

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] Seq=
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] Seq=
12	10:19:37.656065	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=

▶ 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: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 (0x0800)

2) 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?

Answer:

00:06:25:da:af:73

No

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

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] Seq=
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] Seq=
12	10:19:37.656065	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=

▶ 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: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 (0x0800)

Answer:
IPv4 (0x0800)
See screenshot below.

Answer:
54 bytes
See screenshot below.

Answer:
00:06:25:da:af:73
Neither
My router has this as its Ethernet address.
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] Seq=...
15	10:19:37.684187	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=...
16	10:19:37.684552	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/css)
17	10:19:37.684587	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=...

▶ Frame 16: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface 0
 ▼ 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)

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] Seq=
15	10:19:37.684187	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=
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] Seq=

▶ 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) ←

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 → 80 [ACK] Seq=
15	10:19:37.684187	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=
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] Seq=

▶ 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) ←

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

Answer:

68

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] Seq=
15	10:19:37.684187	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=
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] Seq=

Type: IPv4 (0x0800)

▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 4381, Ack: 633, Len: 435

▶ [4 Reassembled TCP Segments (4815 bytes): #12(1460), #13(1460), #15(1460), #16(435)]

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Request Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.

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

Answer:

internet address = ip

physical address = Mac

type = static/dynamic

See screenshot below.

```
? (192.168.1.1) at c4:4:15:23:3e:e on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
broadcasthost (255.255.255.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
```

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:ff

See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
1	10:19:20.157130	AmbitMic_a9:3...	Broadcast	ARP	42	Who has 192.168.1.1
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_73:80...	Broadcast	ARP	60	Who has 192.168.1.1
<p>▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)</p> <p>▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)</p> <ul style="list-style-type: none"> ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff) ← ▶ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) ← Type: ARP (0x0806) <p>▶ Address Resolution Protocol (request)</p>						

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.

No.	Time	Source	Destination	Protocol	Length	Info
1	10:19:20.157130	AmbitMic_a9:3...	Broadcast	ARP	42	Who has 192.168.1.1
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 192.168.1.1
10	10:19:37.622500	192.168.1.105	192.168.1.105	HTTP	606	GET /etherpad1/...
▶ 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:ff)						
▶ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)						
Type: ARP (0x0806) ←						
▶ Address Resolution Protocol (request)						

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

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 request is made?

See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
1	10:19:20.157130	AmbitMic_a9:3...	Broadcast	ARP	42	Who has 192.168.1.1
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 192.168.1.1
10	10:19:37.623588	192.168.1.105	192.168.1.105	HTTP	606	GET /etherbase1.js

- ▶ 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)

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

Answer:

Yes - 192.168.1.105

See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
1	10:19:20.157130	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1
2	10:19:20.158148	LinksysG_da:a9:3d:68	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:00:00:00:00:00
6	10:19:33.700104	Telebit_73:8d:68:00:00:00	Broadcast	ARP	60	Who has 192.168.1.1

▶ 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

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.	Time	Source	Destination	Protocol	Length	Info
1	10:19:20.157130	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1
2	10:19:20.158148	LinksysG_da:a9:3d:68	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:00:00:00:00:00
6	10:19:33.700104	Telebit_73:8d:68:00:00:00	Broadcast	ARP	60	Who has 192.168.1.1

▶ 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 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.

The screenshot shows a Wireshark packet capture of an ARP reply. The packet list at the top shows three packets: an ARP request from AmbitMic_a9:3d:68 to Broadcast, an ARP request from LinksysG_da:af:73 to AmbitMic_a9:3d:68, and an ARP reply from LinksysG_da:af:73 to AmbitMic_a9:3d:68. The packet details pane for the selected ARP reply packet shows the following fields: Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.105, and Address Resolution Protocol (reply). The ARP opcode field is highlighted in blue and labeled "Opcode: reply (2)". The packet bytes pane shows the raw data of the packet, with the opcode field highlighted in red. A red arrow points to the opcode field in the packet bytes pane.

No.	Time	Source	Destination	Protocol	Length	Info
1	10:19:20.157130	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.105?
2	10:19:20.158148	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:d0:59:a9:3d:68
6	10:19:33.700104	Telebit_73:8d:c0:a8	Broadcast	ARP	60	Who has 192.168.1.105?

Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
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

0000 00 d0 59 a9 3d 68 00 06 25 da af 73 c0 a8 01 01 ..Y..h. %..S....
0010 08 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01%..S....
0020 00 d0 59 a9 3d 68 c0 a8 01 69 00 00 00 00 00 00 ..Y.=h.. .i.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Bytes 20-21: Opcode (arp.opcode) Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.0 Profile: Default

No.	Time	Source	Destination	Protocol ▲	Length	Info
1	10:19:20.157130	AmbitMic_a9:3...	Broadcast	ARP	42	Who has 192.168.1.1
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 192.168.1.1
10	10:19:37.633500	192.168.1.105	192.168.1.105	UDP	68	GET /ethos/1.js
<p>▶ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)</p> <p>▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)</p> <p>▼ Address Resolution Protocol (reply)</p> <p>Hardware type: Ethernet (1)</p> <p>Protocol type: IPv4 (0x0800)</p> <p>Hardware size: 6</p> <p>Protocol size: 4</p> <p>Opcode: reply (2)</p> <p>Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)</p> <p>Sender IP address: 192.168.1.1</p> <p>Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)</p> <p>Target IP address: 192.168.1.105</p>						

No.	Time	Source	Destination	Protocol	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
16	10:19:37.684553	128.119.245.12	192.168.1.105	HTTP	480	HTTP/1.1 200 OK
<p>▶ Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)</p> <p>▶ Ethernet II, Src: Telebit_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)</p> <p>▼ Address Resolution Protocol (request)</p> <p>Hardware type: Ethernet (1)</p> <p>Protocol type: IPv4 (0x0800)</p> <p>Hardware size: 6</p> <p>Protocol size: 4</p> <p>Opcode: request (1)</p> <p>Sender MAC address: Telebit_73:8d:ce (00:80:ad:73:8d:ce)</p> <p>Sender IP address: 192.168.1.104</p> <p>Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)</p> <p>Target IP address: 192.168.1.117</p>						