

CS 372 Lab 4

Joanna Lew

Summer 2017

Question 1

Q: What is the 48-bit Ethernet address of your computer?

A: The 48-bit Ethernet address of my computer is a0:99:9b:0a:65:57.

No.	Time	Source	Destination	Protocol	Length	Info
5	15:46:36.898325	AsustekC_59:25:e6	Apple_0a:65:57	0x0800	74	IPv4
6	15:46:36.898424	Apple_0a:65:57	AsustekC_59:25:e6	0x0800	66	IPv4
7	15:46:36.898844	Apple_0a:65:57	AsustekC_59:25:e6	0x0800	448	IPv4
8	15:46:37.003432	AsustekC_59:25:ed	Apple_0a:65:57	0x0800	66	IPv4
9	15:46:37.003437	AsustekC_59:25:ed	Apple_0a:65:57	0x0800	1514	IPv4
10	15:46:37.003438	AsustekC_59:25:ed	Apple_0a:65:57	0x0800	1514	IPv4

▶	Frame 7: 448 bytes on wire (3584 bits), 448 bytes captured (3584 bits) on interface 0
▼	Ethernet II, Src: Apple_0a:65:57 (a0:99:9b:0a:65:57), Dst: AsustekC_59:25:e6 (2c:56:dc:59:25:e6)
▼	Destination: AsustekC_59:25:e6 (2c:56:dc:59:25:e6)
	Address: AsustekC_59:25:e6 (2c:56:dc:59:25:e6)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)
▼	Source: Apple_0a:65:57 (a0:99:9b:0a:65:57)
	Address: Apple_0a:65:57 (a0:99:9b:0a:65:57)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)
	Type: IPv4 (0x0800)
▶	Data (434 bytes)

0000	2c 56 dc 59 25 e6 a0 99 9b 0a 65 57 08 00 45 00	,V.Y%... ..eW..E.
0010	01 b2 23 5c 40 00 40 06 89 55 c0 a8 56 68 80 77	..#\@.@. .U..Vh.w
0020	f5 0c e8 6e 00 50 a3 68 c2 f6 49 c8 99 cc 80 18	...n.P.h .I.....
0030	10 15 c6 a5 00 00 01 01 08 0a 27 25 9e f6 11 c9'%.o....
0040	4b 77 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b	KwGET /w ireshark
0050	2d 6c 61 62 73 2f 48 54 54 50 2d 65 74 68 65 72	--labs/HT TP-ether
0060	65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33 2e 68 74	eal-lab- file3.ht

Question 2

Q: 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?

A: The 48-bit destination address is 2c:56:dc:59:25:e6. No, it is not the Ethernet address of gaia.cs.umass.edu. It is the Ethernet address of the router to which my computer is connected.

Question 3

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

A: The hex value for the Frame type field is 0x800. This indicates it is an IPv4 type frame.

Question 4

Q: How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

A: The “G” appears 54 bytes from the start of the frame. The Ethernet frame is 14 bytes, which can be obtained with Total size – Data size = 448 – 434 = 14 bytes. The IP and TCP headers are each 20 bytes. Therefore 20 + 20 + 14 = 54 bytes.

Question 5

Q: What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu? What device has this as its Ethernet address?

A: The Ethernet source address is 2c:56:dc:59:25:e6. This is the address of the router to which my computer is connected to.

No.	Time	Source	Destination	Protocol	Length	Info
5	15:46:36.898325	AsustekC_59:25:e6	Apple_0a:65:57	0x0800	74	IPv4
6	15:46:36.898424	Apple_0a:65:57	AsustekC_59:25:e6	0x0800	66	IPv4
7	15:46:36.898844	Apple_0a:65:57	AsustekC_59:25:e6	0x0800	448	IPv4
8	15:46:37.003432	AsustekC_59:25:ed	Apple_0a:65:57	0x0800	66	IPv4
9	15:46:37.003437	AsustekC_59:25:ed	Apple_0a:65:57	0x0800	1514	IPv4
10	15:46:37.003438	AsustekC_59:25:ed	Apple_0a:65:57	0x0800	1514	IPv4
▶ Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0						
▼ Ethernet II, Src: AsustekC_59:25:ed (2c:56:dc:59:25:ed), Dst: Apple_0a:65:57 (a0:99:9b:0a:65:57)						
▼ Destination: Apple_0a:65:57 (a0:99:9b:0a:65:57)						
Address: Apple_0a:65:57 (a0:99:9b:0a:65:57)						
.... 0. = LG bit: Globally unique address (factory default)						
.... 0. = IG bit: Individual address (unicast)						
▼ Source: AsustekC_59:25:ed (2c:56:dc:59:25:ed)						
Address: AsustekC_59:25:ed (2c:56:dc:59:25:ed)						
.... 0. = LG bit: Globally unique address (factory default)						
.... 0. = IG bit: Individual address (unicast)						
Type: IPv4 (0x0800)						
▶ Data (1500 bytes)						
0000	a0 99 9b 0a 65 57 2c 56	dc 59 25 ed 08 00 45 00	...eW,V .Y%...E.			
0010	05 dc d2 2d 40 00 28 06	ee 59 80 77 f5 0c c0 a8	...-@.(. .Y.w....			
0020	56 68 00 50 e8 6e 49 c8	99 cc a3 68 c4 74 80 10	Vh.P.nI. ...h.t..			
0030	00 eb a9 a5 00 00 01 01	08 0a 11 c9 4b e0 27 25K.'%			
0040	9e 6f 48 54 54 50 2f 31	2e 31 20 32 30 30 20 4f	.oHTTP/1 .1 200 0			
0050	4b 0d 0a 44 61 74 65 3a	20 54 75 65 2c 20 31 35	K..Date: Tue, 15			
0060	20 41 75 67 20 32 30 31	37 20 32 32 3a 34 36 3a	Aug 201 7 22:46:			

Question 6

Q: What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

A: The destination address is a0:99:9b:0a:65:57. Yes, it is the Ethernet address of my computer.

Question 7

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

A: The hex value for the Frame type field is 0x800, which corresponds to IPv4.

Question 8

Q: 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?

A: The Ethernet frame is 14 bytes, and the IP and TCP are each 20 bytes. There is an additional 13 bytes since the “O” is preceded by HTTP/1.1 200 . $14 + 20 + 20 + 13 = 67$ bytes. Therefore, “O” is the 68th byte.

Question 9

Q: Write down the contents of your computers ARP cache. What is the meaning of each column value?

```
[joannas-mbp:~ Eggo$ arp -n -l -a]
Neighbor                Linklayer Address  Expire(0)  Expire(I)      Netif Refs Prbs
192.168.86.1             2c:56:dc:59:25:e6  1m5s      1m1s           en0      1
192.168.86.101           f4:f5:d8:a4:7a:9c  1m12s     1m12s          en0      1
192.168.86.113           0:71:cc:45:4b:ab   1m58s     1m58s          en0      1
224.0.0.251              1:0:5e:0:0:fb      (none)     (none)         en0
239.255.255.250          1:0:5e:7f:ff:fa    (none)     (none)         en0
```

A: The “Neighbor” column shows the IPv4 addresses of the devices connected to the network, while the “Linklayer Address” column shows the corresponding MAC address. A value in the Expire columns shows that the entries are dynamic, meaning they will be removed after a period of time. Having (none) in the Expire column means they are static/permanent ARP cache entries.

Question 10

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

A: The source address is 2c:56:dc:59:25:e6. The destination address is a0:99:9b:0a:65:57.

No.	▲ Time	Source	Destination	Protocol	Length	Info
393	14:10:39.549445	Google_a4:7a:9c	IPv4mcast_7f:ff:fa	0x0800	136	IPv4
394	14:10:39.960297	AsustekC_59:25:e6	Apple_0a:65:57	ARP	42	Who has 192.168.86.104? Tell 192.168.86.1
395	14:10:39.960344	Apple_0a:65:57	AsustekC_59:25:e6	ARP	42	192.168.86.104 is at a0:99:9b:0a:65:57
396	14:10:42.826718	WesternD_00:9a:78	IPv4mcast_7f:ff:fa	0x0800	372	IPv4
397	14:10:43.031626	WesternD_00:9a:78	IPv4mcast_7f:ff:fa	0x0800	381	IPv4
398	14:10:43.032398	WesternD_00:9a:78	IPv4mcast_7f:ff:fa	0x0800	426	IPv4
▶ Frame 394: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
▶ Ethernet II, Src: AsustekC_59:25:e6 (2c:56:dc:59:25:e6), Dst: Apple_0a:65:57 (a0:99:9b:0a:65:57)						
▼ Address Resolution Protocol (request)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: request (1)						
Sender MAC address: AsustekC_59:25:e6 (2c:56:dc:59:25:e6)						
Sender IP address: 192.168.86.1						
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)						
Target IP address: 192.168.86.104						

Question 11

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

A: The hex value for the Frame type field is 0x0806. This corresponds to ARP.

Question 12

Q: Find the first of two frames that contain ARP messages.

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

The ARP opcode field begins 20 bytes from the beginning of the Ethernet frame. There are 6 bytes each for the source and destination MAC addresses, 2 bytes for the Frame type, and 6 bytes for the header fields that precede Operation (HTYPE, PTYPE, HLEN, PLEN). $6 + 6 + 6 + 2 = 20$ bytes.

- (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?

The Opcode value is 1. This indicates it is an ARP request.

- (c) Does the ARP message contain the IP address of the sender?

Yes, it contains the Sender's IP address, which is 192.168.86.1.

- (d) Where in the ARP request does the question appear the Ethernet address of the machine whose corresponding IP address is being queried?

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

Question 13

Q: 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?

The ARP opcode field begins 20 bytes from the 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?

The value of the opcode field is 2. This indicates it is a reply.

- (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?

The answer to the ARP request is in the "Sender MAC address" field. It has the Ethernet address a0:99:9b:0a:65:57 for the sender with corresponding IP address 192.168.86.104.

No.	▲ Time	Source	Destination	Protocol	Length	Info
393	14:10:39.549445	Google_a4:7a:9c	IPv4mcast_7f:ff:fa	0x0800	136	IPv4
394	14:10:39.960297	AsustekC_59:25:e6	Apple_0a:65:57	ARP	42	Who has 192.168.86.104? Tell 192.168.86.1
395	14:10:39.960344	Apple_0a:65:57	AsustekC_59:25:e6	ARP	42	192.168.86.104 is at a0:99:9b:0a:65:57
396	14:10:42.826718	WesternD_00:9a:78	IPv4mcast_7f:ff:fa	0x0800	372	IPv4
397	14:10:43.031626	WesternD_00:9a:78	IPv4mcast_7f:ff:fa	0x0800	381	IPv4
398	14:10:43.032398	WesternD_00:9a:78	IPv4mcast_7f:ff:fa	0x0800	426	IPv4
▶ Destination: AsustekC_59:25:e6 (2c:56:dc:59:25:e6) ▶ Source: Apple_0a:65:57 (a0:99:9b:0a:65:57) 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: Apple_0a:65:57 (a0:99:9b:0a:65:57) Sender IP address: 192.168.86.104 Target MAC address: AsustekC_59:25:e6 (2c:56:dc:59:25:e6) Target IP address: 192.168.86.1						

Question 14

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

A: The source address is a0:99:9b:0a:65:57. The destination address is 2c:56:dc:59:25:e6.

Question 15

Q: Open the ethernet-ethereal-trace-1 trace file. 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?

A: There is no ARP reply because the reply is sent by the computer with the requested IP address (192.168.1.117) directly to the sender (192.168.1.104). Since we are not the sender or destination, we do not see the reply.