CS 1652 – Data Communication and Computer Networks – Project#4[1]

Due: Monday August 3rd @ 11:59pm

Late submission: No Late submission date

OVERVIEW

Purpose: To analyze link-layer protocols in captured packet traces

Goal 1: To analyze the Ethernet and ARP protocols.

Goal 2: To analyze the 802.11 Wi-Fi protocol.

More specific details follow below.

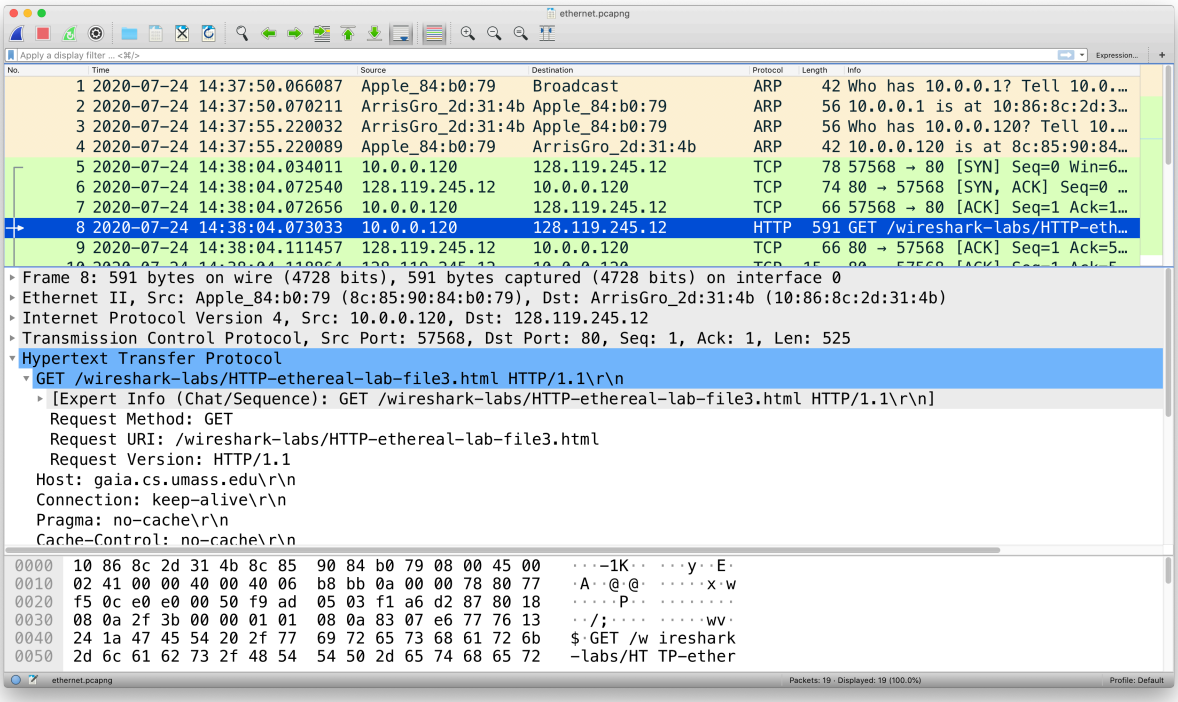
PART 1: ETHERNET AND ARP

In this part, we'll investigate the Ethernet protocol and the ARP protocol. Before beginning this lab, you'll probably want to review sections 6.4.1 (Link-layer addressing and ARP) and 6.4.2 (Ethernet) in the text[2]. RFC 826 (ftp://ftp.rfc-editor.org/in-notes/std/std37.txt) contains the gory details of the ARP protocol, which is used by an IP device to determine the IP address of a remote interface whose Ethernet address is known.

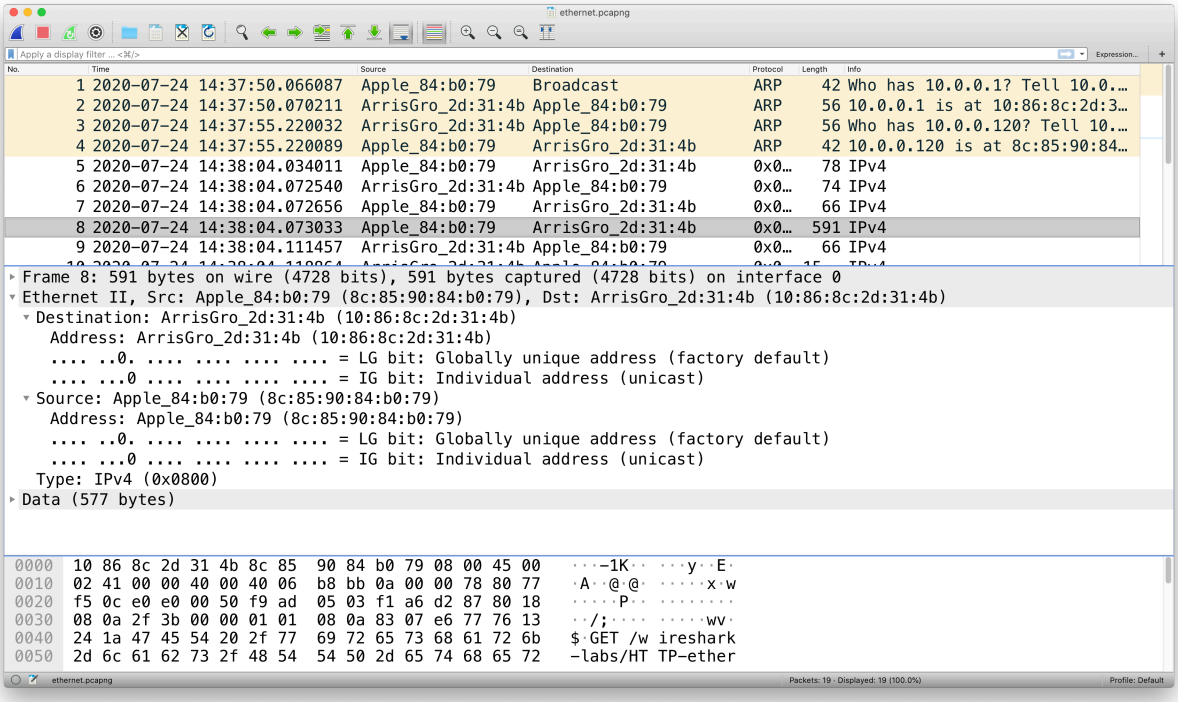
- Download the file ethernet.pcapng from the Project 4 page on Canvas. The trace file was collected by Wireshark running on one of your instructor's computers, while opening the page http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the downloaded trace file. You can then use this trace file to answer the questions below.
- First, find the packet numbers (the leftmost column in the upper Wireshark window) of the HTTP GET message that was sent from your computer to gaia.cs.umass.edu, as well as the beginning of the HTTP response message sent to your computer by gaia.cs.umass.edu. You should see a screen that looks something like this (where packet 8 in the screen shot below contains the HTTP GET message)

[1] Adapted from the Ethernet and ARP v7.0 and the 802.11 v7.0 lab exercises from Computer Networking: A Top-Down Approach, 7th ed., J.F. Kurose and K.W. Ross.

[2] References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down Approach, 7th ed.,* J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.



- Since this part is about Ethernet and ARP, we're not interested in IP or higher-layer protocols. So, let's change Wireshark's "listing of captured packets" window so that it shows information only about protocols below IP. To have Wireshark do this, select *Analyze->Enabled Protocols.* Then uncheck the IPv4 box and select *OK*. You should now see a Wireshark window that looks like:



In order to answer the following questions, you'll need to look into the packet details and packet contents windows (the middle and lower display windows in Wireshark).

Select the Ethernet frame containing the HTTP GET message. (Recall that the HTTP GET message is carried inside of a TCP segment, which is carried inside of an IP datagram, which is carried inside of an Ethernet frame; reread section 1.5.2 in the text if you find this encapsulation a bit confusing). Expand the Ethernet II information in the packet details window. Note that the contents of the Ethernet frame (header as well as payload) are displayed in the packet contents window.

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message. Whenever possible, when answering a question, you should attach an annotated printout of the packet(s) within the trace that you used to answer the question asked. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question. What we mean by annotation is to highlight the relevant part(s) of the packet that you used to answer the question.

1-1.What is the 48-bit Ethernet address of the instructor's computer?

1-2.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.]

1-3.Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

1-4.How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

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

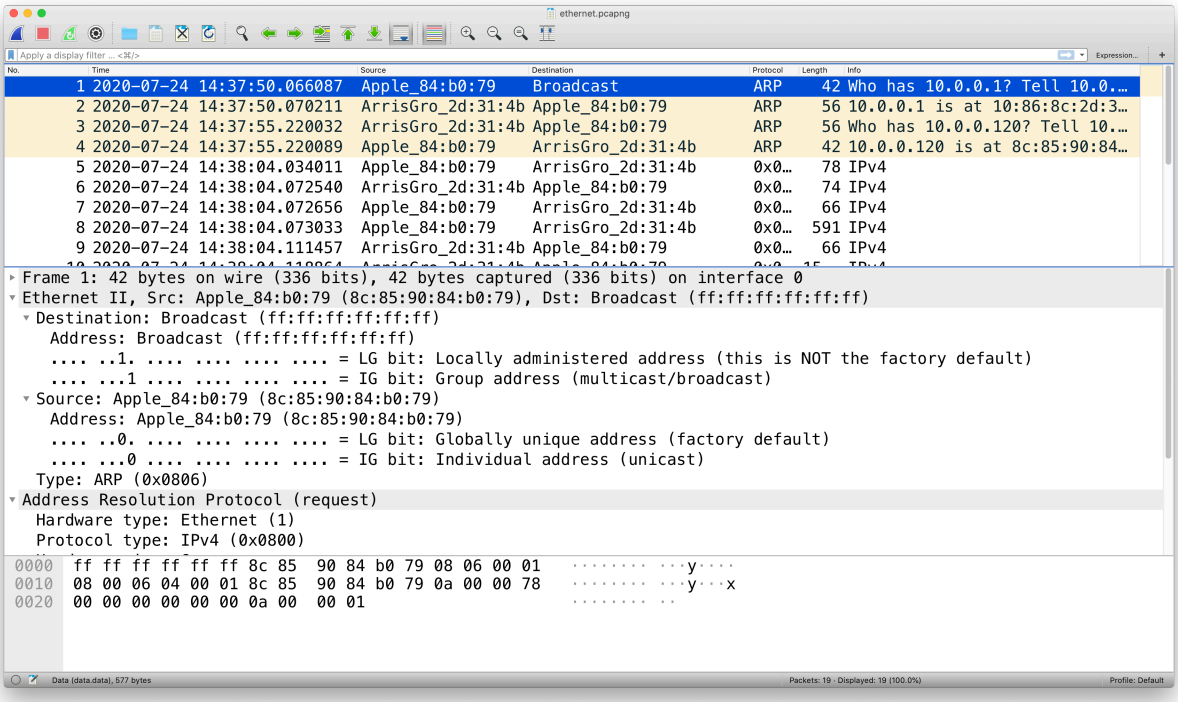
1-5. What is the value of the Ethernet source address? Is this the address of the instructor's computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this as its Ethernet address?

1-6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

1-7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

1-8. 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?

Next, we'll observe the ARP protocol in action. We strongly recommend that you re-read section 6.4.1 in the text before proceeding.



In the figure above, the first four frames in the trace contain ARP messages (as does the 6th message).

Answer the following questions:

1-9. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the first ARP request message?

1-10. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

1-11. Now find the ARP reply that was sent in response to the ARP request.

1-12. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

1-13. 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?

1-14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

PART 2: 802.11 (WI-FI)

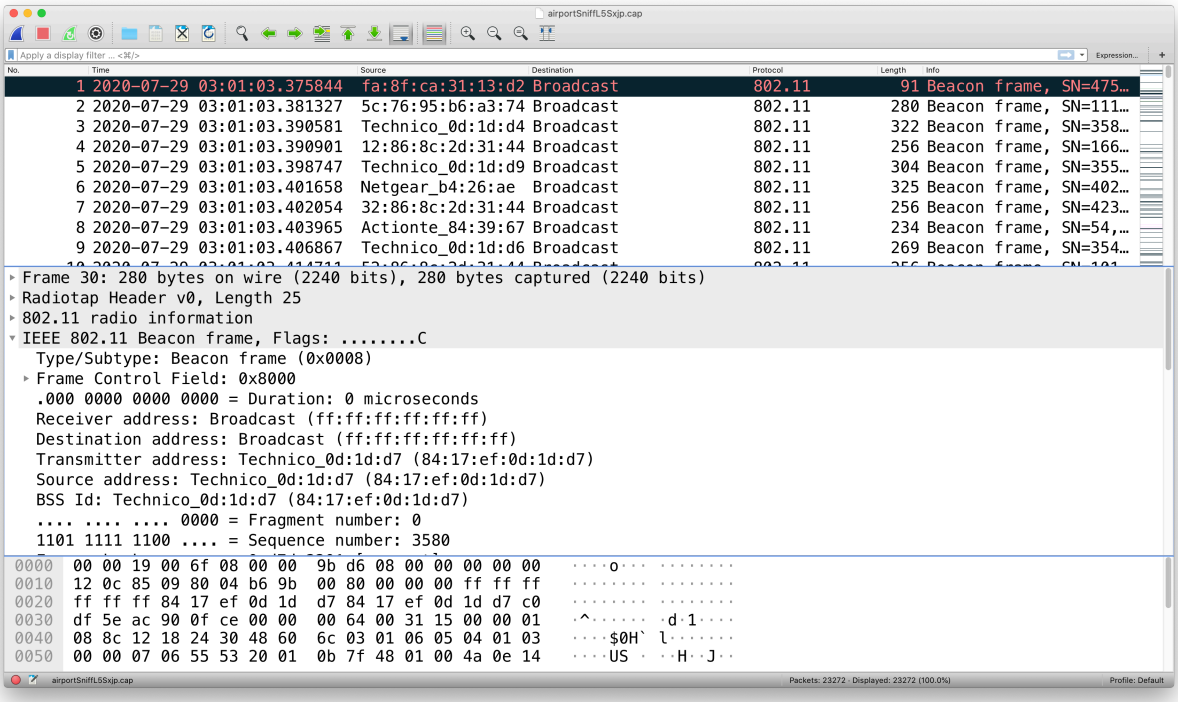
In this part, we'll investigate the 802.11 wireless network protocol. Before beginning this part, you might want to re-read Section 7.3 in the text. Since we'll be delving a bit deeper into 802.11 than is covered in the text, you might want to check out "A Technical Tutorial on the 802.11Protocol," by Pablo Brenner (Breezecom Communications), http://www.sss-mag.com/pdf/802_11tut.pdf, and "Understanding 802.11 Frame Types,"

by Jim Geier, http://www.wi-fiplanet.com/tutorials/article.php/1447501. And, of course, there is the standard itself, "ANSI/IEEE Std 802.11, 1999 Edition (R2003)," http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf. In particular, you may find Table 1 on page 36 of the standard particularly useful when looking through the wireless trace.

Download the file 802_11.pcapng. This trace was collected using Wireshark running on a computer in the home network of the instructor. In this trace file, we'll see frames captured on channel 6. Since the host and AP that we are interested in are not the only devices using channel 6, we'll see a lot of frames that we're not interested in for this part, such as beacon frames advertised by other APs also operating on channel 6. The wireless host activities taken in the trace file are:

- The host is already associated with the *xfinitywifi* AP when the trace begins.
- Starting from packet no .1108, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12.
- Starting from packet no. 19531*, t*he host makes an HTTP request to http://www.cs.pitt.edu/~skhattab/cs1652/, whose IP address is 136.142.35.172.

Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the 802_11.pcapng trace file. The resulting display should look just like the figure below.



Recall that **beacon frames** are used by an 802.11 AP to advertise its existence. To answer some of the questions below, you'll want to look at the details of the "IEEE 802.11" frame and subfields in the middle Wireshark window. Whenever possible, when answering a question below, you should include a printout of the packet(s) within the trace that you used to answer the question asked. To print a packet,

use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

Hint: You can filter for the beacon frames using the expression wlan.fc.type_subtype == 8.

2-1. What are the intervals of time between the transmissions of the beacon frames from the *xfinitywifi* access point? From the *KHATTAB-2.4* access point? (Hint: this interval of time is contained in the beacon frame itself).
2-2. What (in hexadecimal notation) is the source MAC address on the beacon frame from *xfinitywifi*? **Hint**: the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).
2-3. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *KHATTAB-2.4*?
2-4. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *xfinitywifi*?
2-5. The beacon frames from the *xfinitywifi* access point advertise that the access point can support eight data rates. What are these rates in Mbit/sec?

Let's look at a data transfer. Recall that in this trace, starting from packet no. 1108, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12. Then, starting from packet no. 19531*, t*he host makes an HTTP request to http://www.cs.pitt.edu/~skhattab/cs1652/ .The IP address of www.cs.pitt.edu is 136.142.35.172.

2-6. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device?
2-7. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).

Recall from Section 7.3.1 in the text that a host must first *associate* with an access point before sending data. Association in 802.11 is performed using the ASSOCIATE REQUEST frame (sent from host to AP, with a frame type 0 and subtype 0, see Section 7.3.3 in the text) and the ASSOCIATE RESPONSE frame (sent by the AP to a host with a frame type 0 and subtype of 1, in response to a received ASSOCIATE REQUEST). For a detailed explanation of each field in the 802.11 frame, see page 34 (Section 7) of the 802.11 spec at http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf.

2-8. Examine the trace file and look for AUTHENICATION frames (wlan.fc.type_subtype == 11) sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the *xfinitywifi* AP (which has a MAC address of 84:17:ef:0d:1d:d6) starting at packet no. 7514*?* .
2-9. Does the host want the authentication to require a key or be open?

2-10. Do you see a reply AUTHENTICATION from the *xfinitywifi* AP in the trace?

2-11. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associate with an AP. At which packet no. is there an ASSOCIATE REQUEST from host to the *xfinitywifi*? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == f0:6e:0b:ba:d7:71" to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

2-12. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the Tagged parameters fields of the 802.11 wireless LAN management frame.

SUBMISSION INSTRUCTIONS

Answer the questions in this document and upload it to the Project page on Canvas.

GRADE BREAKDOWN

Item	**Number of Points**
Each question	4