LAB 3

Ivan Martinovic

HTTP GET:
Packet 26

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

The MAC address of my computer is the source Address of packet 26:
30:3a:64:b3:a4:c0

Note: It could also be found using CMD ipconfig /all (see additional screenshot for Question1)

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 MAC address is:

e4:18:6b:7c:b0:b0

This address corresponds to the MAC address of my home address.

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

The hex value of the Type field is: **0x0800**
It 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?

The ASCII G starts (16*3+6)=**54 bytes** from the very start of the Ethernet frame.

HTTP OK
Packet 30

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 MAC address is:
e4:18:6b:7c:b0:b0

This corresponds to the MAC address of **my home router**.

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

The destination MAC address is:
30:3a:64:b3:a4:c0

This indeed corresponds to the MAC 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 of the Type field is: **0x0800**
It again corresponds to the **IPv4 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 ASCII O appears (4*16+3)=**67 bytes** from the very start of the Ethernet frame.

Note: the response message itself (the first character H) starts (3*16+6)=54 bytes from the very start of the Ethernet frame, same as for question 4

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

Interface: 192.168.2.174 --- 0x8

Internet Address	Physical Address	Type
192.168.2.1	e4-18-6b-7c-b0-b0	dynamic
192.168.2.22	8c-89-a5-cd-3a-9d	dynamic
192.168.2.255	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

The first column is the IP address of a host. The second column is the MAC address of the host to which that IP address corresponds to. The third is the type of the interface (static or dynamic).

ARP REQUEST

Packet 4

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

The source MAC address is:
30:3a:64:b3:a4:c0

The destination MAC address is:
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?

The hex value of the Type field is: **0x0806**
This corresponds to the **ARP protocol**.

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?

Based on the specification, the opcode should begin **20 bytes** after the very beginning of the Ethernet frame. This is confirmed by the screenshot.

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?

When a request is made the value of the opcode field is **0x0001** which corresponds to:
ares_op$REQUEST

c) Does the ARP message contain the IP address of the sender?
Yes, it must contain the IP address of the server. In hex the IP address of the sender is: **c0:a8:02:ae** which corresponds to **192.168.2.174**

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

The questions starts 32 bytes from the start of the frame. The MAC address is: **00:00:00:00:00:00** indicating it is unknown and the IP address is **c0:a8:02:01** which corresponds to **192.168.2.1**

ARP RESPONSE
Packet 5

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 opcode begins **20 bytes** from the start of the 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 value of the opcode field is: **0x0002** which corresponds to **ares_op$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 begins **22 bytes** from the start of the frame. It says MAC address **e4:18:6b:7c:b0:b0** corresponds to IP address **c0:a8:02:01** or **192.168.2.1**

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

The source MAC address is: **e4:18:6b:7c:b0:b0**
The destination MAC address is: **30:3a:64:b3:a4:c0**

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?

Because the host computer does not know the MAC address of 192.168.1.117.