Eddie C. Fox

March 19, 2017

CS 372 Introduction to Networking

Lab 5

Part 1: Capturing and Analyzing Ethernet Frames

Note: I had difficulties with a live capture, so I used the Ethernet ethereal trace 1 as shown on the footnotes of Page 1. It's kind of ambiguous which packet corresponds to the HTTP get message and which one corresponds to the first frame of the response, since the packets are all filtered and I couldn't find any HTTP get packets, so I am going to assume that "my" computer and source of the get is the first one I could find: AmbitMic, and the destination is LinksysG. It could be the reverse, but please grade based on the first assumption since this is the best I could do with the ethereal trace information given to me.

1. My 48-bit address is 00:d0:59:a9:3d:68. http://puu.sh/uR3LH/72aaf98a74.png
2. 48 bit address of the destination is 00:06:25:da:af:73. It is not the address of the ultimate destination, gaia, but the address of the Linksys router we are connected to, used to get off the subnet. http://puu.sh/uR3NI/03ea8be683.png
3. The hex value for the frame field is 0x800 (IPV4) http://puu.sh/uR3YL/e43220aab7.png
4. 54 bytes from the start if we count the first byte as 0 from the start. http://puu.sh/uR4wQ/ab848a6e91.png
5. The source address is 00:06:25:da:af:73. As before, this is not the address of gaia but the Linksys router we are connected to, used to get off the subnet.
6. The destination address is 00:d0:59:a9:3d:68, which is our computer. http://puu.sh/uR4Nj/30cd4df283.png
7. The hex value is 0x800, corresponding to IPV4. http://puu.sh/uR4Ss/82c5b8d4aa.png
8. 67 bytes from the start if we count the first byte as 0 from the start. http://puu.sh/uR56M/f9b6818f57.png

Part 2: The Address Resolution Protocol

9. The contents of ARP are here: http://puu.sh/uR5hH/12da402509.png
   157.55.85.212 is my internet address and 00-aa-00-62-c6-08 is my physical mac address.
10. As I had difficulties earlier, I am still using the Ethernet Etheral Trace 1, which came with ARP protocol packets. The hex value for the source address is 00:d0:59:a9:3d:68, my computer. The destination is ff:ff:ff:ff:ff:ff, the broadcast address. http://puu.sh/uR5Ey/c0a1dbe182.png
11. The hex value of the frame type is 0x806, corresponding to the ARP protocol. http://puu.sh/uR5Jg/2d0160b77f.png
12.

a. The opcode field begins 20 bytes after the start of the Ethernet frame. http://puu.sh/uR6dS/55ec077b44.png
b. 0x001, for request. http://puu.sh/uR6dS/55ec077b44.png
c. Yes, it contains the address of the sender. http://puu.sh/uR6f5/3f4effccd8.png
d. The "question" is the targets MAC address, which is set to 00:00:00:00:00:00 by default http://puu.sh/uR6j9/6e9b0c311c.png

13.
a. The opcode begins 20 bytes after the start. http://puu.sh/uR6rY/10c71f1ce9.png
b. 0x002, for reply. http://puu.sh/uR6vj/8cacf76a7a.png
c. The "answer" is in the sender MAC address of the reply. http://puu.sh/uR6wY/7b809eadbf.png

14. The source address is 00:06:25:da:af:73 corresponding to the Linksys router, and the destination address is 00:d0:59:a9:3d:68, corresponding to "my" computer. http://puu.sh/uR6D8/b43a5e7dee.png
15. I've been using the trace this entire time, so I don't need to open it up. To answer the question though, there is no reply because we aren't on the computer or machine that sent the request. The ARP was broadcast to all machines on the subnet, but the response would only go to the querying computer, not to everyone. As we are not the querying computer, we don't get a response.