Class: CS-372 Term: Fall 2017

Author: Jon-Eric Cook Date: December 3, 2017

Lab: #5

NOTE:

I was unable to run Wireshark live on my computer. Due to this, I downloaded the provided zip file and used the **ethernet**—**etherreal-trace-1** file to answer the questions of this lab.

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

Answer:

00:d0:59:a9:3d:68 See screenshot below.

No.		Time	Source	Destination	Protocol	Length	Info			
	9	10:19:37.623057	192.168.1.105	128.119.245.12	TCP	54	1058 → 80	[ACK] Se		
•	10	10:19:37.623598	192.168.1.105	128.119.245.12	HTTP	686	GET /ether	eal-labs		
	11	10:19:37.651896	128.119.245.12	192.168.1.105	TCP	60	80 → 1058	[ACK] S€		
		10-10-27 CECACE			TCD	1511		[ACV] C		
F₁	rame	10: 686 bytes or	n wire (5488 bi†	ts), 686 bytes c	aptured	(5488 bi	lts)			
▼ E	ther	net II, Src: Amb	itMic_a9:3d:68	(00:d0:59:a9:3d:	68), Dst	: Linksy	sG_da:af:7	'3 (00:06:25:d		
>	Des	stination: Linksy	sG_da:af:73 (00	:06:25:da:af:73)						
•	► Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)									
	Тур	oe: IPv4 (0x0800)								

2) What is the 48-bit destination address in the Ethernet fame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

Answer:

00:06:25:da:af:73

No

It is the Mac address for my router or internet gateway address.

No.		Time	Source	Destination	Protocol	Length	Info		
	9	10:19:37.623057	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Se		
•	10	10:19:37.623598	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs		
	11	10:19:37.651896			TCP		80 → 1058 [ACK] Se		
_	- 12	10.10.27 CECACE			TCD		OR 10ED [ACK] C		
▶ 1	rame	10: 686 bytes o	n wire (5488 bi1	ts), 686 bytes c	aptured	(5488 b	its)		
	▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da								
	Des	stination: Linksy	/sG_da:af:73 (00	:06:25:da:af:73) 🕇				
)	⊳ Soι	urce: AmbitMic_a	:3d:68 (00:d0:5	9:a9:3d:68)					
	Тур	oe: IPv4 (0x0800)							

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

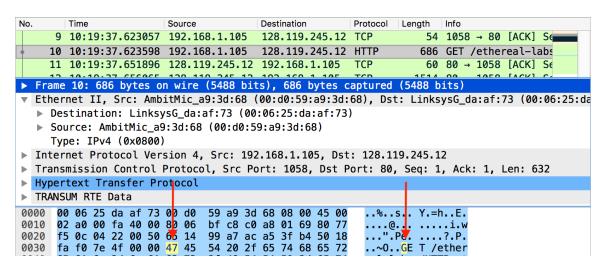
Answer: IPv4 (0x0800) See screenshot below.

No.		Time	Source	Destination	Protocol	Length	Info		
	9	10:19:37.623057	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Se		
•	10	10:19:37.623598	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs		
	11	10:19:37.651896	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Se		
	17	10.10.37 CECACE	120 110 245 12	100 100 1 105	TCD	1511	00 10E0 [ACK] C		
•	Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)								
▼	Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da								
	▶ Des	stination: Linksy	/sG_da:af:73 (00	:06:25:da:af:73)				
	▶ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)								
	Type: IPv4 (0x0800)								

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

Answer: 47 bytes

See screenshot below.



5) 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?

Answer:

00:06:25:da:af:73

Neither

My router has this as its Ethernet address.

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 Yes See screenshot below.

No.		Time	Source	Destination	Protocol	Length	Info			
	14	10:19:37.657199	192.168.1.105	128.119.245.12	TCP	54	1058 → 80	[ACK]	Se	
•	15	10:19:37.684187	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058	[ACK]	S€	
4-	16	10:19:37.684552	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1	200 OK	(
	17	10:19:37.684587	192.168.1.105	128.119.245.12	TCP	54	1058 → 80	[ACK]	Sŧ	
▶	Frame	16: 489 bytes o	n wire (3912 bit	ts), 489 bytes c	aptured	(3912 b	its)			
▼	Ether	net II, Src: Lin	ksysG_da:af:73 ((00:06:25:da:af:	73), Ds1	t: Ambit	Mic_a9:3d:	68 (00:	d0:59:a	
	▶ Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)									

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

Answer:

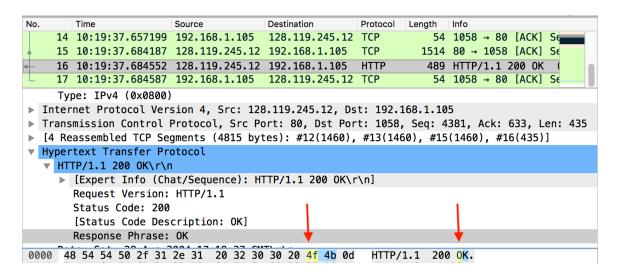
Type: IPv4 (0x0800) See screenshot below.

No.		Time	Source	Destination	Protocol	Length	Info		
	14	10:19:37.657199	192.168.1.105	128.119.245.12	TCP	54	1058 → 8	0 [ACK]	Se
•	15	10:19:37.684187	128.119.245.12	192.168.1.105	TCP	1514	80 → 105	8 [ACK]	S€
4	16	10:19:37.684552	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1	200 OK	
L	17	10:19:37.684587	192.168.1.105	128.119.245.12	TCP	54	1058 → 8	0 [ACK]	Se
	Frame	16: 489 bytes o	n wire (3912 bit	ts) , 489 bytes c	aptured	(3912 b	its)		
▼	Ether	net II, Src: Lin	ksysG_da:af:73	(00:06:25:da:af:	73), Ds ¹	t: Ambit	Mic_a9:3d	1:68 (00	:d0:59:a9
	▶ Des	stination: AmbitM	lic_a9:3d:68 (00	:d0:59:a9:3d:68)				
	▶ Soι	ırce: LinksysG_da	a:af:73 (00:06:2	5:da:af:73)					
	Тур	oe: IPv4 (0x0800)	-						

8) How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" appear in the Ethernet frame?

Answer:

4f



9) Write down the contents of your computer's ARP cache. What is the meaning of each column value?

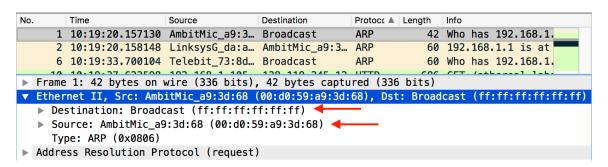
Answer:

I was unable to run Wireshark live on my computer. Due to this, I downloaded the provided zip file and used the **ethernet**—**etherreal-trace-1** file to answer the questions of this lab.

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

Answer:

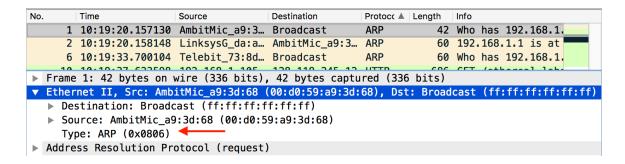
Source: 00:d0:59:a9:3d:68 Destination: ff:ff:ff:ff:ff See screenshot below.



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

Answer:

Type: ARP (0x0806) See screenshot below.



12)

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

Answer: 20 bytes See screenshot below.

Ethernet transmission layer (not necessarily accessible to the user):

(8 hit: Ethernet address of destination (6 hytes)

```
48.bit: Ethernet address of destination (6 bytes)
48.bit: Ethernet address of sender (6 bytes)
16.bit: Protocol type = ether_type$ADDRESS_RESOLUTION (2 bytes)
Ethernet packet data:
16.bit: (ar$hrd) Hardware address space (e.g., Ethernet,
Packet Radio Net.) (2 bytes)

16.bit: (ar$pro) Protocol address space. For Ethernet
hardware, this is from the set of type
fields ether_typ$<protocol>. (2 bytes)

8.bit: (ar$hln) byte length of each hardware address (1 byte)
8.bit: (ar$pln) byte length of each protocol address (1 byte)
16.bit: (ar$pln) opcode (ares op$REQUEST | ares op$REPLY) (2 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?

Answer:

Opcode: request (1) See screenshot below.

```
No.
                                                      Protocc ▲ | Length | Info
     1 10:19:20.157130 AmbitMic_a9:3... Broadcast ARP 42 Who has 192.168.1.
     2 10:19:20.158148 LinksysG_da:a... AmbitMic_a9:3... ARP
                                                               60 192.168.1.1 is at
     6 10:19:33.700104 Telebit_73:8d... Broadcast
                                                     ARP
                                                                60 Who has 192.168.1.
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
                                                                 COC CET /athancal lahe
▶ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
     Hardware type: Ethernet (1)
     Protocol type: IPv4 (0x0800)
     Hardware size: 6
     Protocol size: 4
    Opcode: request (1)
```

C) Does the ARP message contain the IP address of the sender?

Answer:

Yes - 192.168.1.105 See screenshot below.

```
Time
                        Source
                                       Destination
                                                       Protocc ▲ Length Info
     1 10:19:20.157130 AmbitMic_a9:3... Broadcast
                                                       ARP 42 Who has 192.168.1.
                                                      ARP
     2 10:19:20.158148 LinksysG_da:a... AmbitMic_a9:3... ARP
                                                                   60 192.168.1.1 is at
     6 10:19:33.700104 Telebit_73:8d... Broadcast
                                                                  60 Who has 192.168.1.
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
                                                                 COC CET /othoroal labor
▶ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ 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
```

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

Answer:

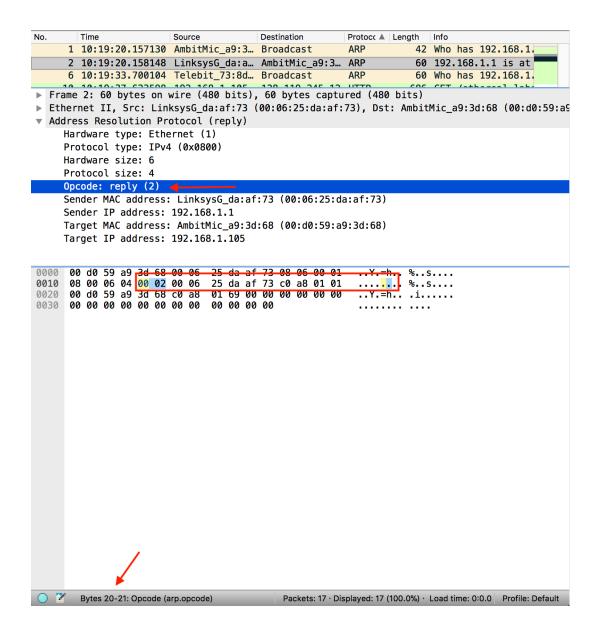
In the Target MAC address field in the form of 00:00:00:00:00:00 See screenshot below.

```
No.
                        Source
                                       Destination
                                                      Protocc ▲ Length Info
                                                      ARP 42 Who has 192.168.1.
      1 10:19:20.157130 AmbitMic_a9:3... Broadcast
     2 10:19:20.158148 LinksysG_da:a... AmbitMic_a9:3... ARP
                                                                  60 192.168.1.1 is at
     6 10:19:33.700104 Telebit_73:8d... Broadcast ARP
                                                                 60 Who has 192.168.1.
► 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)
▼ 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...i
0020 00 00 00 00 00 c0 a8 01 01
```

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: 20 bytes See screenshot below.



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:

Opcode: reply (2) See screenshot below.

```
No.
                        Source
                                                       Protocc ▲ Length Info
                                       Destination
      1 10:19:20.157130 AmbitMic_a9:3... Broadcast
                                                       ARP
                                                                  42 Who has 192.168.1.
      2 10:19:20.158148 LinksysG_da:a... AmbitMic_a9:3... ARP
                                                                   60 192.168.1.1 is at
                                                      ARP
      6 10:19:33.700104 Telebit_73:8d... Broadcast
                                                                   60 Who has 192.168.1.
▶ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
                                                                  COC CET /othorool lohe
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9
▼ Address Resolution Protocol (reply)
     Hardware type: Ethernet (1)
     Protocol type: IPv4 (0x0800)
     Hardware size: 6
     Protocol size: 4
     Opcode: reply (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?

Answer:

The Target MAC address was queried from 00:00:00:00:00:00 to 00:d0:59:a9:3d:68. Also, the Target IP address changed from 192.168.1.1 to 192.168.1.105. See screenshot below.

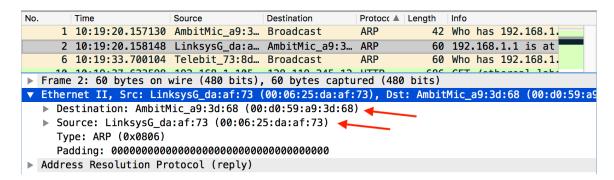
```
Source
                                                      Protocc ▲ Length Info
     1 10:19:20.157130 AmbitMic_a9:3... Broadcast
                                                      ARP 42 Who has 192.168.1.
     2 10:19:20.158148 LinksysG_da:a... AmbitMic_a9:3... ARP
                                                                  60 192.168.1.1 is at
                                                     ARP 60 Who has 192.168.1.
     6 10:19:33.700104 Telebit_73:8d... Broadcast
▶ 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
▼ 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 is the hexadecimal values for the source and destination address in the Ethernet frame containing the ARP reply message?

Answer:

Source: 00:06:25:da:af:73 Destination: 00:d0:59:a9:3d:68

See screenshot below.



15) Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

Answer:

The target IP address is within the same subnet that the router has already mapped in its ARP table.

```
Source
                                      Destination
                                                     Protocc ▲ Length Info
     2 10:19:20.158148 LinksysG_da:a... AmbitMic_a9:3... ARP 60 192.168.1.1 is at
     6 10:19:33.700104 Telebit_73:8d... Broadcast ARP
                                                                60 Who has 192.168.1.
    10 10:19:37.623598 192.168.1.105 128.119.245.12 HTTP 686 GET /ethereal-labs
▶ Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▶ Ethernet II, Src: Telebit_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
     Protocol type: IPv4 (0x0800)
    Hardware size: 6
     Protocol size: 4
     Opcode: request (1)
     Sender MAC address: Telebit_73:8d:ce (00:80:ad:73:8d:ce)
     Sender IP address: 192.168.1.104
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00)
    Target IP address: 192.168.1.117
```