# Lab 6 Wireshark Ethernet ARP v8.0

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

**Answer:** 00:d0:59:a9:3d:68.

No.	Time	Source	Destination	Protocol	Length	Info
	1 0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
	2 0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
	3 0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	Pv4
	4 2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	Pv4
	5 8.971488	AmbitMic a9:3d:68	LinksysG da:af:73	0x0800	62	Pv4
> Fra	me 3: 62 bytes	on wire (496 bits), 6	2 bytes captured (496	bits)		
Y Eth	ernet II, Src:	AmbitMic_a9:3d:68 (00	:d0:59:a9:3d:68), Dst	: Linksys	G_da:af	f:73 (00:06:25:da:af:73)
>	Destination: Li	inksysG_da:af:73 (00:0	6:25:da:af:73)			
>	Source: AmbitMi	ic_a9:3d:68 (00:d0:59:	a9:3d:68)			
	Type: IPv4 (0x0	9800)				
> Dat	a (48 bytes)					

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?

# Answer:

- 00:06:25:da:af:73
- It is the address of my Linksys router, which is the link used to get off the subnet.

No.	Time	Source	Destination	Protocol	Length	Info
	1 0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
	2 0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
	3 0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	Pv4
	4 2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	Pv4
	5 8.971488	AmbitMic a9:3d:68	LinksysG da:af:73	0x0800	62	Pv4
	•	on wire (496 bits), 6 AmbitMic a9:3d:68 (00			G da:af	f:73 (00:06:25:da:af:73)
> 5		inksysG_da:af:73 (00:0 ic_a9:3d:68 (00:d0:59: 0800)		•	_	· ,
> Data	a (48 bytes)					

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

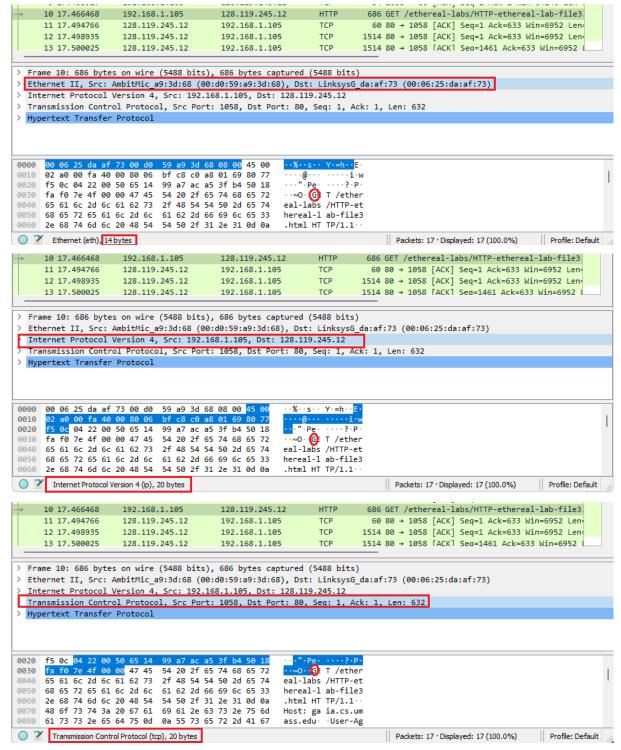
**Answer:** The hex value for the Frame type field is 0x0800

No.	Time	Source	Destination	Protocol	Length	Info
	1 0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
	2 0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
	3 0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
	4 2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
	5 8.971488	AmbitMic a9:3d:68	LinksysG da:af:73	0x0800	62	IPv4
V Eth	nernet II, Src: Destination: Li Source: Am <mark>bit</mark> Mi	inksysG_da:af:73 (00:0 ic_a9:3d:68 (00:d0:59:	:d0:59:a9:3d:68), Dst 6:25:da:af:73)		G_da:a1	f:73 (00:06:25:da:af:73)
> Eth	nernet II, Src: Destination: Li	AmbitMic_a9:3d:68 (00 inksysG_da:af:73 (00:0 ic_a9:3d:68 (00:d0:59:	:d0:59:a9:3d:68), Dst 6:25:da:af:73)		G_da:af	f:73 (00:06:25:da:af:73)

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

# Answer:

- The ASCII "G" appears 54 bytes from the start of the ethernet frame.
- There are 14 B Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.



5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

#### Answer:

- 00:06:25:da:af:73

- It is the address of my Linksys router, which is the link used to get onto my subnet

```
14 17.500069
                     AmbitMic_a9:3d:68 LinksysG_da:af:73
                                                              0x0800
                                                                          54 IPv4
     15 17.527057
                     LinksysG da:af:73
                                        AmbitMic a9:3d:68
                                                               0x0800
                                                                        1514 IPv4
     16 17.527422 LinksysG_da:af:73 AmbitMic_a9:3d:68
                                                               0x0800
                                                                         489 IPv4
> Frame 16: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
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 (475 bytes)
0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 40
                                                       ..Y.=h.. %..s..E@
0010 01 db 8f 32 40 00 37 06
                              7b 15 80 77 f5 0c c0 a8
                                                       · · · 2@ · 7 · { · · w · ·
0020 01 69 00 50 04 22 ac a5 50 d0 65 14 9c 1f 50 18
                                                       ·i·P·"·· P·e···P·
0030 1b 28 49 75 00 00 3c 68 33 3e 41 6d 65 6e 64 6d
                                                       ·(Iu··<h 3>Amendm
0040 65 6e 74 20 49 58 3c 2f
                              68 33 3e 3c 2f 73 74 72
                                                       ent IX</ h3></str
                                                       ong></a> ··</p
0050 6f 6e 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70
0060 3e 3c 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 74
                                                       >The enumerat
     60 6f 6e 20 60 6e 20 74 68 65 20 43 6f 6e 73 74
                                                       ion in t he Const
```

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

**Answer:** 00:d0:59:a9:3d:68

```
14 17.500069
                      AmbitMic a9:3d:68 LinksysG da:af:73
                                                                           54 IPv4
     15 17.527057
                      LinksysG da:af:73
                                           AmbitMic a9:3d:68
                                                                0x0800
                                                                         1514 IPv4
     16 17.527422
                      LinksysG_da:af:73 AmbitMic_a9:3d:68
                                                                0x0800
                                                                          489 IPv4
> Frame 16: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
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 (475 bytes)
0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 40
                                                        ..Y·=h.. %..s..E@
                                                        ...2@.7. {..w....
.i.P.".. P.e...P.
0010 01 db 8f 32 40 00 37 06 7b 15 80 77 f5 0c c0 a8
0020 01 69 00 50 04 22 ac a5 50 d0 65 14 9c 1f 50 18
                                                        ·(Iu··<h 3>Amendm
0030 1b 28 49 75 00 00 3c 68 33 3e 41 6d 65 6e 64 6d
0040 65 6e 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 72
                                                        ent IX</ h3></str
0050 6f 6e 67 3e 3c 2f 61 3e
                              0a 0a 3c 70 3e 3c 2f 70
                                                        ong></a> ··</p
0060 3e 3c 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 74
                                                        >The enumerat
                                                        ion in + he Const
0070 60 6f 60 70 60 60 70 71 68 65 70 13 6f 60 73 71
```

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

**Answer:** The hex value for the Frame type field is 0x0800.

```
14 17.500069 AmbitMic a9:3d:68 LinksysG_da:af:73 0x0800 54 IPv4
     15 17.527057
                      LinksysG da:af:73
                                          AmbitMic a9:3d:68
                                                                          1514 IPv4
     16 17.527422 LinksysG da:af:73 AmbitMic a9:3d:68
                                                                0x0800 489 IPv4
> Frame 16: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
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 (475 bytes)
0000 00 d0 59 a9 3d 68 00 06
                               25 da af 73 08 00 45 40
                                                         ..Y.=h.. %..s..E@
0010 01 db 8f 32 40 00 37 06 7b 15 80 77 f5 0c c0 a8
                                                         · · · 2@ · 7 · { · · w · · ·
0020 01 69 00 50 04 22 ac a5 50 d0 65 14 9c 1f 50 18
                                                         ·i·P·"·· P·e···P·
0030 1b 28 49 75 00 00 3c 68 33 3e 41 6d 65 6e 64 6d 0040 65 6e 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 72
                                                         ·(Iu··<h 3>Amendm
                                                         ent IX</ h3></str
0050 6f 6e 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70
                                                         ong></a> ··</p
0060 3e 3c 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 74
                                                         >The enumerat
0070 60 6f 60 20 60 60 20 74 68 65 20 43 6f 60 73 74
```

8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

# **Answer:**

- The ASCII "O" appears 52 bytes from the start of the ethernet frame.
- There are 14 bytes of Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.
- 9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

#### **Answer:**

- The Internet Address column contains the IP address
- The Physical Address column contains the MAC address
- The type indicates the protocol type.

```
C:\Users\Admin>arp -a
Interface: 192.168.1.6 --- 0x4
 Internet Address
                      Physical Address
                                              Type
 192.168.1.1
                       d4-9a-a0-22-65-30
                                             dynamic
 192.168.1.255
                       ff-ff-ff-ff-ff
                                             static
                       01-00-5e-00-00-16
 224.0.0.22
                                              static
 224.0.0.251
                       01-00-5e-00-00-fb
                                              static
 224.0.0.252
                       01-00-5e-00-00-fc
                                             static
 239.255.255.250
                       01-00-5e-7f-ff-fa
                                             static
                       ff-ff-ff-ff-ff
 255.255.255.255
                                             static
::\Users\Admin>
```

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

#### **Answer:**

- The hex value for the source address is 00:d0:59:a9:3d:68.
- The hex value for the destination address is ff:ff:ff:ff:ff:ff;ff:ff; the broadcast address.

```
1 0.000000 AmbitMic_a9:3d:68 Broadcast
                                                                              42 Who has 192.168.1.1? Tell 192.168.1.105
       2 0.001018
                   LinksysG_da:af:73 AmbitMic_a9:3d:68
                                                                  ARP
                                                                             60 192.168.1.1 is at 00:06:25:da:af:73
                       AmbitMic_a9:3d:68 LinksysG_da:af:73
AmbitMic_a9:3d:68 LinksysG_da:af:73
       3 0.001028
                                                                  0x0800
                                                                              62 TPv4
       4 2.962850
                                                                              62 IPv4
                                                                  0x0800
> 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)

   > Destination: Broadcast (ff:ff:ff:ff:ff)
   > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
     Type: ARP (0x0806)
> Address Resolution Protocol (request)
```

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

**Answer:** Ethernet Frame type field is 0x0806, for ARP.

```
1 0.000000
                      AmbitMic_a9:3d:68
                                           Broadcast
                                                                            42 Who has 192.168.1.1? Tell 192.168.1.105
                                           AmbitMic_a9:3d:68
                                                                ARP
       2 0.001018
                      LinksysG_da:af:73
                                                                            60 192.168.1.1 is at 00:06:25:da:af:73
       3 0.001028
                      AmbitMic_a9:3d:68
                                           LinksysG_da:af:73
                                                                0x0800
                                                                            62 IPv4
                      AmbitMic_a9:3d:68
       4 2.962850
                                           LinksysG_da:af:73
                                                                0x0800
                                                                            62 IPv4
> 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)

   > Destination: Broadcast (ff:ff:ff:ff:ff)
   > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
     Type: ARP (0x0806)
> Address Resolution Protocol (request)
```

12.Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at

http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

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

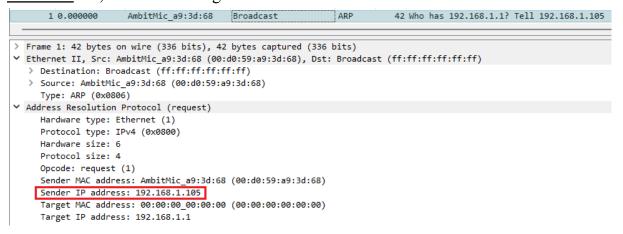
**Answer:** The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame

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

**Answer:** The hex value for opcode field withing the ARP-payload of the request is 0x0001, for request

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

**Answer:** Yes, the ARP message contains the IP address 192.168.1.105 for the sender.



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

**Answer:** The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.105) is being queried.

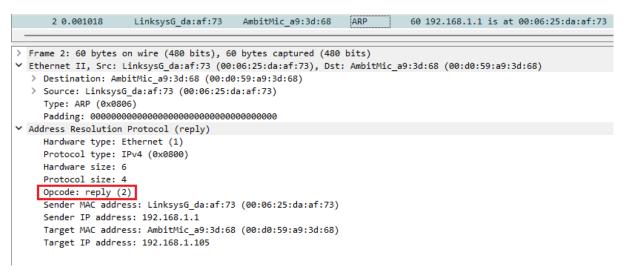
- 13. Now find the ARP reply that was sent in response to the ARP request.
  - a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

**Answer:** The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

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?

# **Answer:**

-0x0002



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?

**Answer:** The answer to the earlier ARP request appears in the "Sender MAC address" field, which contains the Ethernet address 00:06:25:da:af:73 for the sender with IP address 192.168.1.1

```
60 192.168.1.1 is at 00:06:25:da:af:73
                     LinksysG_da:af:73
                                        AmbitMic_a9:3d:68
                                                            ARP
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
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: ARP (0x0806)

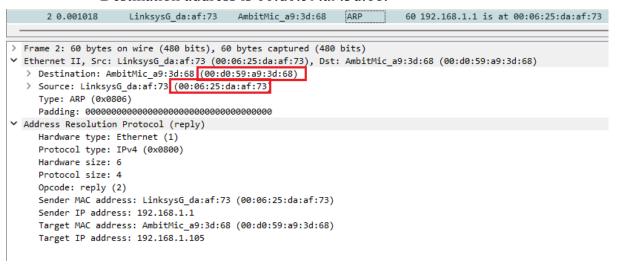
✓ Address Resolution Protocol (reply)

    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 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
```

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

# **Answer:**

- Source address is 00:06:25:da:af:73
- Destination address is 00:d0:59:a9:3d:68.



# 15. Open the ethernet-ethereal-trace-1 trace file in

http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But 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?

**Answer:** There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address