Arthur Liou
CS372
Lab 5

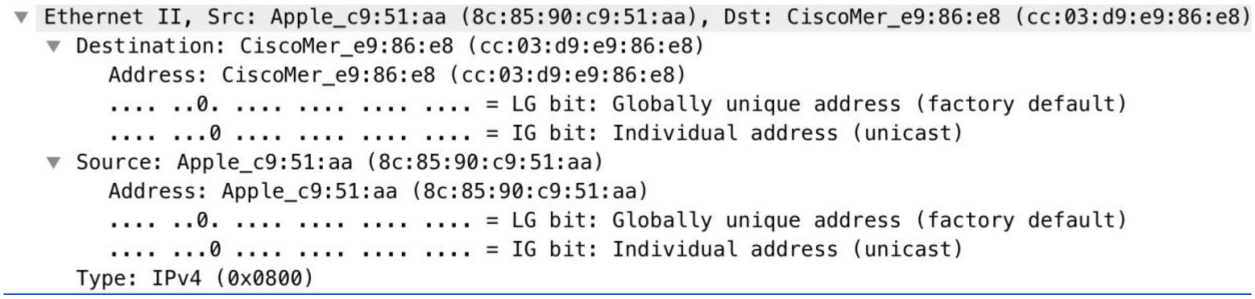
Notes: I've attached my screenshots and boxed in red where I annotated my output.

1. What is the 48-bit Ethernet address of your computer?
8c:85:90:c9:51:aa

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.]
cc:03:d9:e9:86:e8
No, it's for the local router.

3. Give the hexadecimal value for for the two-byte Frame type field. What upper layer protocol does this correspond to?
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?
TCP header is 20 bytes, IP header is 20 bytes, the Ethernet frame is 34 byes. Thus, begins at byte 75.



```
▼ Ethernet II, Src: Apple_c9:51:aa (8c:85:90:c9:51:aa), Dst: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
  ▼ Destination: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
      Address: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: Apple_c9:51:aa (8c:85:90:c9:51:aa)
      Address: Apple_c9:51:aa (8c:85:90:c9:51:aa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

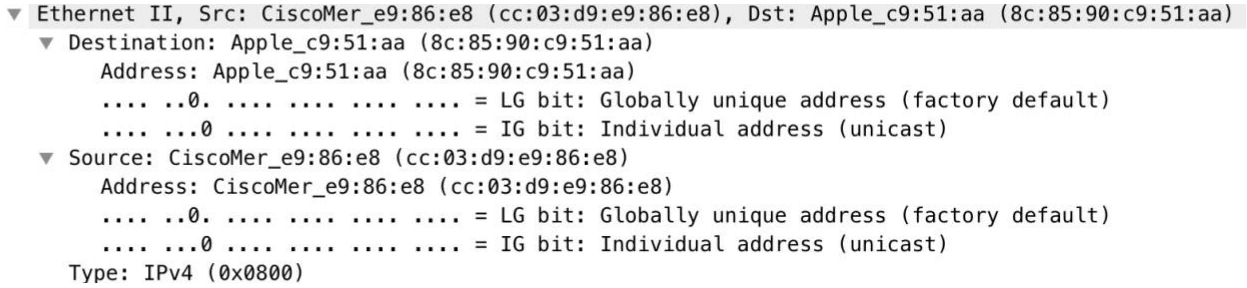
5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this as its Ethernet address?
cc:03:d9:e9:86:e8
No, it's for the local router.

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
8c:85:90:c9:51:aa, yes

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
IPv4 (0x0800)

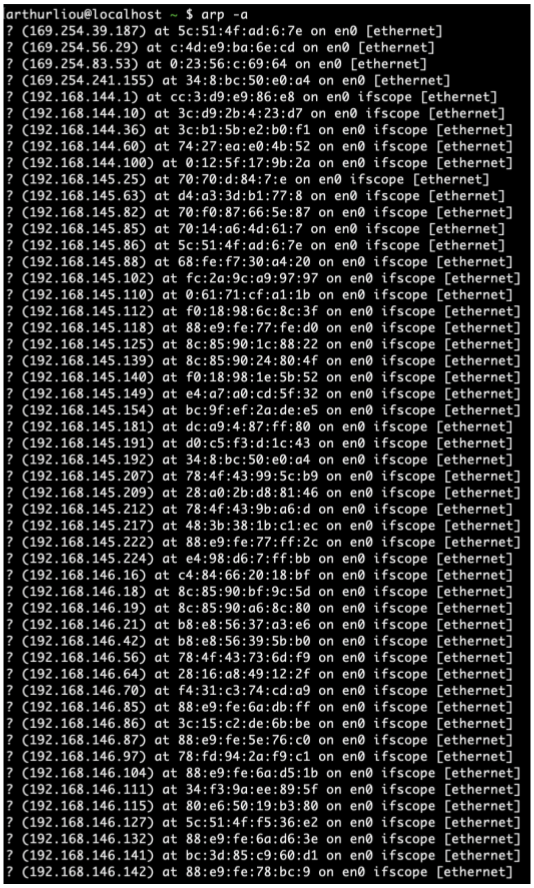
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK"

(i.e., the HTTP response code) appear in the Ethernet frame?
TCP header is 20 bytes, IP header is 20 bytes, the Ethernet frame is 34 byes. Thus, begins at byte 75.



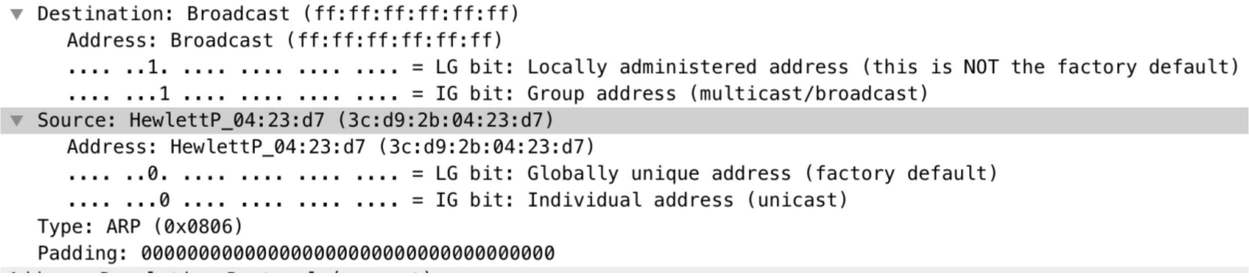
```
▼ Ethernet II, Src: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8), Dst: Apple_c9:51:aa (8c:85:90:c9:51:aa)
  ▼ Destination: Apple_c9:51:aa (8c:85:90:c9:51:aa)
      Address: Apple_c9:51:aa (8c:85:90:c9:51:aa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
      Address: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

9. Write down the contents of your computer’s ARP cache. What is the meaning of each column value?
IP address, Mac address, and protocol type



```
arthurliou@localhost ~ $ arp -a
? (169.254.39.187) at 5c:51:4f:ad:6:7e on en0 [ethernet]
? (169.254.56.29) at c:4d:e9:ba:6e:cd on en0 [ethernet]
? (169.254.83.53) at 0:23:56:c:69:64 on en0 [ethernet]
? (169.254.241.155) at 34:8:bc:50:e0:a4 on en0 [ethernet]
? (192.168.144.1) at cc:3:d9:e9:86:e8 on en0 ifscope [ethernet]
? (192.168.144.10) at 3c:d9:2b:4:23:d7 on en0 ifscope [ethernet]
? (192.168.144.36) at 3c:b1:5b:e2:b0:f1 on en0 ifscope [ethernet]
? (192.168.144.60) at 74:27:ea:e0:4b:52 on en0 ifscope [ethernet]
? (192.168.144.100) at 0:12:5f:17:9b:2a on en0 ifscope [ethernet]
? (192.168.145.25) at 70:70:d:84:7:e on en0 ifscope [ethernet]
? (192.168.145.63) at d4:a3:3d:b1:77:8 on en0 ifscope [ethernet]
? (192.168.145.82) at 70:f0:87:66:5e:87 on en0 ifscope [ethernet]
? (192.168.145.85) at 70:14:a6:4d:61:7 on en0 ifscope [ethernet]
? (192.168.145.86) at 5c:51:4f:ad:6:7e on en0 ifscope [ethernet]
? (192.168.145.88) at 68:fe:f7:30:a4:20 on en0 ifscope [ethernet]
? (192.168.145.102) at fc:2a:9c:a9:97:97 on en0 ifscope [ethernet]
? (192.168.145.110) at 0:61:71:cf:a1:1b on en0 ifscope [ethernet]
? (192.168.145.112) at f0:18:98:6c:8c:3f on en0 ifscope [ethernet]
? (192.168.145.118) at 88:e9:fe:77:fe:d0 on en0 ifscope [ethernet]
? (192.168.145.125) at 8c:85:90:1c:88:22 on en0 ifscope [ethernet]
? (192.168.145.139) at 8c:85:90:24:80:4f on en0 ifscope [ethernet]
? (192.168.145.140) at f0:18:98:1e:5b:52 on en0 ifscope [ethernet]
? (192.168.145.149) at e4:a7:a0:cd:5f:32 on en0 ifscope [ethernet]
? (192.168.145.154) at bc:9f:ef:2a:de:e5 on en0 ifscope [ethernet]
? (192.168.145.181) at dc:a9:4:87:ff:80 on en0 ifscope [ethernet]
? (192.168.145.191) at d0:c5:f3:d:1c:43 on en0 ifscope [ethernet]
? (192.168.145.192) at 34:8:bc:50:e0:a4 on en0 ifscope [ethernet]
? (192.168.145.207) at 78:4f:43:99:5c:b9 on en0 ifscope [ethernet]
? (192.168.145.209) at 28:a0:2b:d8:81:46 on en0 ifscope [ethernet]
? (192.168.145.212) at 78:4f:43:9b:a6:d on en0 ifscope [ethernet]
? (192.168.145.217) at 48:3b:38:1b:c1:ec on en0 ifscope [ethernet]
? (192.168.145.222) at 88:e9:fe:77:ff:2c on en0 ifscope [ethernet]
? (192.168.145.224) at e4:98:d6:7:ff:bb on en0 ifscope [ethernet]
? (192.168.146.16) at c4:84:66:20:18:bf on en0 ifscope [ethernet]
? (192.168.146.18) at 8c:85:90:bf:9c:5d on en0 ifscope [ethernet]
? (192.168.146.19) at 8c:85:90:a6:8c:80 on en0 ifscope [ethernet]
? (192.168.146.21) at b8:e8:56:37:a3:e6 on en0 ifscope [ethernet]
? (192.168.146.42) at b8:e8:56:39:5b:b0 on en0 ifscope [ethernet]
? (192.168.146.56) at 78:4f:43:73:6d:f9 on en0 ifscope [ethernet]
? (192.168.146.64) at 28:16:a8:49:12:2f on en0 ifscope [ethernet]
? (192.168.146.70) at f4:31:c3:74:cd:a9 on en0 ifscope [ethernet]
? (192.168.146.85) at 88:e9:fe:6a:db:ff on en0 ifscope [ethernet]
? (192.168.146.86) at 3c:15:c2:de:6b:be on en0 ifscope [ethernet]
? (192.168.146.87) at 88:e9:fe:5e:76:c0 on en0 ifscope [ethernet]
? (192.168.146.97) at 78:fd:94:2a:f9:c1 on en0 ifscope [ethernet]
? (192.168.146.104) at 88:e9:fe:6a:d5:1b on en0 ifscope [ethernet]
? (192.168.146.111) at 34:f3:9a:ee:89:5f on en0 ifscope [ethernet]
? (192.168.146.115) at 80:e6:50:19:b3:80 on en0 ifscope [ethernet]
? (192.168.146.127) at 5c:51:4f:f5:36:e2 on en0 ifscope [ethernet]
? (192.168.146.132) at 88:e9:fe:6a:d6:3e on en0 ifscope [ethernet]
? (192.168.146.141) at bc:3d:85:c9:60:d1 on en0 ifscope [ethernet]
? (192.168.146.142) at 88:e9:fe:78:bc:9 on en0 ifscope [ethernet]
```

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
Source: 3c:d9:2b:94:23:d7
Destination: ff:ff:ff:ff:ff:ff
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
ARP (0x0806)



```
▼ 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: HewlettP_04:23:d7 (3c:d9:2b:04:23:d7)
    Address: HewlettP_04:23:d7 (3c:d9:2b:04:23:d7)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 000000000000000000000000000000000000
```

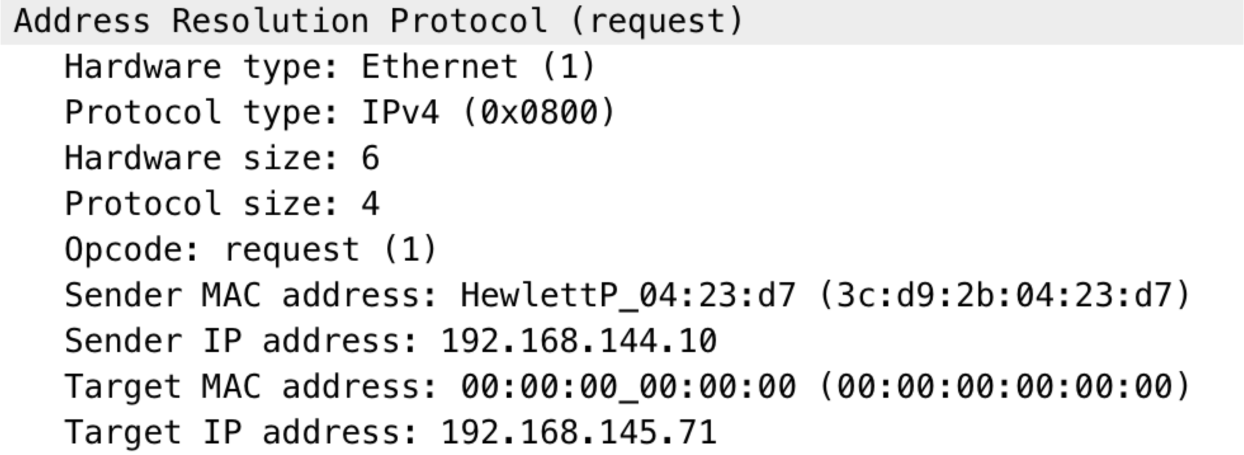
12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
Starts at the 21st byte

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?
1

c) Does the ARP message contain the IP address of the sender?
Yes, 192.168.144.10

d) Where in the ARP request does the "question" appear - the Ethernet address of the machine whose corresponding IP address is being queried?
It's saved in the Target IP address field



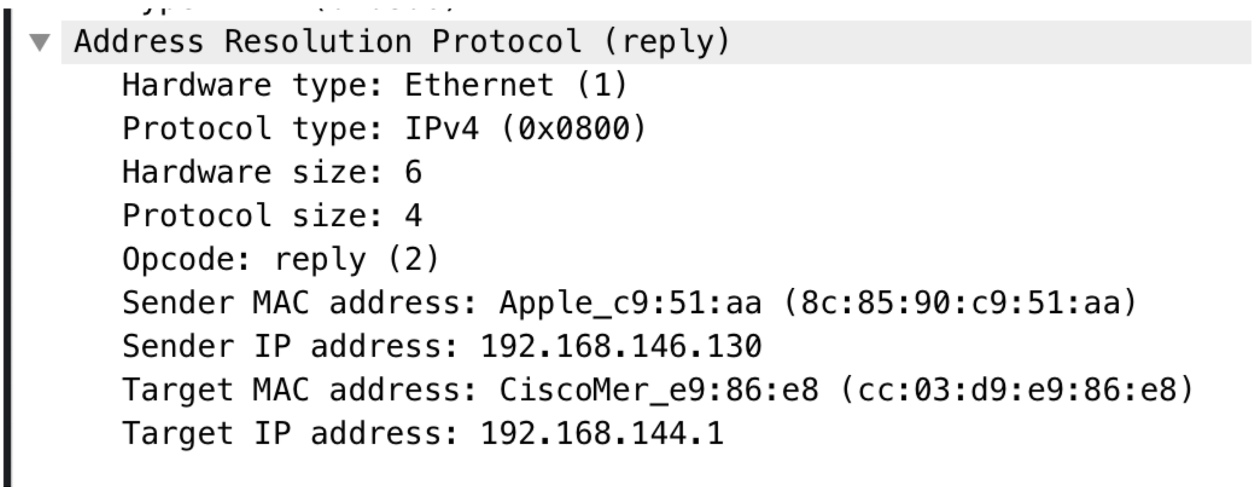
```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HewlettP_04:23:d7 (3c:d9:2b:04:23:d7)
    Sender IP address: 192.168.144.10
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.145.71
```

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?
Starts at the 21st byte

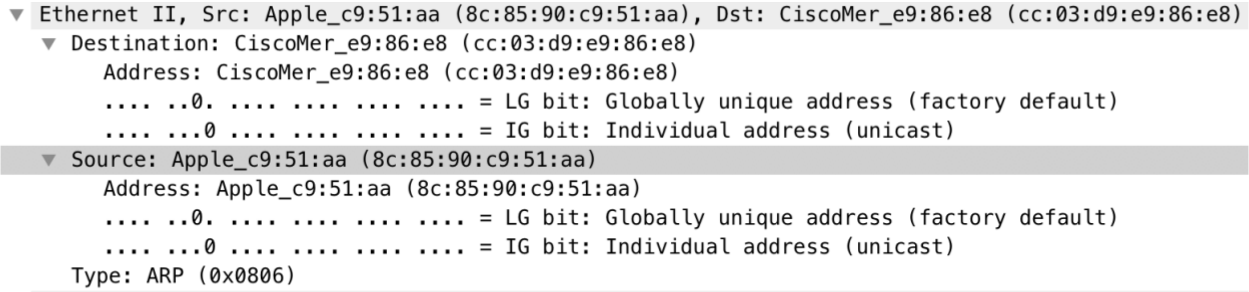
b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
2

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?
Response is saved in the Target MAC address (previously blank).



```
▼ 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_c9:51:aa (8c:85:90:c9:51:aa)
    Sender IP address: 192.168.146.130
    Target MAC address: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
    Target IP address: 192.168.144.1
```

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?
Source: 8c:85:90:c9:51:aa
Address: cc:03:d9:e9:86:e8



```
▼ Ethernet II, Src: Apple_c9:51:aa (8c:85:90:c9:51:aa), Dst: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
  ▼ Destination: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
      Address: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: Apple_c9:51:aa (8c:85:90:c9:51:aa)
      Address: Apple_c9:51:aa (8c:85:90:c9:51:aa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
```

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?
Answer: There’s no reply because the local machine (running Wireshark) isn’t the one that’s addressed in the Destination field, which is set to Broadcast ff:ff:ff:ff:ff:ff

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?

Answer: It would cause connectivity issues. The PC would look at the MAC address (from the IP address) and try to connect to a non-existent (or invalid) location. Until the values were removed, this would continue on

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.
Answer: Static entries only manually altered. Dynamic entries have a timeout of 10 minutes.
Source: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc958841(v=technet.10)