ENGR 3321 - Lab 7: Ethernet ARP

4 November 2022

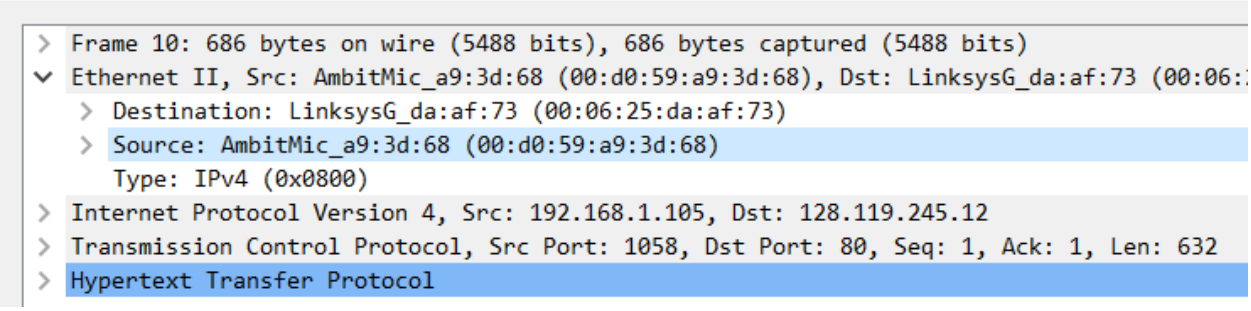
Nathan Cauwet

873271826

Note: I had to use the gaia.cs.umass.edu traces because I had too many things open so I was not able to clear my cache at the time.

Part 1 (Ethernet frames):

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



00:d0:59:a9:3d:68

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 destination is 00:06:25:da:af:73. Note that this is not the ethernet address of gaia.cs.umass.edu, it is the ethernet address of the router (in this case the Linksys router).

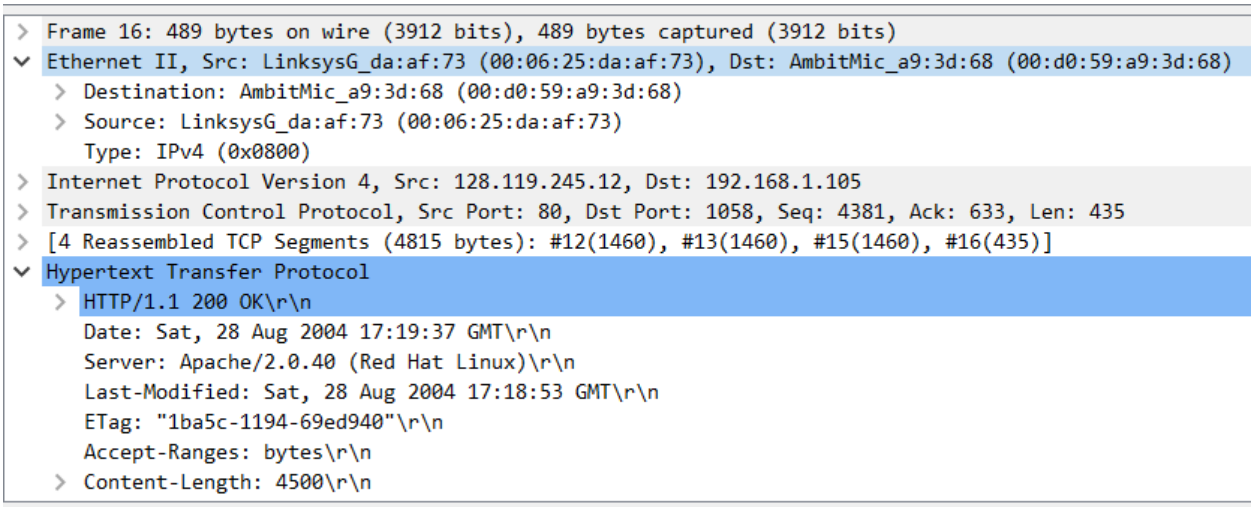
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hexadecimal value is 0x0800 which corresponds to the IPv4 protocol

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

52 bytes from the start of the ethernet frame. There are 14 bytes for the ethernet frame, 20 bytes for the IPv4 header, and 20 bytes for the TCP header that all precede it.

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.



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?

00:06:25:da:af:73 which is the address of the Linksys router mentioned earlier. Therefore it is neither the client computer or the gaia.cs.umass.edu, it is the step in between.

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 which corresponds to the client computer (“my computer” but I’m using the trace file so it’s that computer, if I’d been able to run it then it would be mine)

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

0x0800 which corresponds to IPv4

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?

52 bytes from the start of the ethernet frame. There are 14 bytes for the ethernet frame, 20 bytes for the IPv4 header, and 20 bytes for the TCP header that all precede it.

Part 2 (ARP):

The Windows arp command with no arguments will display the contents of the ARP cache on your computer. Run the arp command.

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

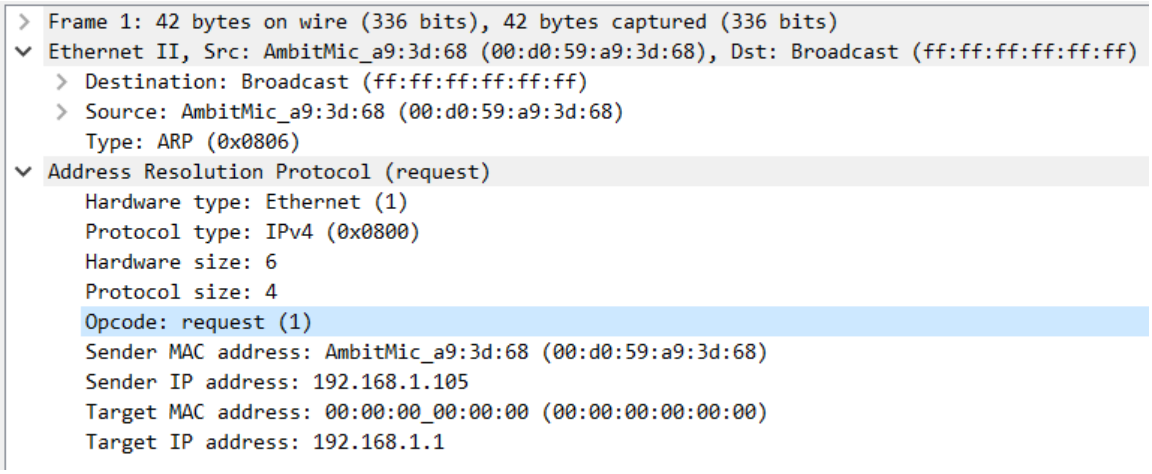
```
Interface: 192.168.0.10 --- 0x9
  Internet Address      Physical Address      Type
  192.168.0.1           ec-4f-82-88-88-71     dynamic
  192.168.0.4           dc-a6-32-be-f0-19     dynamic
  192.168.0.6           dc-a6-32-72-9a-71     dynamic
  192.168.0.16          dc-a6-32-72-9a-73     dynamic
  192.168.0.22          54-67-e6-68-62-d2     dynamic
  192.168.0.31          0c-62-a6-39-da-85     dynamic
  192.168.0.36          e8-84-a5-7d-f2-26     dynamic
  192.168.0.42          52-b3-62-4a-41-3d     dynamic
  192.168.0.255         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
  224.0.0.113           01-00-5e-00-00-71     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xb
  Internet Address      Physical Address      Type
  192.168.56.255        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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\ncauw>
```

Screen capture is above. The leftmost column shows the IPv4 address of the destination, the middle column (Physical Address) shows the MAC address of that device (saved from the last trusted connection), and the Type column shows whether the IP corresponding to the MAC address in the same row is a static or dynamic IP. This is important because if the type is static, the IP association with the corresponding MAC address should not change (so in the event that it does change either an error or a "are you sure you trust ____" is displayed). Dynamic IPs get recycled on some interval that is defined by their network, so a possible change is expected.

In the example, the first two frames in the trace contain ARP messages (as does the 6th message). The screen shot below corresponds to the trace mentioned earlier.



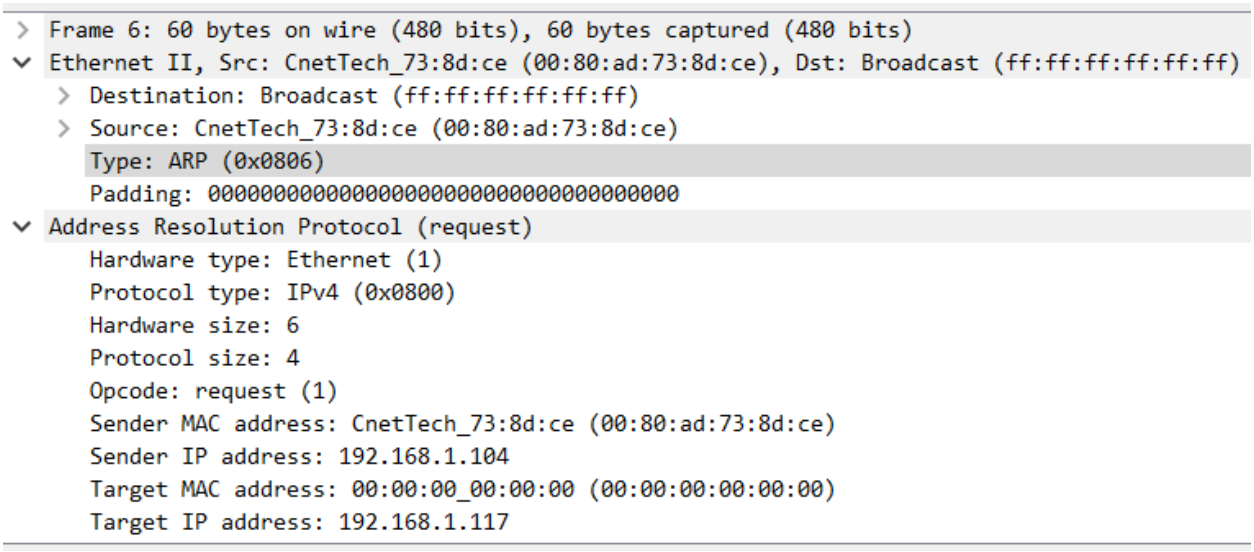
10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

The source is 00:d0:59:a9:3d:68 (client machine) and the destination is ff:ff:ff:ff:ff:ff (Broadcast)

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

The hex value of the two-byte ethernet frame is 0x0806 which corresponds to 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 code is 20 bytes from the start 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?

In the ARP payload part of the ethernet frame the opcode field is 0x0001 which in the context of ARP corresponds to ‘request’. (arp-request)

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

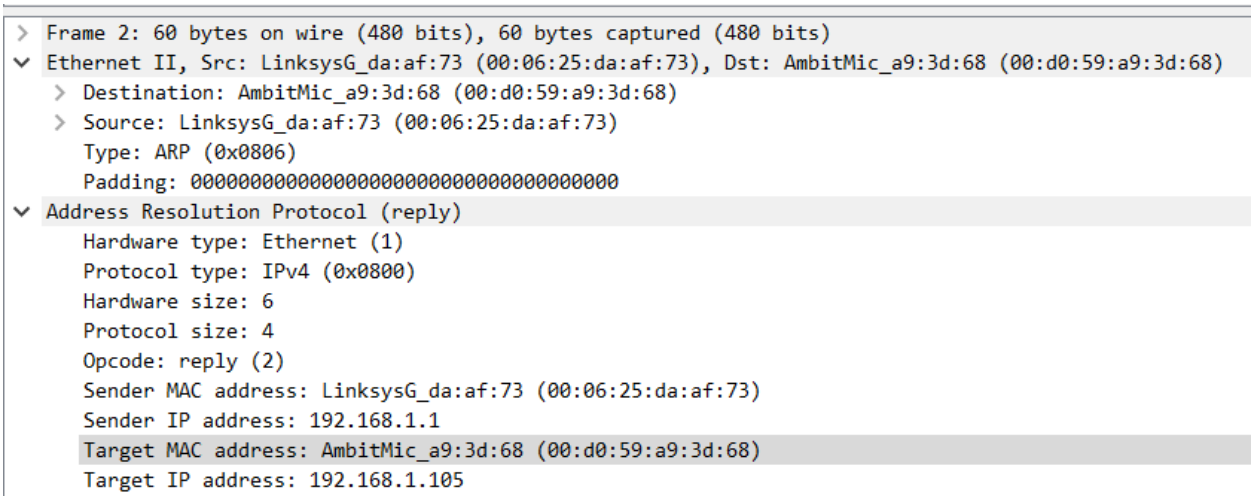
Yes, the IP of the sender is 192.168.1.105

(note: this is a subnet ip address, the target 192.168.1.1 is presumably the address of the router managing the subnet)

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

The ‘question’ appears in the ARP request in the field “Target MAC Address”. Since we do not yet know the physical address of the target IP, it is set to 00:00:00:00:00:00 so that it can find out what that MAC address is and assign it to the ARP tables. In other words, the MAC address of all 0s indicates that the sender is querying the target IP for its corresponding physical address.

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?

The ARP code starts 20 bytes from the 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 opcode in the ARP-payload part of the ethernet frame is 0x0002 (displayed as ‘2’) which is the opcode corresponding to “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 query request from earlier appears in the "Sender MAC address" field. The "Sender IP address" is 192.168.1.1 (the device that was queried by the client) and it is sending its MAC address 00:06:25:da:af:73 to the client that queried it. The target is of IP 192.168.1.105 and MAC address 00:d0:59:a9:3d:68, this is our client mentioned above.

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

The hexadecimal values in the ethernet frame containing the ARP reply are as follows:

Source (sender): 00:06:25:da:af:73

Destination (target): 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?

We see the broadcast for the other computer because a broadcast goes to the whole network, however, we do not see the reply for the request sent by the other computer because the ARP reply only sends it’s answer to the machine that requested it.