# Lab 7-G WIFI

Name – Sati, Ankit Date – 9/30/2021

Section - 001

Total in points (Maximum 100 points)–

Professors Comments –

Affirmation of Independent Effort – Ankit Sati

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

**Answer**

An SSID is a one or two word identifiers of the access point. In this case, Cisco-Li’s SSID is 30 Munroe St,

and LinksysG\_67:22:94’s SSID is linksys12.

Table

Description automatically generated

1. 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).

**Answer**

**0.1024 seconds.**



1. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 6.13 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 ?

**Answer - 00:16:b6:f7:1d:51** - Background pattern

Description automatically generated with low confidence

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

**Answer :- it is a probing broadcast, it is addressed to ff:ff:ff:ff:ff:ff.**

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

**Answer :- The BSS Id for 30 Munroe is Cisco-LI-f7:1d:51 (00:16:b6:f7:1d:51) which is also the source address.**

Graphical user interface, application, table

Description automatically generated

1. 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?

**Answer** - This data is found within the IEEE 802.11 wireless LAN management frame, within the Tagged parameters subfield. The four supported rates are 1(B), 2(B), 5.5(B) AND 11(B). The 8 Extended Unsupported Rates are 6(B), 9, 12(B), 18, 24(B), 36, 48 and 54. All these rates are measured in Mbit/sec.

Graphical user interface, text, application, email

Description automatically generated

1. 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.

**Answer -**

The frame that contains this is No. 488, at time t = 24.850314. The three MAC addresses are the Destination Address of 00:13:02:d1:b6:4f, as well as the Source Address & BSS Id, both having a value of 00:16:b6:f7:1d:51. The host is 00:13:02:d1:b6:4f. The access point is 00:16:b6:f7:1d:51, which is also the first hop router.

1. 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 5.19 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).

**Answer**

D. Association/Disassociation

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 Figure 6.13 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>.

1. 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?

Answer

To end the association with 30 Munroe (at t = 49.609617) a Deauthentication is sent out, and only after that is ACK’ed, does the probe request get sent out.

Each frame consists of the following basic components:  
a) A MAC header, which comprises frame control, duration, address, and sequence control information;  
b) A variable length frame body, which contains information specific to the frame type;  
c) A frame check sequence (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

I saw a MAC header, specifically, frame control = 0x00c0(Normal), duration = 44, address: = (destination addr = Cisco-Li\_f7:1d:51 & source addr = InterCor\_d1:b6:4f), and sequence control information(Fragment number = 0, Sequence number = 1605).

I saw a FCS: 0x9c8b4a3b [correct].

Graphical user interface, text, application, email

Description automatically generated

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?



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

**Answer** 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, and 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.

Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?

**Answer :- NO**

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? (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.)

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

Reply AUTHENTICATION from AP to Host: t = 63.169071

An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated 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? (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.)

**Answer** :- Associate Request: t = 63.169910

Associate Reply: t = 63.192191

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

Answer

Host transmission rates in Mbit/sec: 1(B), 2(B), 5.5(B), 11(B), 6(B), 9(B), 12(B), & 18(B). Extended rates are also offered at 24(B), 36, 48 and 54.

AP transmission rates (30 Munroe or f7:1d:51) in Mbit/sec: 1(B), 2(B), 5.5(B), 11(B). Extended rates are also offered at 6(B), 9, 12(B), 18, 24(B), 36, 48 and 54.

E. Other Frame types

Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.