

INTERNET PROTOCOL LAB ASSIGNMENT -6

Name: Siriparapu Sparshika

Roll No: CYS22006

Date: 05-11-2022

TITLE: **Analyzing ARP request and response using Wireshark**

AIM:

To analyze ARP request and response using Wireshark.

PROCEDURE:

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?

48-bit ethernet address of the source computer is 00:d0:59:a9:3d:68

```
[Protocols in frame: eth:ethertype:data]
▼ 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 (0x0000)
▼ Data (672 bytes)
  Data: 450002a000fa40008006bfc8c0a801698077f50c04220050651499a7aca53fb45018faf0...
```

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)
v 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: TPv4 (0x0800)
```

0000	00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00	..%.s..Y=h..E..
0010	02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77@....i-w
0020	f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18	...".Pe-...?P.
0030	fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72	...~0..GE T/ether
0040	65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74	eal-labs /HTTP-et
0050	68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33	hereal-l ab-file3
0060	2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HT TP/1.1..
0070	48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d	Host: ga ia.cs.um
0080	61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67	ass.edu- User-Ag
0090	65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30	ent: Moz illa/5.0
00a0	20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69	(Window s; U; Wi
00b0	6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e	ndows NT 5.1; en

Router mac's address

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

Ipv4 – 0x0800 – ethernet frame – 2 byte frame field

```
16 0.000365 LinksysG_da:af:73 AmbitMic_a9:3d:68 0x0800 489 IPv4
```

0000	00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00	..%.s..Y=h..E..
0010	02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77@....i-w
0020	f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18	...".Pe-...?P.
0030	fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72	...~0..GE T/ether
0040	65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74	eal-labs /HTTP-et
0050	68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33	hereal-l ab-file3
0060	2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HT TP/1.1..
0070	48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d	Host: ga ia.cs.um
0080	61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67	ass.edu- User-Ag
0090	65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30	ent: Moz illa/5.0
00a0	20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69	(Window s; U; Wi
00b0	6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e	ndows NT 5.1; en
00c0	2d 55 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47	-US; rv: 1.0.2) G
00d0	65 63 6b 6f 2f 32 30 30 33 30 32 30 38 20 4e 65	ecko/200 30208 Ne
00e0	74 73 63 61 70 65 2f 37 2e 30 32 0d 0a 41 63 63	tscape/7 .02..Acc
00f0	65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c 61 70	ept: tex t/xml,ap
0100	70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70	plicatio n/xml,ap
0110	70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b	plicatio n/xhtml+
0120	78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d	xml;text /html;q=
0130	30 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e 3b 71	0.9;text /plain;q
0140	3d 30 2e 38 2c 76 69 64 65 6f 2f 78 2d 6d 6e 67	=0.8,vid eo/x-mng
0150	2c 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65	,image/p ng,image
0160	2f 6a 70 65 67 2c 69 6d 61 67 65 2f 67 69 66 3b	/jpeg,image/gif;

Type (eth.type), 2 bytes Packets: 17 - Displayed: 17 (100.0%)

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?

8	0.021479	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	0.000025	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	0.000541	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	0.028298	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	0.004169	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	0.001090	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
14	0.000044	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
15	0.026988	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
16	0.000365	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4

ethernet source address in reply packet is 00:06:25:da:af:73

> Source: LinksysG_da:af:73 (00:06:25:da:af:73)	0110	69	76	65	3a	20	74	69	6d
Type: IPv4 (0x0800)	0120	20	6d	61	78	3d	31	30	30
▼ Data (1500 bytes)	0130	74	69	6f	6e	3a	20	4b	65
	0140	84	8a	a3	6f	6a	74	65	6a

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

of your computer?

Yes, it's the ethernet address of my 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)
> Source: LinksysG_da:af:73 (00:06:25:da:af:73)
Type: IPv4 (0x0800)
▼ Data (1500 bytes)
Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b28...
[Length: 1500]

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

[Frame is marked: False]
[Frame is ignored: False]
[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)
> Source: LinksysG_da:af:73 (00:06:25:da:af:73)
Type: IPv4 (0x0800)
▼ Data (1500 bytes)
Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b28...
[Length: 1500]

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?

The address of

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

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

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	28	Request from 192.168.1.1 to 192.168.1.100
5	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
6	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
7	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
8	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
9	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
10	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
11	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
12	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
13	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
14	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
15	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
16	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100
17	0.000000	LinksysG_da:af:73	LinksysG_da:af:73	ARP	62	Reply to 192.168.1.1 from 192.168.1.100

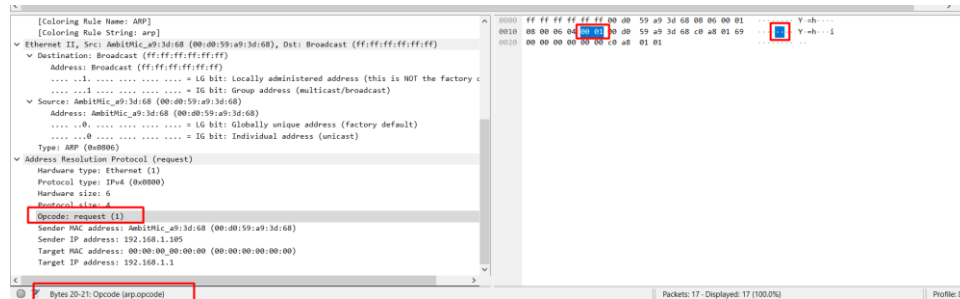
b. Give the hexadecimal value for the two-byte Ethernet Frame type field.

- [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)

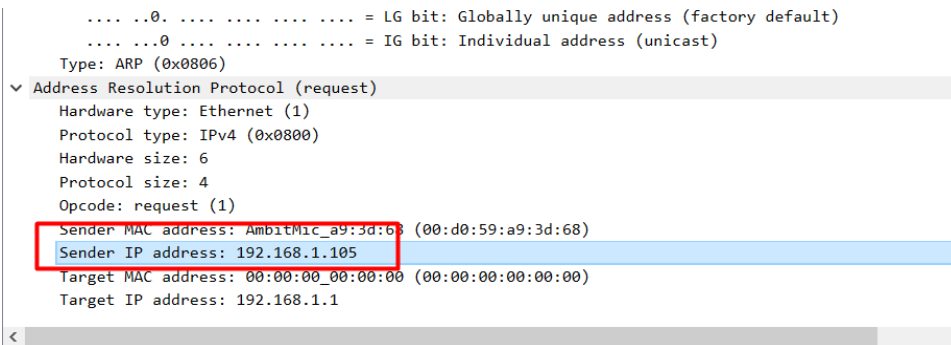
c. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

[Coloring Rule Name: ARP]	
[Coloring Rule String: arp]	
▼ 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)	
Address: Broadcast (ff:ff:ff:ff:ff:ff)	
...1 ...0 ...0 ...0 ...0 ...0 = IG bit: Locally administered address (this is NOT the factory default)	
...1 ...0 ...0 ...0 ...0 ...0 = IG bit: Group address (multicast/broadcast)	
▼ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)	
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)	
...0 ...0 ...0 ...0 ...0 ...0 = IG bit: Globally unique address (factory default)	
...0 ...0 ...0 ...0 ...0 ...0 = IG bit: Individual address (unicast)	
Type: ARP (0x0806)	
▼ Address Resolution Protocol (request)	
Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 6	
Opcode: request (1)	
Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)	
Sender IP address: 192.168.1.100	
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)	
Target IP address: 192.168.1.1	

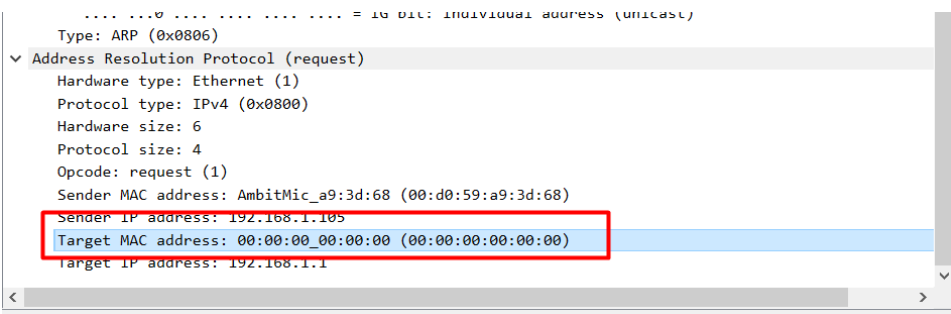
d. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?



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

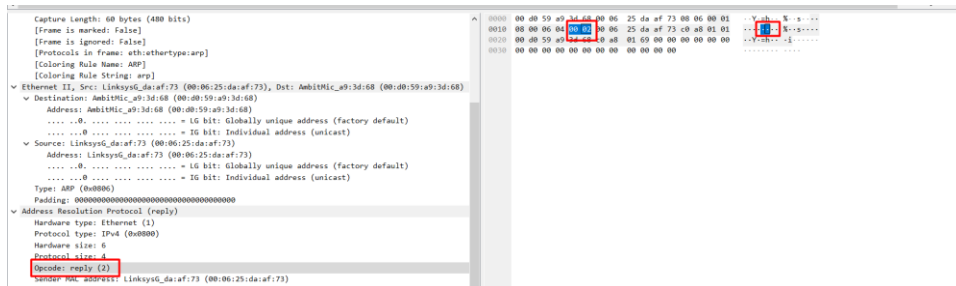


f. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

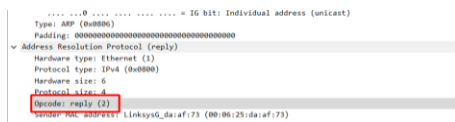


4. Answer the following questions based on the contents of the ARP Reply packets.

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



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?



By analyzing send mac address along with sender Ip address

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

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 25 da af 73	08 06 00 00	00 d0 59 a9 3d 68	00 06 25 da af 73	08 06 00 01
08 00 06 04 00 02	00 06 25 da af 73	c0 a8 01 00	00 d0 59 a9 3d 68	c0 a8 01 69	00 00 00 00
00 d0 59 a9 3d 68	c0 a8 01 69	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00

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?

No.	Time	Source	Src. code	Destination	Dst. code	Distance	Length	Info
1	0.000000	AmbiTMic_a9:3d:68		Broadcast		42	Who has 192.168.1.1? Tell 192.168.1.105	
2	0.000018	Linksys0_daf:73		AmbiTMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:00:25:da:af:73	
3	0.000038	AmbiTMic_a9:3d:68		Linksys0_daf:73	0x0000	62	IPv4	
4	2.961822	AmbiTMic_a9:3d:68		Linksys0_daf:73	0x0000	62	IPv4	
5	6.000638	AmbiTMic_a9:3d:68		Linksys0_daf:73	0x0000	62	IPv4	
6	4.571486	CnetTech_73:8d:cce		Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104	
7	3.981449	AmbiTMic_a9:3d:68		Linksys0_daf:73	0x0000	62	IPv4	
8	0.021479	Linksys0_daf:73		AmbiTMic_a9:3d:68	0x0000	62	IPv4	
9	0.000025	AmbiTMic_a9:3d:68		Linksys0_daf:73	0x0000	54	IPv4	
10	0.000541	AmbiTMic_a9:3d:68		Linksys0_daf:73	0x0000	606	IPv4	
11	0.020298	Linksys0_daf:73		AmbiTMic_a9:3d:68	0x0000	60	IPv4	
12	0.004169	Linksys0_daf:73		AmbiTMic_a9:3d:68	0x0000	1514	IPv4	
13	0.001090	Linksys0_daf:73		AmbiTMic_a9:3d:68	0x0000	1514	IPv4	
14	0.000044	AmbiTMic_a9:3d:68		Linksys0_daf:73	0x0000	54	IPv4	
15	0.020988	Linksys0_daf:73		AmbiTMic_a9:3d:68	0x0000	1514	IPv4	
16	0.000365	Linksys0_daf:73		AmbiTMic_a9:3d:68	0x0000	489	IPv4	
17	0.000035	AmbiTMic_a9:3d:68		Linksys0_daf:73	0x0000	54	IPv4	

There is no response for the second ARP request packet because ARP request packet - broadcast
message - arp response is unicast.

The computer which has the ip that is queried by the server will send a unicast response packet back to the router.

RESULT:

Thus, ARP requests and responses have been done observed successfully using Wireshark.