Computer Network 1

LAB 7

Wireshark lab 802.11 WIFI

Student Name: Alexandre Rousseau

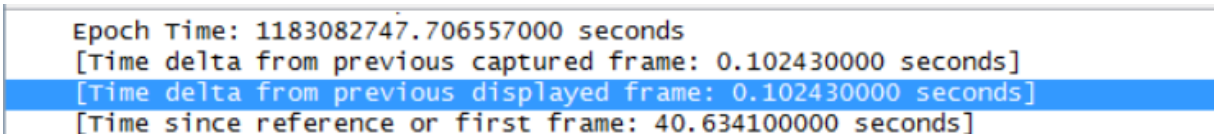
Student ID: 1952001

1) What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

The two access points that are issuing most of the beacon frames have an SSID of “30 Munroe St” and “linsys_SES_24086”.

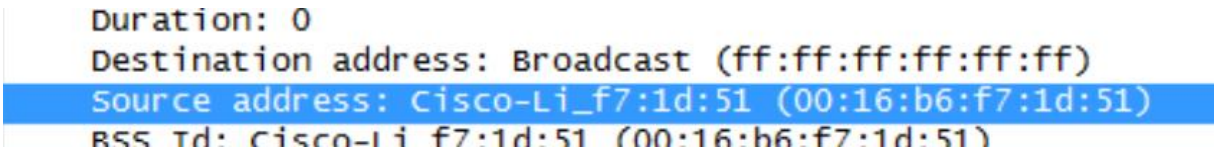
2) What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point?

The beacon interval for both access points in reported in the Beacon Interval of the 802.11 wireless LAN Management frame as 0.1024 seconds.



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.

The source MAC address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51.



4) What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St?

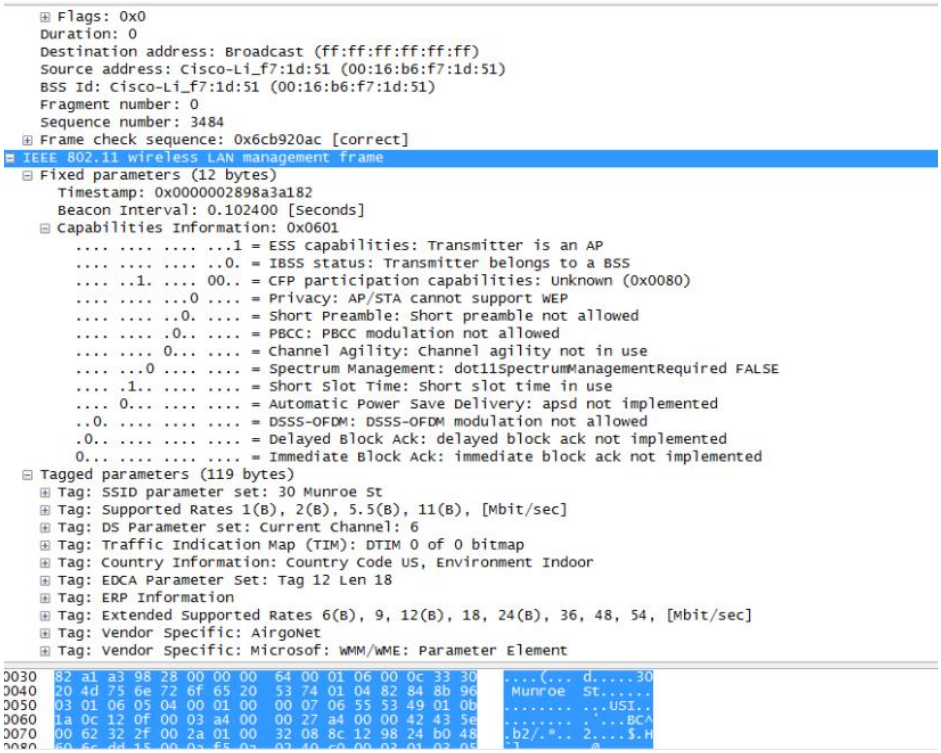
The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff.

5) What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?

The MAC BSS ID address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51 which also the source address.

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?

The support rates are 1.0, 2.0, 5.5, 11.0 Mbps. The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 Mbps.



7) 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? Explain.

The TCP SYN is sent at t = 24.811093 seconds into the trace. The MAC address for the host sending the TCP SYN is 00:13:02:d1:b6:4f. The MAC address for the destination, which the first hop router to which the host is connected, is 00:16:b6:f4:eb:a8. The MAC address for the BSS is 00:16:b6:f7:1d:51. The IP address of the host sending the TCP SYN is 192.168.1.109. Note that this is a NATed address. The destination address is 128.199.245.12. This corresponds to the server gaia.cs.umass.edu. It is important to understand that the destination MAC address of the frame containing the SYN, is different from the destination IP address of the IP packet contained within this frame. Make sure you understand this distinction! (If you're a bit hazy on this, re-read pages 468 and 469 in the 4th edition of the text).

8) 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?

The TCP SYNACK is received at t = 24.827751 seconds into the trace. The MAC address for the sender of the 802.11 frame containing the TCP SYNACK segment is 00:16:b6:f4:eb:a8, which is the 1st hop router to which the host is attached . The MAC address for the destination, which the host itself, is 91:2a:b0:49:b6:4f. (Curiously, this is different from the MAC address of the host used in the frame that sends the TCP SYN. The host wireless interface is behaving as if it has two interface addresses - interesting!). The MAC address for the BSS is 00:16:b6:f7:1d:51. The IP address of the server sending the TCP SYNACK is 128.199.245.12 (gaia.cs.umass.edu) The destination address is 192.168.1.109 (our wireless PC).

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

At t = 49.583615 a DHCP release is sent by the host to the DHCP server (whose IP address is 192.168.1.1) in the network that the host is leaving. At t = 49.609617, the host sends a DEAUTHENTICATION frame (Frametype = 00 [Management], subframe type = 12[Deauthentication]). One might have expected to see a DISASSOCIATION request to have been sent.

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?

The first AUTHENTICATION from the host to the AP is at t = 49.638857.

11) Does the host want the authentication to require a key or be open?

To determine if a system is open or uses a key, one must look for the value on the Authentication Algorithm Number field, per Section 7.3.1.1. Composed of 2 octets, it is either 0 for open system, or 1 for shared key authentication. This is contained in the 1740th packet instance, a t=49.638857, and further located in the IEEE 802.11 wireless LAN management frame. It indicates an Authentication Algorithm field of "Open System (0)", and Authentication SEQ of 0x0001, as well as a Status Code of Successful, or 0x0000. This is a shared key system.

12) Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?

No.

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 AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply?

AUTHENTICATION from Host to 30 Munroe (AP): t = 63.168087

Reply AUTHENTICATION from AP to Host: t = 63.169071

14) 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 what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent?

Associate Request: t = 63.169910

Associate Reply: t = 63.192191

15) What transmission rates is the host willing to use? The AP?

In the ASSOCIATION REQUEST frame, the supported rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps. The same rates are advertised in the ASSOCIATION RESPONSE.

16) What is the sender, receiver, and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?

Probe Request: Sender = InterCor_d1:b6:4f, Receiver = Broadcast (ff:ff:ff:ff:ff:ff) & BSS Id = Broadcast (ff:ff:ff:ff:ff:ff)

Probe Response: Sender = Cisco-Li_f7:1d:51, Receiver =InterCor_d1:b6:4f & BSS Id = Cisco-Li_f7:1d:51.

Probe requests & responses are generated for active scanning. Unlike passive scanning, where an STA listens to each channel for a set duration, once a probe response is received and processed, authorization can be commenced as directly after ACK'ing a probe request.