checksum: 0x8d27 [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 192.168.116.128
  - Destination: 202.88.235.13
- ▶ Transmission Control Protocol, Src Port: 56374, Dst Port: 443, Seq: 2050, Ack: 1943464, Len: 0

FIGURE : IPv4 PACKET

### B. Destination of ARP packet

There can 3 destinations for an ARP packet

1. Broadcast where the request for the MAC address for the system is sent to a router having a network of systems

No.	Time	Source	Destination	Protocol	Length	Info
1059	65.023914027	VMware_59:8f:39	VMware_f3:29:16	ARP	42	Who has 192.168.116.254? Tell 192.168.116.128
1060	65.024445654	VMware_f3:29:16	VMware_59:8f:39	ARP	60	192.168.116.254 is at 00:59:56:f3:29:16
1349	137.472527824	VMware_f7:57:da	Broadcast	ARP	60	Who has 192.168.116.128? Tell 192.168.116.2
1341	137.472550721	VMware_59:8f:39	VMware_f7:57:da	ARP	42	192.168.116.128 is at 00:0c:29:59:8f:39
1601	224.511695908	VMware_59:8f:39	VMware_f7:57:da	ARP	42	Who has 192.168.116.2? Tell 192.168.116.128
1602	224.512150246	VMware_f7:57:da	VMware_59:8f:39	ARP	60	192.168.116.2 is at 00:50:56:f7:57:da

```

▶ Frame 1340: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface ens33, id 0
▼ Ethernet II, Src: VMware_f7:57:da (00:50:56:f7:57:da), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: VMware_f7:57:da (00:50:56:f7:57:da)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: VMware_f7:57:da (00:50:56:f7:57:da)
  Sender IP address: 192.168.116.2
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.116.128

```

2. A reply where the requested MAC address is sent back to the client.

No.	Time	Source	Destination	Protocol	Length	Info
3	5.166966030	VMware_59:8f:39	VMware_f7:57:da	ARP	42	Who has 192.168.116.2? Tell 192.168.116.128
4	5.167499719	VMware_f7:57:da	VMware_59:8f:39	ARP	60	192.168.116.2 is at 00:50:56:f7:57:da
230	53.529056966	VMware_f7:57:da	Broadcast	ARP	60	Who has 192.168.116.128? Tell 192.168.116.2
231	53.529081173	VMware_59:8f:39	VMware_f7:57:da	ARP	42	192.168.116.128 is at 00:0c:29:59:8f:39

▶ Frame 231: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface ens33, id 0

▼ Ethernet II, Src: VMware\_59:8f:39 (00:0c:29:59:8f:39), Dst: VMware\_f7:57:da (00:50:56:f7:57:da)

- ▶ Destination: VMware\_f7:57:da (00:50:56:f7:57:da)
- ▶ Source: VMware\_59:8f:39 (00:0c:29:59:8f:39)
- Type: ARP (0x0806)

▼ Address Resolution Protocol (reply)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2)
- Sender MAC address: VMware\_59:8f:39 (00:0c:29:59:8f:39)
- Sender IP address: 192.168.116.128
- Target MAC address: VMware\_f7:57:da (00:50:56:f7:57:da)
- Target IP address: 192.168.116.2

0000	00 50 56 f7 57 da 00 0c	29 59 8f 39 08 06 00 01	.PV.W... )Y.9....
0010	08 00 06 04 00 02 00 0c	29 59 8f 39 c0 a8 74 80	..... )Y.9...t.
0020	00 50 56 f7 57 da c0 a8	74 02	.PV.W... t.

3. A request to know the MAC address from the client to a specific IP address

arp						
No.	Time	Source	Destination	Protocol	Length	Info
1059	65.023914027	VMware_59:8f:39	VMware_f3:29:16	ARP	42	Who has 192.168.116.254? Tell 192.168.116.128
1060	65.024445654	VMware_f3:29:16	VMware_59:8f:39	ARP	60	192.168.116.254 is at 00:50:56:f3:29:16
1340	137.472527824	VMware_f7:57:da	Broadcast	ARP	60	Who has 192.168.116.128? Tell 192.168.116.2
1341	137.472550721	VMware_59:8f:39	VMware_f7:57:da	ARP	42	192.168.116.128 is at 00:0c:29:59:8f:39

Frame 1059: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface ens33, id 0
▼ Ethernet II, Src: VMware_59:8f:39 (00:0c:29:59:8f:39), Dst: VMware_f3:29:16 (00:50:56:f3:29:16)
Destination: VMware_f3:29:16 (00:50:56:f3:29:16)
Source: VMware_59:8f:39 (00:0c:29:59:8f:39)
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: VMware_59:8f:39 (00:0c:29:59:8f:39)
Sender IP address: 192.168.116.128
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.116.254

### C. Type of ARP packets

Here there are 2 ARP packets: a request and a reply. The 1 and 3 are requests and the 2 is a reply. The first is a request broadcasted to all devices; the 3 is to one device and the 2 is a reply, i.e. the MAC address from the device back.

### D. Payloads of ARP packets

The Payload contains

Payload of ARP Request Packet

MAC Address of the sender : 00:50:56:f7:57:da

IP address of the sender : 192.168.116.2

MAC address of the the receiver : 00:00:00:00:00:00

IP address of the receiver : 192.168.116.128

arp						
No.	Time	Source	Destination	Protocol	Length	Info
1059	65.023914027	VMware_59:8f:39	VMware_f3:29:16	ARP	42	Who has 192.168.116.254? Tell 192.168.116.128
1060	65.024445654	VMware_f3:29:16	VMware_59:8f:39	ARP	60	192.168.116.254 is at 00:50:56:f3:29:16
1340	137.472527824	VMware_f7:57:da	Broadcast	ARP	60	Who has 192.168.116.128? Tell 192.168.116.2
1341	137.472550721	VMware_59:8f:39	VMware_f7:57:da	ARP	42	192.168.116.128 is at 00:0c:29:59:8f:39
1601	224.511695908	VMware_59:8f:39	VMware_f7:57:da	ARP	42	Who has 192.168.116.2? Tell 192.168.116.128
1602	224.512150246	VMware_f7:57:da	VMware_59:8f:39	ARP	60	192.168.116.2 is at 00:50:56:f7:57:da

▶ Frame 1340: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface ens33, id 0
▼ Ethernet II, Src: VMware_f7:57:da (00:50:56:f7:57:da), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Source: VMware_f7:57:da (00:50:56:f7:57:da)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000
▼ Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: VMware_f7:57:da (00:50:56:f7:57:da)
Sender IP address: 192.168.116.2
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.116.128

Payload of the ARP reply packet

MAC Address of the sender : 00:0c:29:59:8f:39

IP address of the sender : 192.168.116.128

MAC address of the the receiver : 00:50:56:f7:57:da

IP address of the receiver : 192.168.116.2

No.	Time	Source	Destination	Protocol	Length	Info
3	5.166966030	VMware_59:8f:39	VMware_f7:57:da	ARP	42	Who has 192.168.116.2? Tell 192.168.116.128
4	5.167499719	VMware_f7:57:da	VMware_59:8f:39	ARP	60	192.168.116.2 is at 00:50:56:f7:57:da
230	53.529056966	VMware_f7:57:da	Broadcast	ARP	60	Who has 192.168.116.128? Tell 192.168.116.2
231	53.529081173	VMware_59:8f:39	VMware_f7:57:da	ARP	42	192.168.116.128 is at 00:0c:29:59:8f:39

▶ Frame 231: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface ens33, id 0 ▼ Ethernet II, Src: VMware_59:8f:39 (00:0c:29:59:8f:39), Dst: VMware_f7:57:da (00:50:56:f7:57:da) ▶ Destination: VMware_f7:57:da (00:50:56:f7:57:da) ▶ Source: VMware_59:8f:39 (00:0c:29:59:8f:39) Type: ARP (0x0806) ▼ Address Resolution Protocol (reply) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: reply (2) Sender MAC address: VMware_59:8f:39 (00:0c:29:59:8f:39) Sender IP address: 192.168.116.128 Target MAC address: VMware_f7:57:da (00:50:56:f7:57:da) Target IP address: 192.168.116.2
--

0000	00 50 56 f7 57 da 00 0c	29 59 8f 39 08 06 00 01	.PV.W... )Y.9....
0010	08 00 06 04 00 02 00 0c	29 59 8f 39 c0 a8 74 80	..... )Y.9...t.
0020	00 50 56 f7 57 da c0 a8	74 02	.PV.W... t.

## E. Skype and Zoom

Skype uses TCP to initiate connection or bypass any firewalls and use UDP to send audio and video over UDP. Firewalls block UDP because of the connectionless nature of UDP. UDP is a connection less protocol.

Zoom also uses combination of TCP and UDP, UDP are encrypted using a key negotiated over TLS