Lab 7 – 802.11

IT 520-A – Enterprise Infrastructure & Networks Due Date: 11/05/18 (Handed in at the beginning of class)

Instructions:

Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file Wireshark_802_11.pcap. This trace was collected using AirPcap and Wireshark running on a computer in a 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. 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 http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12.
- At t=32.82, the host makes an HTTP request to http://www.cs.umass.edu, 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.

Once you have downloaded the trace, and unzip it, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the Wireshark 802 11.pcap trace file. The resulting display should look just like Figure 1.

Time 1 0.000000 2 0.005101 3 0.005474 4 0.187919 5 0.188100	Source Cisco-Li f7:1d:51 b6:78:8c:c1:ae:	Destination	Protocol		Expression.
1 0.000000 2 0.062101 3 0.085474 4 0.187919	Cisco-Li_f7:1d:51			Lengt Info	and the second
2 0.062101 3 0.085474 4 0.187919		Broadcast	802.11	183 Beacon frame, SN=2854, FN=0, Flags=C, BI=180, SSID=30 Munroe St	
4 0.187919		c 65:a8:d5:b2:c1		1624 892.11 Block Ack Reg, Flagsmop.PT.	
	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN-2855, FN-0, FlagsC, BI-100, SSID-30 Munroe St	
5 0.188100	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2856, FN=0, Flags=C, BI=100, SSID=30 Munroe St	
	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51		54 QoS Null function (No data), SN-1482, FN-0, FlagsTC	
6 0.188201 7 0.188935	IntelCor_d1:b6:4f	IntelCor_d1:b6		38 Acknowledgement, Flags=C 54 005 Null function (Ne data), SM-1488, FN-9, Flags=PTC	
8 0,189934	IntelCor_d1:D6:41	IntelCor d1:b6		34 QOS MALI TUNCTION (NO GATA), SM-146S, FN-0, FLAGSPIC. 38 Acknowledgement, Flacs	
9 0.298284	Cisco-Li_f7:1d:51	Broadcast	802.11	30 MCKNOWLEGGROWNTH, Flags	
10 0.294432	Linksys6 67:22:94	Broadcast	802.11	99 Beacon frame, 581-3072, FN-0, Flags, BI-02, 5510-11/557\277\275\001\004\357\277[Malformed Packet]	
11 0.393174	Cisco-Li f7:1d:51	Broadcast	802.11	183 Beacon frame, SN-2858, FN-0, FlagsC, BI-100, SSID-30 Munroe St	
12 0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a		90 Association Response, SN=3073, FN=0, Flags=	
13 0.495032	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN-2859, FN-0, FlagsC, BI-100, SSID-30 Munroe St	
14 0.499197	Linksys6_67:22:94	Broadcast	802.11	90 Beacon frame, SN=3074, FN=0, Flags=, BI=100, SSID=linksys12	
15 0.597382	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN-2860, FN-0, FlagsC, BI-100, SSID-30 Munroe St	
16 0.601687 17 0.699847	Linksys6_67:22:94	Broadcast Broadcast	802.11 802.11	90 Beacon frame, SN=3075, FN=0, Flags=C, BI=100, SSID=linksys12	
18 0.802226	Cisco-Li_f7:1d:51 Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SH-2861, FH-0, FlagrC, BI-100, SSID-30 Murror St 183 Beacon frame, SH-2862, FH-0, FlagrC, BI-100, SSID-30 Murror St	
19 0.984619	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SM-2863, FM-9, Flags	
20 1.007015	Cisco-Li f7:1d:51	Broadcast	802.11	183 Beacon frame, SN+2864, FN+0, Flags*C, 81=100, SSID=30 Phonroe St	
21 1.010949	LinksysG 67:22:94	Broadcast	802.11	98 Beacon frame, SN-3079, FN-0, Flags, BI-100, SSID-linksys12	
22 1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2865, FN=0, Flags=C, BI=100, SSID=30 Munroe St	
23 1.113691	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame, SN-3000, FN-0, Flags, BI-100, SSID-,\357\277\275nksys	
24 1.211843	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2866, FN=0, Flags=C, BI=100, SSID=30 Munroe St	
25 1.211992 26 1.212889	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51 IntelCor_d1:b6		54 QOS Mull function (No data), SN-1484, FN-0, FlagsTC 38 Acknowledgement, FlagsC	
26 1.212009	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f		38 ACKNOWLEGGREENT, Flags=	
28 1.212282	C13C0-C1_17.10.31	Cisco-Li f7:10		38 Acknowledgement, FlagsC	
2.11 radio info EE 802.11 Beaco EE 802.11 wireld	frame, flags:	c			

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

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. When answering a question below, you should hand in a screenshot of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. 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.

Questions:

- 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 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*?