

Name : MOHAMMED TOUSIF  
Roll: CB.EN.P2CYS22008

## ARP USING WIRESHARK

Date :- 05-11-2022

Aim :- To understand ARP(Address Resolution Protocol) using wireshark.

Tools Required :- Windows OS , Wireshark.

Procedure :-

Using arp.pcap file.

1. Answer the following questions based on the contents of the Ethernet frame containing the HTTP GET message.

a. What is the 48-bit Ethernet address of your computer?

```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (
> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst:
> Data (672 bytes)
```

**The 48-bit Ethernet address is : 00:d0:59:a9:3d:68**

b. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68),
  Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
    Address: LinksysG da:af:73 (00:06:25:da:af:73)
```

**The 48-bit Ethernet address is : 00:06:25:da:af:73**

**It is the address of router or gateway that getting request from the source computer.**

c. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

```
Ethernet II, Src: AmbitMic_a
> Destination: LinksysG_da:
> Source: AmbitMic_a9:3d:68
Type: IPv4 (0x0800)
Data (48 bytes)
```

**The hexadecimal value is : 0x0800 and it corresponds to IPv4 protocol.**

2. Answer the following questions based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

a. What is the value of the Ethernet source address?

|    |          |                 |                   |                   |        |      |      |
|----|----------|-----------------|-------------------|-------------------|--------|------|------|
| 11 | 2004/241 | 22:49:37.651896 | LinksysG_da:af:73 | AmbitMic_a9:3d:68 | 0x0800 | 60   | IPv4 |
| 12 | 2004/241 | 22:49:37.656065 | LinksysG_da:af:73 | AmbitMic_a9:3d:68 | 0x0800 | 1514 | IPv4 |
| 13 | 2004/241 | 22:49:37.657155 | LinksysG_da:af:73 | AmbitMic_a9:3d:68 | 0x0800 | 1514 | IPv4 |

```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:
> Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:
> Source: LinksysG_da:af:73 (00:06:25:da:af:73)
Type: IPv4 (0x0800)
```

**Value of Ethernet source address is : 00:06:25:da:af:73**

b. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

**The destination address is : 00:d0:59:a9:3d:68**

```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst:
> Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
```

c. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

```
Ethernet II, Src: LinksysG_da
> Destination: AmbitMic_a9:3d
> Source: LinksysG_da:af:73 (
Type: IPv4 (0x0800)
```

**Hexadecimal value: 0x0800 corresponding to IPv4 protocol.**

3. Answer the following questions based on the contents of the ARP Request packets.

a. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

| Destination | Protocol | Length | Info                                    |
|-------------|----------|--------|---|
| Broadcast   | ARP      | 42     | Who has 192.168.1.1? Tell 192.168.1.105 |

Wireshark · Packet 1 · ARP

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

**Source address : 00:d0:59:a9:3d:68**

**Destination address : ff:ff:ff:ff:ff:ff**

b. Give the hexadecimal value for the two-byte Ethernet Frame type field.

**Hexadecimal value : 0x0806**

- ▼ Ethernet II, Src: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast
  - > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  - > Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)
  - Type: ARP (0x0806)

c. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

|      |   |                |
|------|---|----------------|
| 0000 | ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 | ..... Y.=h.... |
| 0010 | 08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 | ..... Y.=h...i |
| 0020 | 00 00 00 00 00 00 c0 a8 01 01                   | ..... ..       |

Bytes 20-21: Opcode (arp.opcode)

☒ Show packet bytes

As shown Bytes 20-21 is the Opcode byte and ARP opcode field begins at 20<sup>th</sup> Byte.

d. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

|   |   |                |
|---|---|----------------|
| Opcode: request (1)                                       |   |                |
| Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) |   |                |
| Sender IP address: 192.168.1.105                          |   |                |
| Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00) |   |                |
| Target IP address: 192.168.1.1                            |   |                |
| 0000  | ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 | ..... Y.=h.... |
| 0010  | 08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 | ..... Y.=h...i |
| 0020  | 00 00 00 00 00 00 c0 a8 01 01                   | ..... ..       |

e. Does the ARP message contain the IP address of the sender?

```
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  Sender IP address: 192.168.1.105
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 00:00:00:00:00:00 (00:00:00:00:00:00)
```

**Yes , It is 192.168.1.105**

f. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

```
Who has 192.168.1.1? Tell 192.168.1.105
Wireshark · Packet 1 · ARP
.....0..... = IG bit: Individual address
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: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  Sender IP address: 192.168.1.105
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.1
```

4. Answer the following questions based on the contents of the ARP Reply packets.

a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

It begins at 20<sup>th</sup> field.

|   |  |  |  |  |  |  |  |  |  |  |  |
|---|--|--|--|--|--|--|--|--|--|--|--|
| Opcode: reply (2)   |  |  |  |  |  |  |  |  |  |  |  |
| Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73) |  |  |  |  |  |  |  |  |  |  |  |
| Sender IP address: 192.168.1.1                            |  |  |  |  |  |  |  |  |  |  |  |
| Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) |  |  |  |  |  |  |  |  |  |  |  |
| Target IP address: 192.168.1.105                          |  |  |  |  |  |  |  |  |  |  |  |

|      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |                  |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 0000 | 00 | d0 | 59 | a9 | 3d | 68 | 00 | 06 | 25 | da | af | 73 | 08 | 06 | 00 | 01 | ..Y.=h.. %..s... |
| 0010 | 08 | 00 | 06 | 04 | 00 | 02 | 00 | 06 | 25 | da | af | 73 | c0 | a8 | 01 | 01 | ..... %..s...    |
| 0020 | 00 | d0 | 59 | a9 | 3d | 68 | c0 | a8 | 01 | 69 | 00 | 00 | 00 | 00 | 00 | 00 | ..Y.=h.. .i..... |
| 0030 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |

b. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

Opcode: reply (2)  
 Sender MAC address: LinksysG\_da:af:73 (00:06:25:da:af:73)  
 Sender IP address: 192.168.1.1

**Value of Opcode field is : 2**

c. Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

Address Resolution Protocol (reply)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: reply (2)  
 Sender MAC address: LinksysG\_da:af:73 (00:06:25:da:af:73)  
 Sender IP address: 192.168.1.1  
 Target MAC address: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  
 Target IP address: 192.168.1.105

This packet has answer of IP address of machine having Ethernet address whose corresponding IP address is being queried.

d. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

```
Source: LinksysG_da:af:73 (00:06:25:da:af:73)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000
dress Resolution Protocol (reply)
```

```
00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01 ..Y.=h..%..s....
```

```
Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Source: LinksysG_da:af:73 (00:06:25:da:af:73)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000
dress Resolution Protocol (reply)
```

```
00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01 ..Y.=h..
```

**Hexadecimal values of Source address : 00 06 25 da af 73**

**Hexadecimal values of Destination address : 00 d0 59 a9 3d 68**

e. There is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

|   |          |                 |                   |           |     |    |   |
|---|----------|-----------------|-------------------|-----------|-----|----|---|
| 6 | 2004/241 | 22:49:33.700104 | CnetTech_73:8d:ce | Broadcast | ARP | 60 | Who has 192.168.1.117? Tell 192.168.1.104 |
|---|----------|-----------------|-------------------|-----------|-----|----|---|

As this traffic is captured from the computer of IP .105. There is no ARP reply for the 6<sup>th</sup> packet request. Because ARP request is sent as Broadcast. But the reply/response is sent as Unicast by the corresponding computer.

As reply is sent as Unicast, Other computers can't capture the reply message of that computer. Thus , we couldn't see the ARP reply.

Result : Thus , understanding Address Resolution Protocol (ARP) using wireshark is successfully done.