

# CS 372 – Lab 5

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

**My 48-bit address is 00:d0:59:a9:3d:68**

Apply a display filter ... <Ctrl-/>

| 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? Tell 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 00:06:25:da:af:73               |
| 3   | 10:19:20.158158 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=146... |
| 4   | 10:19:23.119980 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 5   | 10:19:29.128618 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 6   | 10:19:33.700104 | CnetTech_73:8d:ce | Broadcast         | ARP      | 60     | Who has 192.168.1.117? Tell 192.168.1.104         |
| 7   | 10:19:37.601553 | 192.168.1.105     | 128.119.245.12    | TCP      | 62     | 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460... |
| 8   | 10:19:37.623032 | 128.119.245.12    | 192.168.1.105     | TCP      | 62     | 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=... |
| 9   | 10:19:37.623057 | 192.168.1.105     | 128.119.245.12    | TCP      | 54     | 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0       |
| 10  | 10:19:37.623598 | 192.168.1.105     | 128.119.245.12    | HTTP     | 686    | GET /ethereal-labs/HTTP-ethereal-lab-file3.htm... |
| 11  | 10:19:37.651896 | 128.119.245.12    | 192.168.1.105     | TCP      | 60     | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0      |
| 12  | 10:19:37.656065 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=146... |
| 13  | 10:19:37.657155 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=... |
| 14  | 10:19:37.657199 | 192.168.1.105     | 128.119.245.12    | TCP      | 54     | 1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0  |
| 15  | 10:19:37.684187 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=... |
| 16  | 10:19:37.684552 | 128.119.245.12    | 192.168.1.105     | HTTP     | 489    | HTTP/1.1 200 OK (text/html)                       |

> 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)

0000 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 ..... ..

Bytes 6-11: Address (eth.addr) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

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?  
[Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

**The 48-bit destination address is 00:06:25:da:af:73**

**This is the first-hop router; the mac address for my router or internet gateway address.**

| 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? Tell 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 00:06:25:da:af:73               |
| 3   | 10:19:20.158158 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=146... |
| 4   | 10:19:23.119980 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 5   | 10:19:29.128618 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 6   | 10:19:33.700104 | CnetTech_73:8d:ce | Broadcast         | ARP      | 60     | Who has 192.168.1.117? Tell 192.168.1.104         |
| 7   | 10:19:37.601553 | 192.168.1.105     | 128.119.245.12    | TCP      | 62     | 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...  |
| 8   | 10:19:37.623032 | 128.119.245.12    | 192.168.1.105     | TCP      | 62     | 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=... |
| 9   | 10:19:37.623057 | 192.168.1.105     | 128.119.245.12    | TCP      | 54     | 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0       |
| 10  | 10:19:37.623598 | 192.168.1.105     | 128.119.245.12    | HTTP     | 686    | GET /ethereal-labs/HTTP-ethereal-lab-file3.htm... |
| 11  | 10:19:37.651896 | 128.119.245.12    | 192.168.1.105     | TCP      | 60     | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0      |
| 12  | 10:19:37.656065 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=146... |
| 13  | 10:19:37.657155 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=... |
| 14  | 10:19:37.657199 | 192.168.1.105     | 128.119.245.12    | TCP      | 54     | 1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0  |
| 15  | 10:19:37.684187 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=... |
| 16  | 10:19:37.684552 | 128.119.245.12    | 192.168.1.105     | HTTP     | 489    | HTTP/1.1 200 OK (text/html)                       |

> 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)

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

> Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632

> Hypertext Transfer Protocol

|      |   |                     |
|------|---|---------------------|
| 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 | ...~O...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   |

- Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?  
**The hex value for the Frame type field is 0x0800. This corresponds to the IP protocol.**
- How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?  
**After 432 bits or 54 bytes, the 'G' in get appears.**

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

| 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? Tell 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 00:06:25:da:af:73               |
| 3   | 10:19:20.158158 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=146... |
| 4   | 10:19:23.119980 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 5   | 10:19:29.128618 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 6   | 10:19:33.700104 | CnetTech_73:8d:ce | Broadcast         | ARP      | 60     | Who has 192.168.1.117? Tell 192.168.1.104         |
| 7   | 10:19:37.601553 | 192.168.1.105     | 128.119.245.12    | TCP      | 62     | 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460... |
| 8   | 10:19:37.623032 | 128.119.245.12    | 192.168.1.105     | TCP      | 62     | 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=... |
| 9   | 10:19:37.623057 | 192.168.1.105     | 128.119.245.12    | TCP      | 54     | 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0       |
| 10  | 10:19:37.623598 | 192.168.1.105     | 128.119.245.12    | HTTP     | 686    | GET /ethereal-labs/HTTP-ethereal-lab-file3.htm... |
| 11  | 10:19:37.651896 | 128.119.245.12    | 192.168.1.105     | TCP      | 60     | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0      |
| 12  | 10:19:37.656065 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=146... |
| 13  | 10:19:37.657155 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=... |
| 14  | 10:19:37.657199 | 192.168.1.105     | 128.119.245.12    | TCP      | 54     | 1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0  |
| 15  | 10:19:37.684187 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=... |
| 16  | 10:19:37.684552 | 128.119.245.12    | 192.168.1.105     | HTTP     | 489    | HTTP/1.1 200 OK (text/html)                       |

> [SEQ/ACK analysis]  
> [Timestamps]  
TCP payload (632 bytes)  
Hypertext Transfer Protocol  
GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n  
> [Expert Info (Chat/Sequence): GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n]  
Request Method: GET  
Request URI: /ethereal-labs/HTTP-ethereal-lab-file3.html  
Request Version: HTTP/1.1  
Host: gaia.cs.umass.edu\r\n

0030 fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72 ... GET /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 6d 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

Hypertext Transfer Protocol (http), 632 bytes | Packets: 17 • Displayed: 17 (100.0%) | Profile: Default

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?

**The source address is 00:06:25:da:af:73**

**This is again, the first hop router.**

| ethernet-ethereal-trace-1  |                 |                   |                |          |        |   |
|--|-----------------|-------------------|----------------|----------|--------|---|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help |                 |                   |                |          |        |   |
| Apply a display filter ... <Ctrl-/> Expression...                          |                 |                   |                |          |        |   |
| No.  | Time            | Source            | Destination    | Protocol | Length | Info  |
| 3  | 10:19:20.158158 | 192.168.1.105     | 199.2.53.206   | TCP      | 62     | 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=146... |
| 4  | 10:19:23.119980 | 192.168.1.105     | 199.2.53.206   | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 5  | 10:19:29.128618 | 192.168.1.105     | 199.2.53.206   | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 6  | 10:19:33.700104 | CnetTech_73:8d:ce | Broadcast      | ARP      | 60     | Who has 192.168.1.117? Tell 192.168.1.104         |
| 7  | 10:19:37.601553 | 192.168.1.105     | 128.119.245.12 | TCP      | 62     | 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460... |
| 8  | 10:19:37.623032 | 128.119.245.12    | 192.168.1.105  | TCP      | 62     | 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=... |
| 9  | 10:19:37.623057 | 192.168.1.105     | 128.119.245.12 | TCP      | 54     | 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0       |
| 10   | 10:19:37.623598 | 192.168.1.105     | 128.119.245.12 | HTTP     | 686    | GET /ethereal-labs/HTTP-ethereal-lab-file3.htm... |
| 11   | 10:19:37.651896 | 128.119.245.12    | 192.168.1.105  | TCP      | 60     | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0      |
| 12   | 10:19:37.656065 | 128.119.245.12    | 192.168.1.105  | TCP      | 1514   | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=146... |
| 13   | 10:19:37.657155 | 128.119.245.12    | 192.168.1.105  | TCP      | 1514   | 80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=... |
| 14   | 10:19:37.657199 | 192.168.1.105     | 128.119.245.12 | TCP      | 54     | 1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0  |
| 15   | 10:19:37.684187 | 128.119.245.12    | 192.168.1.105  | TCP      | 1514   | 80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=... |
| 16   | 10:19:37.684552 | 128.119.245.12    | 192.168.1.105  | HTTP     | 489    | HTTP/1.1 200 OK (text/html)                       |
| 17   | 10:19:37.684587 | 192.168.1.105     | 128.119.245.12 | TCP      | 54     | 1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=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)   |
| Type: IPv4 (0x0800)   |
| ▼ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105                                |
| 0100 .... = Version: 4  |
| .... 0101 = Header Length: 20 bytes (5)   |
| > Differentiated Services Field: 0x60 (DSCP: CS3, ECN: Not-ECT)                                       |
| Total Length: 1500  |
| Identification: 0x8f2f (36655)  |
| > Flags: 0x0000 Don't fragment  |

  

|      |   |                    |
|------|---|--------------------|
| 0000 | 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 | ..Y.=h..%:..E`     |
| 0010 | 05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8 | .../7 v.w....      |
| 0020 | 01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10 | .i.P"..."?e..P.    |
| 0030 | 1b 28 5e d0 00 00 48 54 54 50 2f 31 2e 31 20 32 | .(^...HT TP/1.1 2  |
| 0040 | 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 | 00 OK..D ate: Sat  |
| 0050 | 2c 20 32 38 20 41 75 67 20 32 30 30 34 20 31 37 | , 28 Aug 2004 17   |
| 0060 | 3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76 | :19:37 G MT..Serv  |
| 0070 | 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 | er: Apac he/2.0.4  |
| 0080 | 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 | 0 (Red H at Linux  |
| 0090 | 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 | )...Last- Modified |
| 00a0 | 3a 20 53 61 74 2c 20 32 38 20 41 75 67 20 32 30 | : Sat, 2 8 Aug 20  |
| 00b0 | 30 34 20 31 37 3a 31 38 3a 35 33 20 47 4d 54 0d | 04 17:18 :53 GMT   |
| 00c0 | 0a 45 54 61 67 3a 20 22 31 62 61 35 63 2d 31 31 | ETag: " 1ba5c-11   |
| 00d0 | 39 34 2d 36 39 65 64 39 34 30 22 0d 0a 41 63 63 | 94-69ed9 40"...Acc |
| 00e0 | 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 | ept-Rang es: byte  |
| 00f0 | 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 | s...Conte nt-Lengt |
| 0100 | 68 3a 20 34 35 30 30 0d 0a 4b 65 65 70 2d 41 6c | h: 4500...Keep-Al  |
| 0110 | 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 31 30 2c | ive: tim eout=10,  |

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

**The destination address is 00:d0:59:a9:3d:68, and it is the Ethernet address of my computer.**

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

**The hex value is 0x0800 and it corresponds to the IP protocol.**

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?

**The "O" in "OK" appears from 64 bytes in.**

- The internet address column contains the IP address, the physical address column contains the MAC address, and the type indicates the protocol type.

```
Command Prompt
C:\Windows\System32>arp -a

Interface: 10.0.0.125 --- 0xa
Internet Address      Physical Address      Type
10.0.0.1              48-1d-70-22-f1-b4     dynamic
10.0.0.33             74-df-bf-74-c0-df     dynamic
10.0.0.59             44-07-0b-a0-de-d7     dynamic
10.0.0.255            ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22           01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.3.22         01-00-5e-7f-03-16     static
239.255.255.250      01-00-5e-7f-ff-fa     static
255.255.255.255      ff-ff-ff-ff-ff-ff     static

C:\Windows\System32>
```

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?  
**The hex value for the source address is 00:80:ad:73:8d:ce. The hex value for the destination address is ff:ff:ff:ff:ff:ff, the broadcast address.**

The image shows a Wireshark packet capture analysis. The top pane displays a list of 16 network packets. Packet 6, at time 10:19:33.700104, is an ARP request from CnetTech\_73:8d:ce to the broadcast address ff:ff:ff:ff:ff:ff. The middle pane shows the details of this packet, identifying it as an Ethernet II frame containing an ARP request. The bottom pane shows the raw packet data in hexadecimal and ASCII. The first two bytes of the frame are ff ff, which correspond to the Ethernet Frame type field for ARP (0x0806).

| 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? Tell 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 00:06:25:da:af:73               |
| 3   | 10:19:20.158158 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=146... |
| 4   | 10:19:23.119980 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 5   | 10:19:29.128618 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 6   | 10:19:33.700104 | CnetTech_73:8d:ce | Broadcast         | ARP      | 60     | Who has 192.168.1.117? Tell 192.168.1.104         |
| 7   | 10:19:37.601553 | 192.168.1.105     | 128.119.245.12    | TCP      | 62     | 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460... |
| 8   | 10:19:37.623032 | 128.119.245.12    | 192.168.1.105     | TCP      | 62     | 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=... |
| 9   | 10:19:37.623057 | 192.168.1.105     | 128.119.245.12    | TCP      | 54     | 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0       |
| 10  | 10:19:37.623598 | 192.168.1.105     | 128.119.245.12    | HTTP     | 686    | GET /ethereal-labs/HTTP-ethereal-lab-file3.htm... |
| 11  | 10:19:37.651896 | 128.119.245.12    | 192.168.1.105     | TCP      | 60     | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0      |
| 12  | 10:19:37.656065 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=146... |
| 13  | 10:19:37.657155 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=... |
| 14  | 10:19:37.657199 | 192.168.1.105     | 128.119.245.12    | TCP      | 54     | 1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0  |
| 15  | 10:19:37.684187 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=... |
| 16  | 10:19:37.684552 | 128.119.245.12    | 192.168.1.105     | HTTP     | 489    | HTTP/1.1 200 OK (text/html)                       |

> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
> Ethernet II, Src: CnetTech\_73:8d:ce (00:80:ad:73:8d:ce), 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: CnetTech\_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 (00:00:00:00:00:00)  
    Target IP address: 192.168.1.117

```
0000  ff ff ff ff ff 00 80 ad 73 8d ce 08 06 00 01  ....s.....
0010  08 00 06 04 00 01 00 80 ad 73 8d ce c0 a8 01 68  ....s.....h
0020  00 00 00 00 00 00 c0 a8 01 75 00 00 00 00 00  ....u.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
```

Address Resolution Protocol (arp), 28 bytes | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

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

**The hex value for the Ethernet Frame type field is 0x0806, for ARP.**



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?  
**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?  
**The hex value for opcode field within the ARP-payload of the request is 1 for the request.**
  - c) Does the ARP message contain the IP address of the sender?  
**Yes, the ARP message containing the IP address 195.168.1.105 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?  
**In the “Target MAC address” field (destination) in the form of 00:00:00:00:00:00. Once the MAC address is resolved, this would be populated with the corresponding complete MAC address of the server or its relevant router.**

13. Now find the ARP reply that was sent in response to the ARP request.

**Here's a screenshot of the ARP reply**

The screenshot shows the Wireshark interface with the following details:

- Packet List:** A table showing network traffic. The selected packet is number 12, time 10:19:37.656065, source 192.168.1.105, destination 192.168.1.105, protocol TCP, length 1514. The info column shows '80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=146...'.
- Packet Details:**
  - 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)
      - Address: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)
        - .... 00. .... = LG bit: Globally unique address (factory default)
        - .... ..0 .... = IG bit: Individual address (unicast)
    - Source: LinksysG\_da:af:73 (00:06:25:da:af:73)
      - Address: LinksysG\_da:af:73 (00:06:25:da:af:73)
        - .... 00. .... = LG bit: Globally unique address (factory default)
        - .... ..0 .... = IG bit: Individual address (unicast)
    - Type: ARP (0x0806)
    - Padding: 00000000000000000000000000000000
  - 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
- Packet Bytes:**
  - 0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 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 .....

- 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 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?  
**The hex value for opcode field within the ARP-payload of the request is 2 for 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 earlier ARP request appears in the “Sender MAC address” field, which contains the Ethernet address 00:06:25:da:af:73.**
14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?  
**The hex value for the source address is 00:06:25:da:af:73 and for the destination 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?  
**It is an IP address within the same subnet that the router has already mapped in its ARP table and does not need to be rediscovered and chronicled.**

The image shows a Wireshark packet capture window titled "ethernet-ethereal-trace-1". The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter bar shows "Apply a display filter ... <Ctrl-/>". The main packet list table has columns for No., Time, Source, Destination, Protocol, Length, and Info. It shows 12 packets, including ARP requests, TCP SYN and ACK packets, and an HTTP GET request. The packet details pane for packet 6 (Frame 6) is expanded, showing Ethernet II details (Destination: Broadcast, Source: CnetTech\_73:8d:ce), ARP details (Type: ARP, Padding: 00000000000000000000000000000000), and Address Resolution Protocol (request) details (Hardware type: Ethernet, Protocol type: IPv4, Hardware size: 6, Protocol size: 4, Opcode: request, Sender MAC address: CnetTech\_73:8d:ce, Sender IP address: 192.168.1.104, Target MAC address: 00:00:00:00:00:00, Target IP address: 192.168.1.117). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

| 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? Tell 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 00:06:25:da:af:73               |
| 3   | 10:19:20.158158 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=146... |
| 4   | 10:19:23.119980 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 5   | 10:19:29.128618 | 192.168.1.105     | 199.2.53.206      | TCP      | 62     | [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi... |
| 6   | 10:19:33.700104 | CnetTech_73:8d:ce | Broadcast         | ARP      | 60     | Who has 192.168.1.117? Tell 192.168.1.104         |
| 7   | 10:19:37.601553 | 192.168.1.105     | 128.119.245.12    | TCP      | 62     | 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460... |
| 8   | 10:19:37.623032 | 128.119.245.12    | 192.168.1.105     | TCP      | 62     | 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=... |
| 9   | 10:19:37.623057 | 192.168.1.105     | 128.119.245.12    | TCP      | 54     | 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0       |
| 10  | 10:19:37.623598 | 192.168.1.105     | 128.119.245.12    | HTTP     | 686    | GET /ethereal-labs/HTTP-ethereal-lab-file3.htm... |
| 11  | 10:19:37.651896 | 128.119.245.12    | 192.168.1.105     | TCP      | 60     | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0      |
| 12  | 10:19:37.656065 | 128.119.245.12    | 192.168.1.105     | TCP      | 1514   | 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=146... |

> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
▼ Ethernet II, Src: CnetTech\_73:8d:ce (00:80:ad:73:8d:ce), 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. .... = LG bit: Locally administered address (this is NOT the factory default)  
            .... 1. .... = IG bit: Group address (multicast/broadcast)  
    ▼ Source: CnetTech\_73:8d:ce (00:80:ad:73:8d:ce)  
        Address: CnetTech\_73:8d:ce (00:80:ad:73:8d:ce)  
            .... 0. .... = LG bit: Globally unique address (factory default)  
            .... 0. .... = IG bit: Individual address (unicast)  
        Type: ARP (0x0806)  
        Padding: 00000000000000000000000000000000  
    ▼ Address Resolution Protocol (request)  
        Hardware type: Ethernet (1)  
        Protocol type: IPv4 (0x0800)  
        Hardware size: 6  
        Protocol size: 4  
        Opcode: request (1)  
        Sender MAC address: CnetTech\_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 (00:00:00:00:00:00)  
        Target IP address: 192.168.1.117

0000 ff ff ff ff ff 00 80 ad 73 8d ce 08 06 00 01 .....S.....  
0010 08 00 06 04 00 01 00 80 ad 73 8d ce c0 a8 01 68 .....S.....h  
0020 00 00 00 00 00 00 c0 a8 01 75 00 00 00 00 00 .....  
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Address Resolution Protocol (arp), 28 bytes      Packets: 17 · Displayed: 17 (100.0%)      Profile: Default

## Extra Credit

EX-1. The *arp* command:

*arp -s InetAddr EtherAddr*

allows you to manually add an entry to the ARP cache that resolves the IP address *InetAddr* to the physical address *EtherAddr*. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

**The router/adaptor would remove the IP address from the Ethernet frame and using ARP, once the router/adaptor received the destination IP address (even if we entered in the incorrect MAC address). It would get the correct MAC address of the destination.**

EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.

**Since the default time to keep the ARP table entry is 20 minutes, the ARP table will refresh itself every 20 minutes. Though, the neighboring device can be out of the network so the ARP table should be updated according to the network states. When the table gets refreshed the content will get erased and when the chance comes to resolve the MAC address to the known IP address the ARP request will be sent in broadcast mode where the reply will be in Unicast mode.**