

21CY681– Internet Protocol lab

ASSIGNMENT -6

Name: B.Shebu

Register Number : CYS22005

Title: Understanding ARP using wireshark

Date of Assignment provided: 05/11/2022

Aim: Analysing ARP request and response using wireshark.

PROCEDURE -

Use the provided pcap file (Arp) to answer the following questions.

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 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Type: ARP (0x0806)
```

The 48 bit ethernet address of the source computer 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?

```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits) on interface 0
> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Type: IPv4 (0x0800)
```

The 48 bit destination address in the Ethernet frame is 00:06:25:da:af:73 which is the address of the router/gateway

```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits) on interface 0
> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Type: IPv4 (0x0800)
Data (672 bytes)
Data: 450002a000fa0008006bfc8c0a801698077f50c04220050651499a7aca53fb45018faf0...
[Length: 672]
```

No this is the address of the router/gateway to which the source computer is sending the request. From there it gets transferred to the destination computer.

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

```

Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
.... ..0. .... = LG bit: Globally unique address (factory default)
0
.... ..0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Data (48 bytes)
Data: 4500003000f3400080063af3c0a80169c70235ce0421027764d17e0b00000007002faf0...
[Length: 48]
0000 00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00  ..%..s.. Y.=h..E.
0010 00 30 00 f3 40 00 80 06 3a f3 c0 a8 01 69 c7 02  .0..@... :....i..
0020 35 ce 04 21 02 77 64 d1 7e 0b 00 00 00 00 70 02  5..!-wd- ~....p.
0030 fa f0 df d7 00 00 02 04 05 b4 01 01 04 02  ....

```

The hex value of the 2 byte frame field is 0x0800 . 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?

```

10 2004/241 17:19:37.656552 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800  60  IPv4
11 2004/241 17:19:37.651896 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800  60  IPv4
12 2004/241 17:19:37.656065 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800  1514 IPv4
13 2004/241 17:19:37.657155 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800  1514 IPv4
14 2004/241 17:19:37.657199 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800  54  IPv4
15 2004/241 17:19:37.684187 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800  1514 IPv4
16 2004/241 17:19:37.684552 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800  489  IPv4
.... ..0. .... = IG bit: Individual
Source: LinksysG_da:af:73 (00:06:25:da:af:73)
Address: LinksysG_da:af:73 (00:06:25:da:af:73)

```

The value of ethernet source address in reply packet 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?

```

[Protocols in frame: eth:ethertype:data]
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

```

The Ethernet address of destination in reply packet is 00:d0:59;a9:ed:68

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

```

Source: LinksysG_da:af:73 (00:06:25:da:af:73)
Address: LinksysG_da:af:73 (00:06:25:da:af:73)
.... ..0. .... = LG bit: Globally unique address
0
.... ..0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Data (1500 bytes)
Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb46!

```

The hex value of the two byte frame field is 0x0800. It corresponds to IPV4 layer.

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

The address of

Source -> 00:d0:59:a9:3d:6d

Destination -> ff:ff:ff:ff:ff:ff

Type: ARP (0x0806)
 Padding: 00000000000000000000000000000000
 Address Resolution Protocol (reply)

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99
0000	00	d0	59	a9	3d	68	00	06	25	da	af	73	08	06	00	01																																																																																				
0004	08	00	06	04	00	02	00	06	25	da	af	73	c0	a8	01	01																																																																																				

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

```
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: 00:00:00:00:00:00 (00:00:00:00:00:00)
```

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..
0020	00 00 00 00 00 00	c0 a8 01 01	

On clicking the OPCODE field we get to see the hex values 20-21. On clicking the hex values we see that the OPCODE field begins at 20 th field

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?

```
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

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...
0020  00 00 00 00 00 00 c0 a8 01 01  ....
```

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

```
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
```

Yes it contains the sender IP address .

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

```
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
```

From the above we can see that the request where the sender asks which system has the 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?

```
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
```

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

It begins at 20-21 st field

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?

```
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
```

The value of the OPCODE field within the arp payload in response packet 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?

```
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
```

We can confirm that this packet contains the answer since it contains both the sender and receiver’s MAC address along with their IP address.

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

```

.... 0 .... = IG bit: Individual address (unicast)
✓ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
  Address: LinksysG_da:af:73 (00:06:25:da:af:73)
  .... 0 .... = LG bit: Globally unique address (factory default)
  .... 0 .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 00000000000000000000000000000000
✓ Address Resolution Protocol (reply)
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 .....

```

The hex value of the source address is 00 06 25 da af 73

```

✓ Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  .... 0 .... = LG bit: Globally unique address (factory default)
  .... 0 .... = IG bit: Individual address (unicast)
✓ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
  Address: LinksysG_da:af:73 (00:06:25:da:af:73)
  .... 0 .... = LG bit: Globally unique address (factory default)
  .... 0 .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 00000000000000000000000000000000
Address Resolution Protocol (reply)
000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01 ..Y=h.. %..s...
010 08 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01 ..... %..s...
020 00 d0 59 a9 3d 68 c0 a8 01 69 00 00 00 00 00 00 ..Y=h.. -i.....
030 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

The value of the destination address is 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

3	2004/241	17:19:20.158158	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2004/241	17:19:23.119980	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	2004/241	17:19:29.128618	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	2004/241	17:19:33.700104	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	2004/241	17:19:37.601553	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	2004/241	17:19:37.623032	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	2004/241	17:19:37.623057	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	2004/241	17:19:37.623598	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	2004/241	17:19:37.651896	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	2004/241	17:19:37.656065	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	2004/241	17:19:37.657155	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
14	2004/241	17:19:37.657199	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
15	2004/241	17:19:37.684187	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
16	2004/241	17:19:37.684552	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4
17	2004/241	17:19:37.684587	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4

There is no response for the second ARP request packet because ARP request packet is a broadcast message and the arp response is unicast . So the computer which has the ip that is queried by the

server will send a unicast response packet back to the router. So since the traffic is captured from this computer which has the ip .105 we are not able to see the reply arp packet which is sent back.

RESULT –

Thus the experiment to understand ARP requests and responses have been done successfully.