

Jed Alcantara  
G00846927  
Lab 3

```
> Frame 939: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface \Device\NPF_{6656
▼ Ethernet II, Src: IntelCor_5a:aa:0a (94:b8:6d:5a:aa:0a), Dst: Cisco_ff:fd:e0 (00:08:e3:ff:fd:e0)
  ▼ Destination: Cisco_ff:fd:e0 (00:08:e3:ff:fd:e0)
    Address: Cisco_ff:fd:e0 (00:08:e3:ff:fd:e0)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
  ▼ Source: IntelCor_5a:aa:0a (94:b8:6d:5a:aa:0a)
    Address: IntelCor_5a:aa:0a (94:b8:6d:5a:aa:0a)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.151.130.124, Dst: 50.63.7.172
> Transmission Control Protocol, Src Port: 65134, Dst Port: 80, Seq: 1, Ack: 1, Len: 374
> Hypertext Transfer Protocol
```

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

The source mac address is a 48 bit address that is 94:b8:6d:5a:aa:0a.

2. What is the 48 bit destination MAC address in your Ethernet header? Which device does this MAC address correspond to?

The destination mac address is a 48 bit address that is 00:08:e3:ff:fd:e0.

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

The hexadecimal value for the two-byte Frame type field is 0x0800, IPv4. The upper layer protocol it corresponds to is IPv4.

0000	00 08 e3 ff fd e0 94 b8 6d 5a aa 0a 08 00 45 00	..... mZ....E-
0010	01 9e 47 cb 40 00 80 06 ea 90 0a 97 82 7c 32 3f	--G-@-... .. 2?
0020	07 ac fe 6e 00 50 28 b0 f6 60 81 81 1b ce 50 18	...n-P(- ..-P-
0030	02 00 de e5 00 00 47 45 54 20 2f 43 53 35 35 35	.....GE T /CS555
0040	2f 54 43 50 2d 77 69 72 65 73 68 61 72 6b 2e 68	/TCP-wir eshark.h
0050	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f	tml HTTP /1.1..Ho
0060	73 74 3a 20 77 77 77 2e 70 68 70 61 74 68 61 6b	st: www. phpthak
0070	2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74	.com..Us er-Agent
0080	3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57	: Mozill a/5.0 (W
0090	69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20	indows N T 10.0;
00a0	57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 3a 31	Win64; x 64; rv:1
00b0	30 39 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30	09.0) Ge cko/2010
00c0	30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 31 32	0101 Fir efox/112
00d0	2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74	.0..Acce pt: text
00e0	2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f	/html,ap plicatio
00f0	6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c	n/xhtml+ xml,appl
0100	69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e	ication/ xml;q=0.
0110	39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61	9,image/ avif,ima
0120	67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e	ge/webp, */*;q=0.
0130	38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61	8..Accep t-Langua
0140	67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30	ge: en-U S,en;q=0
0150	2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64	.5..Acce pt-Encod

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

G appears after 72bits or 9Bytes.

5. Print the contents of your computer's ARP cache. You can remove the names of personal devices if they appear in the cache if you want.

```
jad@jaddys-pc:~/CS455_Computer_Communications_and_Networking/CS455_Computer_Communications_and_Networking/14$ arp -a
jaddys-pc.mshome.net (172.21.64.1) at 00:15:5d:22:04:4f [ether] on eth0
jad@jaddys-pc:~/CS455_Computer_Communications_and_Networking/CS455_Computer_Communications_and_Networking/14$
```

6. Show the output of the command that prints the ARP cache to show that it is empty.

```
jad@jaddys-pc:~/CS455_Computer_Communications_and_Networking/CS455_Computer_Communications_and_Networking/14$ sudo ip -s -s neigh flush all
172.21.64.1 dev eth0 lladdr 00:15:5d:22:04:4f used 951/951/919 probes 1 STALE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
```

7. Include a screenshot of the ARP request and response from your capture.

2949	17.931604	IntelCor_5a:aa:0a	Google_ae:a8:60	ARP	42 Who has 10.151.128.85? Tell 10.151.130.124
2950	17.988586	Google_ae:a8:60	IntelCor_5a:aa:0a	ARP	60 10.151.128.85 is at ac:67:84:ae:a8:60

  

The screenshot shows the details of an ARP request packet (Frame 2949) in Wireshark. The packet is an Ethernet II frame with source MAC IntelCor\_5a:aa:0a and destination MAC Google\_ae:a8:60. The payload is an ARP request (Opcode: request (1)) for the IP address 10.151.128.85. The sender IP is 10.151.130.124 and the target IP is 10.151.128.85.

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

The source ip address is 10.151.130.124.

The destination ip address is 10.151.128.85.

9. What are the source and destination MAC addresses for your ARP response?

The source hexadecimal value is 94:b8:6d:5a:aa:0a.

The destination hexadecimal value is ac:67:84:ae:a8:60.

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

The ARP request with question appears from the sender, and it's asking for the target MAC address: Target MAC address: Google\_ae:a8:60 (ac:67:84:ae:a8:60) with an ip of 10.151.128.85

11. 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 ARP message has an answer for this MAC address: Sender MAC address: IntelCor\_5a:aa:0a (94:b8:6d:5a:aa:0a) with an ip of 10.151.130.124.