## 21CY681 - INTERNET PROTOCOL LAB - VI

Name: KARTHIKA P Date: 5th October 2022

Assignment Topic: To USE WIRESHARK AND ANALYSE VARIOUS ARP

PACKETS AND PROTOCOL

Register Number: CB. EN. P2CYS22001

- 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?

```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Links
> 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)
```

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 3: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

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)
```

The destination address is LinksysG\_da (00:06:25:da:af:73)

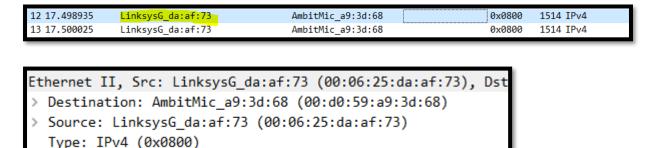
The address which we got is the routers address because source is sending the request to the router and then it is transferred to the detination server.

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

```
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
```

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

- 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?



The value of Ethernet source address is (00:d0:59:a9:3d:68).

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

```
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)
> Source: LinksysG_da:af:73 (00:06:25:da:af:73)
   Type: IPv4 (0x0800)
```

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

The upper layer protocol is ipv4.

- 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?

```
Fethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff)
> Destination: Broadcast (ff:ff:ff:ff:ff)
> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: ARP (0x0806)
```

The address of source:00:d0:59:a9:3d:68

The address of destination:ff:ff:ff:ff

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

The hex value of the two byte field is 0x0806.

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

```
Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

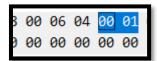
Hardware size: 6

Protocol size: 4

Opcode: request (1)
```

By clicking the opcode we will get hexa value as 00 01. Then bytes will be IN The range 20-21.

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?



00 00 00 00 00 00

```
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
```

The value of opcode is 20-21 bytes field.

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

```
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
```

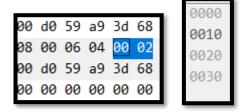
Yes, it contain the IP address of sender.

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
```

The target ip address is where in arp request question appear.

- 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?



The bytes for the opcode field begin is 20-21.

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
```

The value of opcode payload in ARP is 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?

```
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 reveiver'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?

```
00 d0 59 a9 3d 68 00 06
08 00 06 04 00 02 00 06
00 d0 59 a9 3d 68 c0 a8
00 00 00 00 00 00 00 00
```

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

```
a9 3d 68 00 06 25 da af 73 08 04 00 02 00 06 25 da af 73 c0 a9 3d 68 c0 a8 01 69 00 00 00
```

The value of source address is 00:06:25:da:af:73.

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.

.000000	AmbitMic_a9:3d:68	Broadcast	AKP	42 Who has 192.168.1.1? Tell 192.168.1.105
7.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54 IPv4
7.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54 IPv4
7.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54 IPv4
.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60 192.168.1.1 is at 00:06:25:da:af:73
3.542974	CnetTech_73:8d:ce	Broadcast	ARP	60 Who has 192.168.1.117? Tell 192.168.1.104
7.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60 IPv4
.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62 IPv4
.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62 IPv4
.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62 IPv4
7.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62 IPv4
7.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62 IPv4
7.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489 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 number 105 we are not able to see the reply arp packet which is sent back.