CO513 - Lab 07
Wireless Wireshark Lab - 802.11

802.11 Wireless Network Protocol

IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand and are the world's most widely used wireless computer networking standards. IEEE 802.11 is used in most home and office networks to allow laptops, printers, smartphones, and other devices to communicate with each other and access the Internet without connecting wires.

Lab Exercise

This lab focuses on 802.11 wireless network protocol.

For the lab, download the given “wireshark-traces.zip” in FEeLS and extract the file “Wireshark_802_11.pcap”

Description on the Trace File.

This trace was collected using AirPcap and Wireshark running on a computer in the home network, consisting of a Linksys 802.11g combined access point/router, with two wired PCs and one wireless host PC attached to the access point/router. The author is fortunate to have other access points in neighboring houses available as well. 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 lab, such as beacon frames advertised by a neighbor’s AP also operating on channel 6. The wireless host activities taken in the trace file are:

- The host is already associated with the *30 Munroe St* AP when the trace begins.
- At *t = 24.82*, the host makes an HTTP request to website A. The IP address of website B is 128.119.245.12.
- At *t=32.82, t*he host makes an HTTP request to website C, whose IP address is 128.119.240.19.
- At *t = 49.58,* the host disconnects from the *30 Munroe St* AP and attempts to connect to the *linksys_ses_24086*. This is not an open access point, and so the host is eventually unable to connect to this AP.

- At *t=63.0* the host gives up trying to associate with the *linksys_ses_24086 AP,* and associates again with the *30 Munroe St* access point.

Steps to load Wireshark Traces

Open Wireshark

Got to FIle -> Open and select “Wireshark_802_11.pcap” from the extracted directory to load the traces to Wireshark.

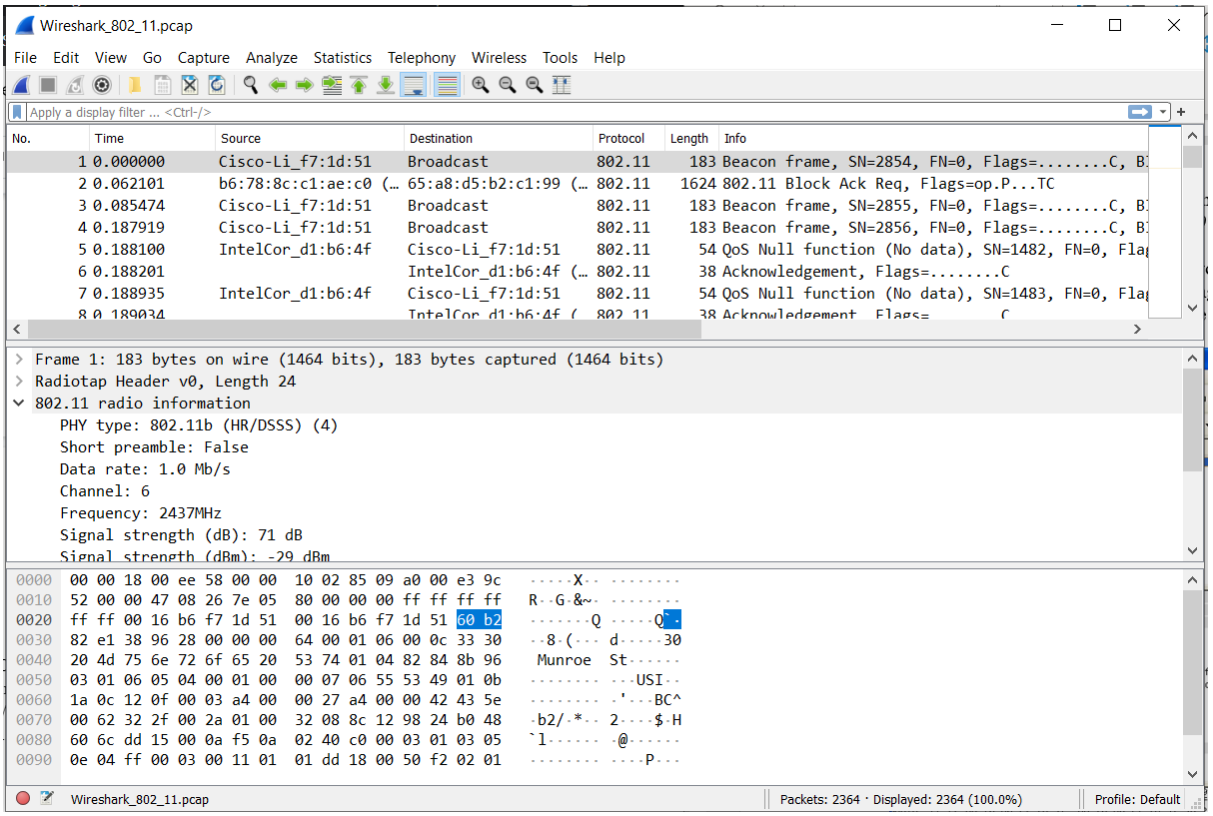

Figure 1: Wireshark window, after opening the Wireshark_802_11.pcap file

1. Beacon Files

Beacon frames are used by an 802.11 AP to advertise its existence. Observe the details of the “IEEE 802.11” frame and subfields in the middle Wireshark window to answer the following questions.
NOTE: For answering, capture the Screenshots of the traces, where the answer for the questions is, highlight and comment on the observations.

Exercise 1

1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?
2. What are the intervals of time between the transmissions of the beacon frames and the *linksys_ses_24086* access point? From the *30 Munroe St*. access point? (Hint: this interval of time is contained in the beacon frame itself).
3. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 7.13 in the text that 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).
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*??
5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *30 Munroe St*?
6. The beacon frames from the *30 Munroe St* access point advertise that the access point can support four data rates and eight additional "extended supported rates." What are these rates?

2. Data Transfer

The trace starts with the host already associated with the AP. First observe the data transfer over an 802.11 association before looking at AP association/disassociation. Given that, in this trace, at t = 24.82, the host makes an HTTP request to website A. The IP address of website B is 128.119.245.12. Then, at t=32.82, the host makes an HTTP request to website C.

Exercise 2

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt).
   - 7.1. What are three MAC address fields in the 802.11 frame?
   - 7.2. Which MAC address in this frame corresponds to the wireless host(in Hexadecimal Representation)?
   - 7.3. Which MAC address in this frame corresponds to the access point ?
   - 7.4. Which MAC address in this frame corresponds to the first-hop router?
   - 7.5. What is the IP address of the wireless host sending this TCP segment?
   - 7.6. What is the destination IP address?
   - 7.7. Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

8. Find the 802.11 frame containing the SYNACK segment for this TCP session.
   8.1. What are three MAC address fields in the 802.11 frame?
   8.2. Which MAC address in this frame corresponds to the host?
   8.3. Which MAC address in this frame corresponds to the access point?
   8.4. Which MAC address in this frame corresponds to the first-hop router?
   8.5. 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: refer text book in reference list if you are unsure of how to answer this question, or the corresponding part of the previous question).

3. Association/Disassociation

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) 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).

NOTE: 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.

Exercise 3

9. What two actions are taken (i.e., frames are sent) by the host in the trace just after *t=49*, to end the association with the *30 Munroe St* AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action).

   Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

10. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the *linksys_ses_24086* AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around *t=49?* .
11. Does the host want the authentication to require a key or be open?
12. Do you see a reply AUTHENTICATION from the *linksys_ses_24086* AP in the trace?
13. Now let's consider what happens as the host gives up trying to associate with the *linksys_ses_24086* AP and now tries to associate with the *30 Munroe St* AP. Look for AUTHENTICATION frames sent from the host to and AP and vice versa. At what times is there an AUTHENTICATION frame from the host

to 30 *Munroe St.* AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to be associated with an AP.
    14.1. At what time is there an ASSOCIATE REQUEST from host to the *30 Munroe St* AP?
    14.2. 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 == IntelCor_d1:b6:4f" to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)
15. To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.
    15.1. What transmission rates is the host willing to use?
    15.2. What transmission rates is the AP? willing to use?

4. Other Frame types

Exercise 4

16. Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.
    16.1. What are the sender, receiver and BSS ID MAC addresses in these frames?
    16.2. What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited at the end of this lab sheet).

Submission

Submit a report renamed as **E16XXX_Lab07.pdf** (XXX is your E Number).

The report should include,

- Answers for the lab exercise questions 1 - 16 with the necessary explanations, screenshots

REFERENCES

- "A Technical Tutorial on the 802.11Protocol," by Pablo Brenner (Breezecom Communications) - http://www.sss-mag.com/pdf/802_11tut.pdf
- "Understanding 802.11 Frame Types," by Jim Geier - http://www.wi-fiplanet.com/tutorials/article.php/1447501
- "ANSI/IEEE Std 802.11, 1999 Edition (R2003)," - http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf.