Mihai Dan

11/28/2015

CS 372

Lab 5

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

The 48-bit Ethernet address of my computer is f4:b7:e2:59:a7:73.

**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 Ethernet destination address is e8:fc:af:83:5d:e4. This is not the address of gaia.cs.umass.edu, but it is the address of my Netgear router. The reason that its Ethernet address is shown is because that is the link between the subnet and the rest of the internet. My computer does not know the destination Ethernet address.

**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 Frame type field is 0x0800. This corresponds to the Internet Protocol, meaning the frame contains an IP datagram.

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

There are 54 bytes between the start of the Ethernet frame and the ASCII value that represents the letter “G”. The reason it appears 54 bytes into the Ethernet frame is because there are 14 Bytes for the Ethernet frame, 20 Bytes for the IP header, and 20 Bytes for the TCP header.

**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 value of the Ethernet source address is e8:fc:af:83:5d:e4. This Ethernet source address is neither that of my computer nor that of gaia.cs.umass.edu; this is the Ethernet address of my router. This is because only the address of the next hop is given, which, in this case, it happens to be my router.

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

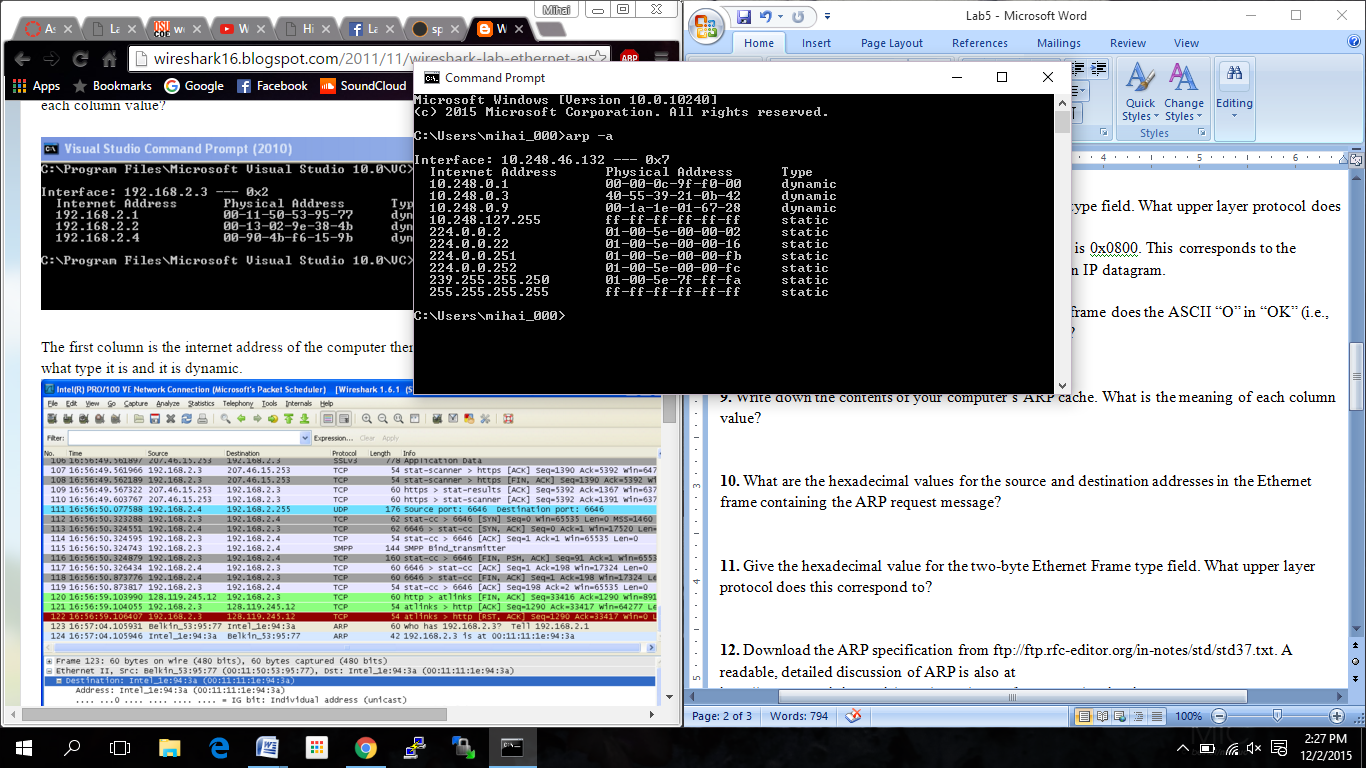
The destination address in this Ethernet frame is f4:b7:e2:59:a7:73. This is the Ethernet address of my computer.

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

The hexadecimal value for the Frame type field is 0x0800. This corresponds to the Internet Protocol, meaning the frame contains an IP datagram.

**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?

There are 54 bytes between the start of the Ethernet frame and the ASCII value that represents the letter “O”. The reason it appears 54 bytes into the Ethernet frame is because there are 14 Bytes for the Ethernet frame, 20 Bytes for the IP header, and 20 Bytes for the TCP header.

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

I. Internet Address column contains the IPv4 addresses.

II. The Physical Address column contains the MAC addresses.

III. The type column shows whether the IPv4 address is static or dynamic.

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

The source address found in this Ethernet frame is the Ethernet address of my computer, which is f4:b7:e2:59:a7:73, while the destination address is the Ethernet Broadcast address, which 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 hexadecimal value for the Ethernet Frame type field is 0x0806. This two-byte value 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 opcode field appears 20 Bytes in to 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 found for the opcode field within the ARP-payload of the request is 0x0001, which means request.

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

Yes, the ARP message contains the IP address of 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?

The MAC address 00:00:00:00:00:00 is set in the Target MAC Address Field to “question” the IP address that is being queried.

**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 opcode field begins 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 hex value found for the opcode field within the ARP-payload of the request is 0x0002, which means 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 ARP message contains a Sender MAC Address Field that contains the address e8:fc:af:83:5d:e4. This MAC address corresponds to the IP address of my router, which is 192.168.1.1

**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 e8:fc:af:83:5d:e4, which is correspondent to my router. The hex value for the destination address is f4:b7:e2:59:a7:73, which is correspondent to my computer.

**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 ARPrequested 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?

The reason that there is no reply message is because my computer is not the machine that sent the request. The ARP request is broadcast, and the ARP reply is sent directly back to the sender’s Ethernet address. Since my machine is not the source of the request, it will not get an ARP reply sent.