CS315: Lab Assignment 12

B Siddharth Prabhu
200010003@iitdh.ac.in

28 March 2023

1 Answers to Part 1: Beacon Frames

Firstly, we use the filter `wlan.fc.type_subtype == 0x8` in the given packet trace `Wireshark_802_11.pcap`. We then sort it by Source Name for simplicity of judging which the most common issuing access points are. The observed trace is as shown in Figure (1):

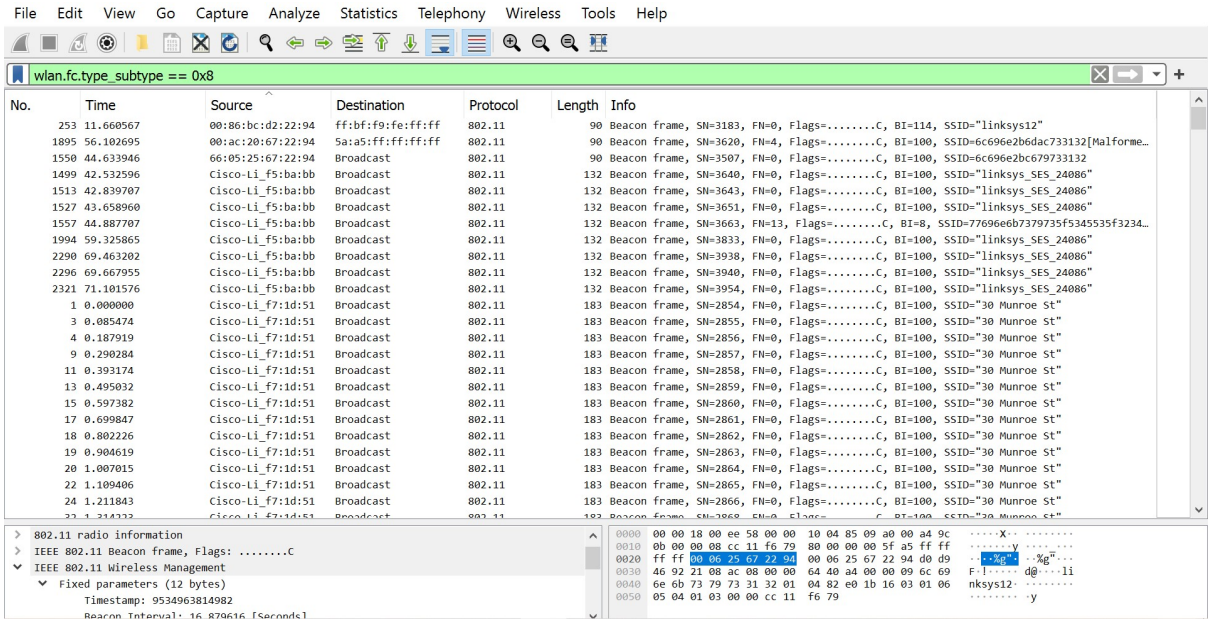

Figure 1: Observed Packet Trace

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

The SSIDs of the two access points that are issuing most of the beacon frames in this trace are `30 Munroe St` and `linksys12`. It can be verified in Figures (2) and (3).

(2) What are the intervals of time between the transmissions of the beacon frames from the linksys_SES_24086 access point? From the 30 Munroe St. access point?

The beacon interval time for transmissions of the beacon frames from the mentioned access points are:

- `0.102400 seconds` (for linksys_SES_24086) (visible in Figure (4).
- `0.102400 seconds` (for 30 Munroe St.) (visible in Figure (2).

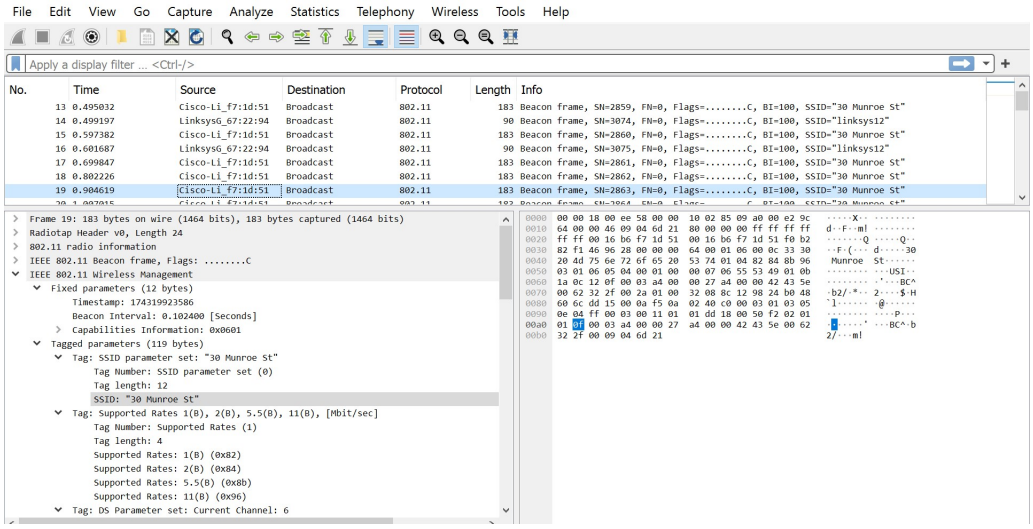

Figure 2: 30 Munroe St

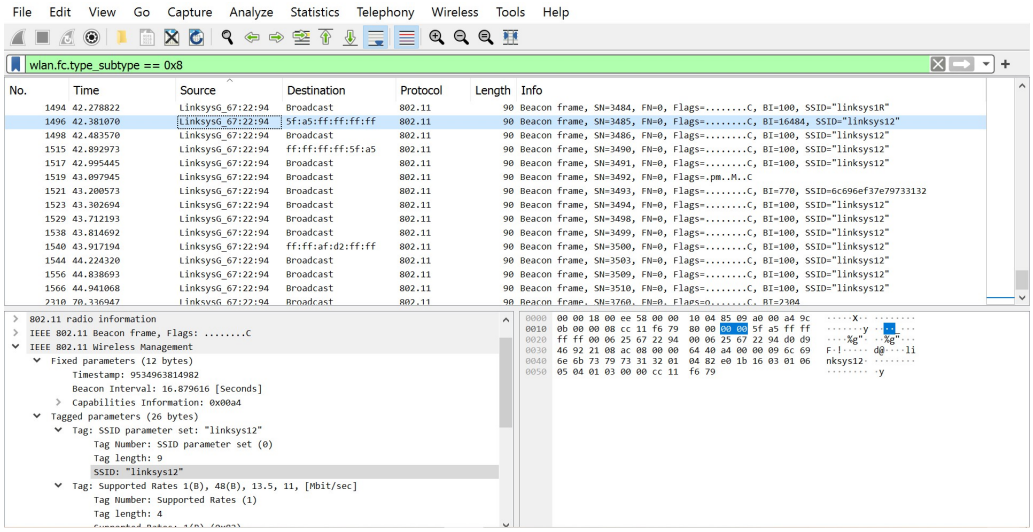

Figure 3: linksys12

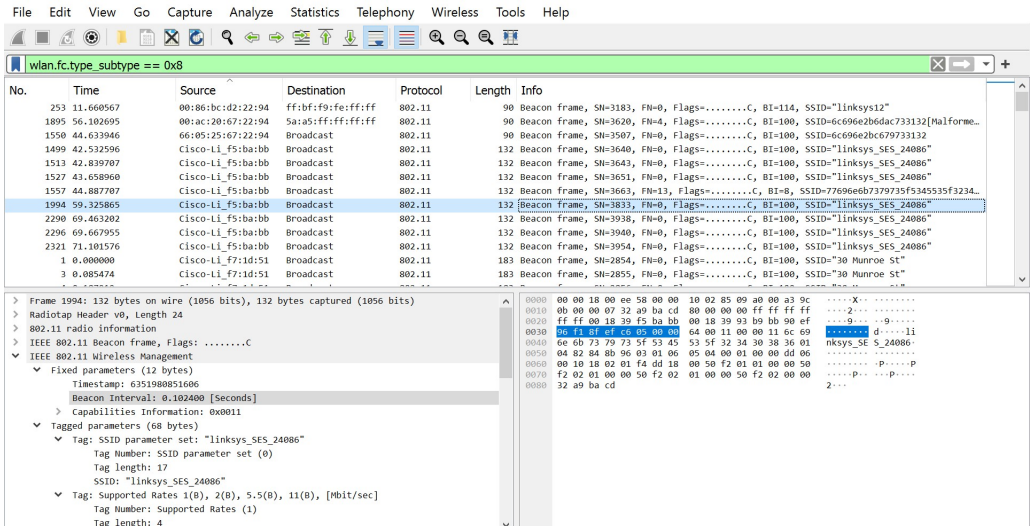

Figure 4: linksys_SES_24086

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

The source MAC address on the beacon frame from 30 Munroe St is `00:16:b6:f7:1d:51` , as visible in Figure (5).

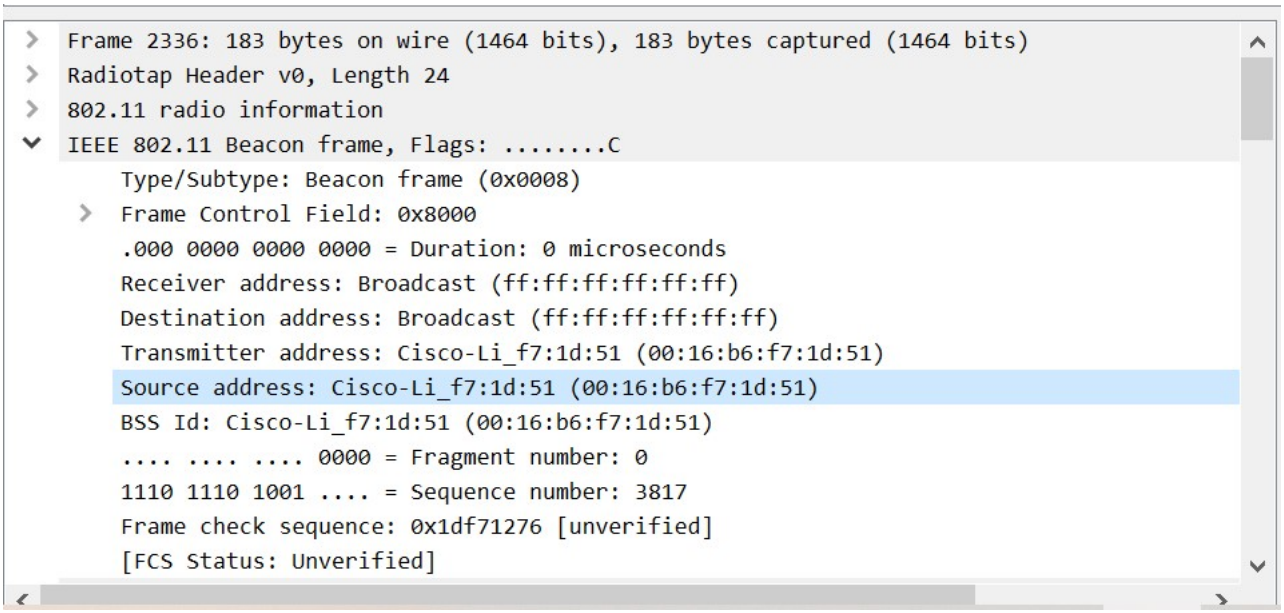

Figure 5: Packet Details for beacon frame from 30 Munroe St

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

The source MAC address on the beacon frame from 30 Munroe St is `ff:ff:ff:ff:ff:ff` , as visible in Figure (5). This is the address for network broadcast.

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

The MAC BSS id on the beacon frame from 30 Munroe St is `00:16:b6:f7:1d:51` , as visible in Figure (5).

(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 four data rates and eight additional extended supported rates supported by the 30 Munroe St access point, as advertised by the beacon frames, are as follows:

- Data Rates: 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
- Extended Support Rates: 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

The same can be observed in Figure (6).

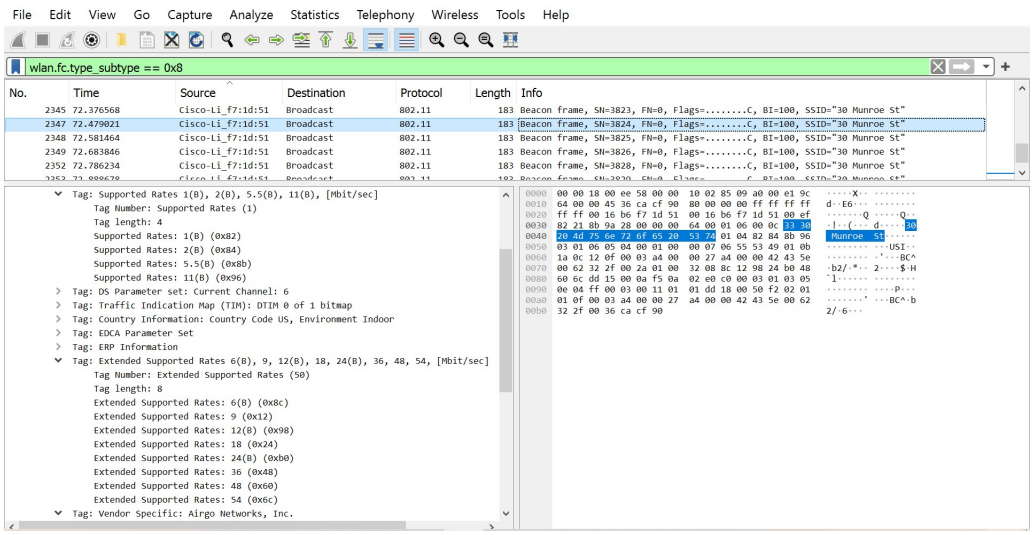

Figure 6: Observed Rates in Packet Detail Window

2 Answers to Part 2: Data Transfer

In this part, we locate the 802.11 frame containing the SYN TCP segment for this first TCP session, and then the 802.11 frame containing the SYNACK segment for this TCP session. The observed packets are in Figures (7) and (9) respectively.

(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? 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.

- There are three UNIQUE MAC address fields in the 802.11 frame. They are:
  - `00:16:b6:f7:1d:51` , which is the Receiver address and BSS id.
  - `00:13:02:d1:b6:4f` , which is the Transmitter address, Source address, and STA Address.
  - `00:16:b6:f4:eb:a8` , which is the Destination address.
- In this frame, the MAC address in this frame corresponding to the wireless host is the source address, `00:13:02:d1:b6:4f` .
- In this frame, the MAC address in this frame corresponding to the access point is the BSS id, `00:16:b6:f7:1d:51` . (BSS ID stands for Basic Service Set Identifier, and it is the MAC physical address of the access point or wireless router that is used to connect to the WiFi.)
- In this frame, the MAC address in this frame corresponding to the first-hop router is the destination address, `00:16:b6:f4:eb:a8` .
- The IP address of the wireless host sending the TCP segment is `192.168.1.109` .
- The destination IP address is `128.119.245.12` . (IP Header info in Figure (8)).
- The destination IP address above corresponds to the **server on which alice.txt is located**. This would probably be a server at `gaia.cs.umass.edu`. This is because the IP header contains IP addresses of the server and client, while the data-link layer frames work on a link-level basis, and contain the MAC addresses of the interfaces on the two ends of a link.

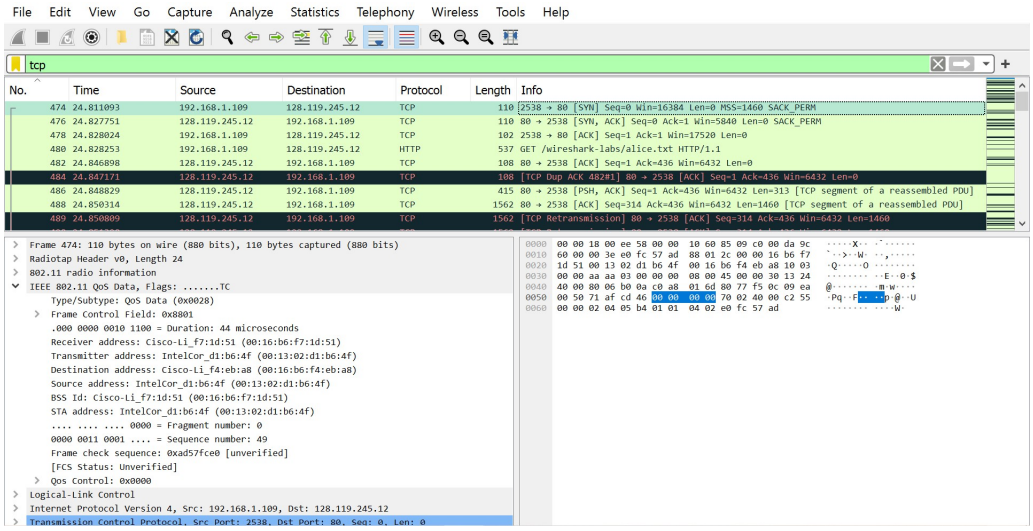

Figure 7: TCP SYN segment

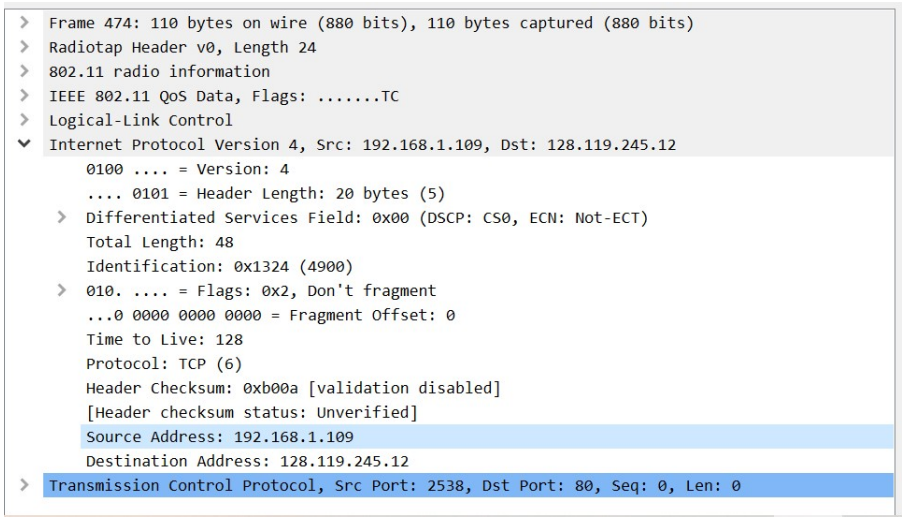

Figure 8: IP header of TCP SYN segment

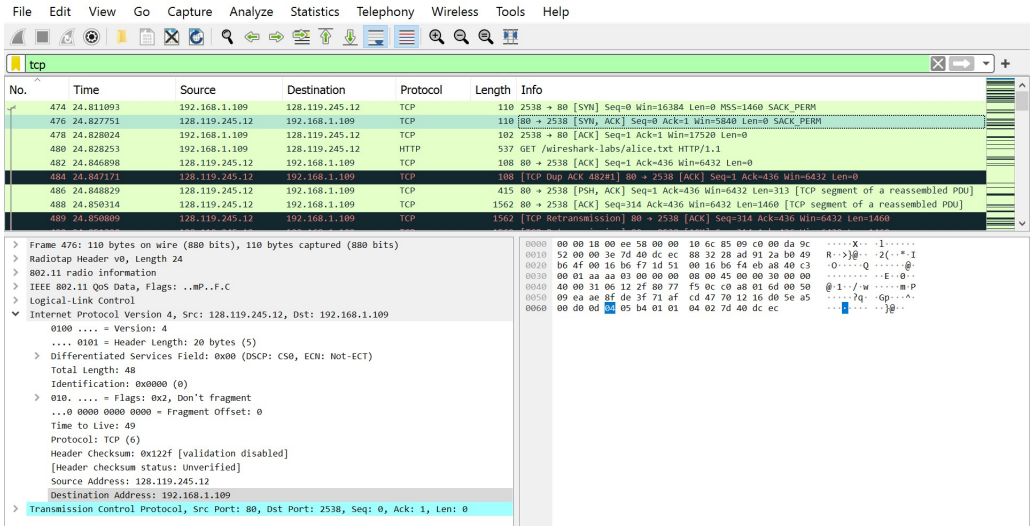

Figure 9: TCP SYNACK segment

(2) 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?

- There are three UNIQUE MAC address fields in the 802.11 frame. They are:
  - `00:16:b6:f7:1d:51` , which is the Transmitter address and BSS id.
  - `91:2a:b0:49:b6:4f` , which is the Receiver address, Destination address, and STA Address.
  - `00:16:b6:f4:eb:a8` , which is the Source address.
- In this frame, the MAC address in this frame corresponding to the wireless host is the destination address, `91:2a:b0:49:b6:4f` .
- In this frame, the MAC address in this frame corresponding to the access point is the BSS id, `00:16:b6:f7:1d:51` . (BSS ID stands for Basic Service Set Identifier, and it is the MAC physical address of the access point or wireless router that is used to connect to the WiFi.)
- In this frame, the MAC address in this frame corresponding to the first-hop router is the source address, `00:16:b6:f4:eb:a8` .
- The sender MAC address in this frame does **NOT** correspond to the device that sent the TCP segment encapsulated within this datagram. This is due to the same reasons mentioned in the last part of the previous question; the IP Header has information of the sender and receiver of the datagram, while the MAC address in a given Frame header deals with the nodes at the ends of a particular link.

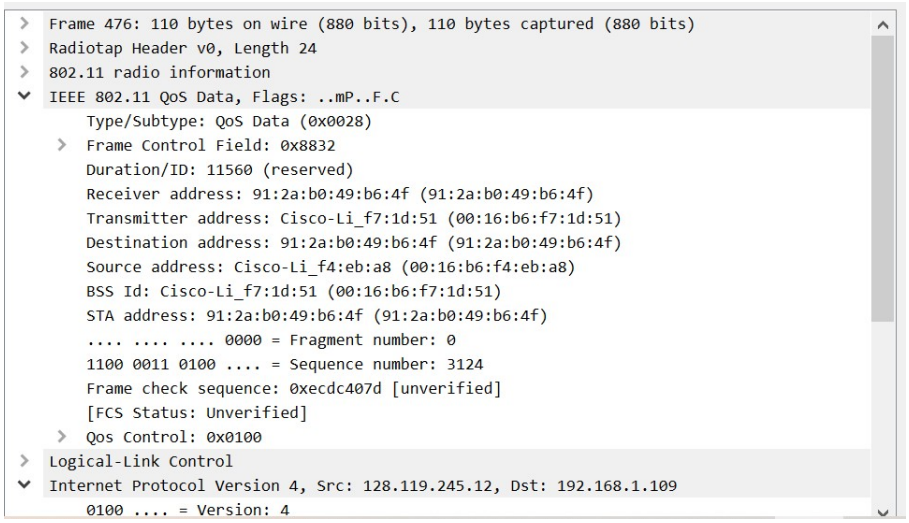

Figure 10: MAC addresses in TCP SYNACK segment

(The next part begins on the next page.)

3 Answers to Part 3: Association/Disassociation

In this part, we take a look at hosts associating/de-associating with access points.

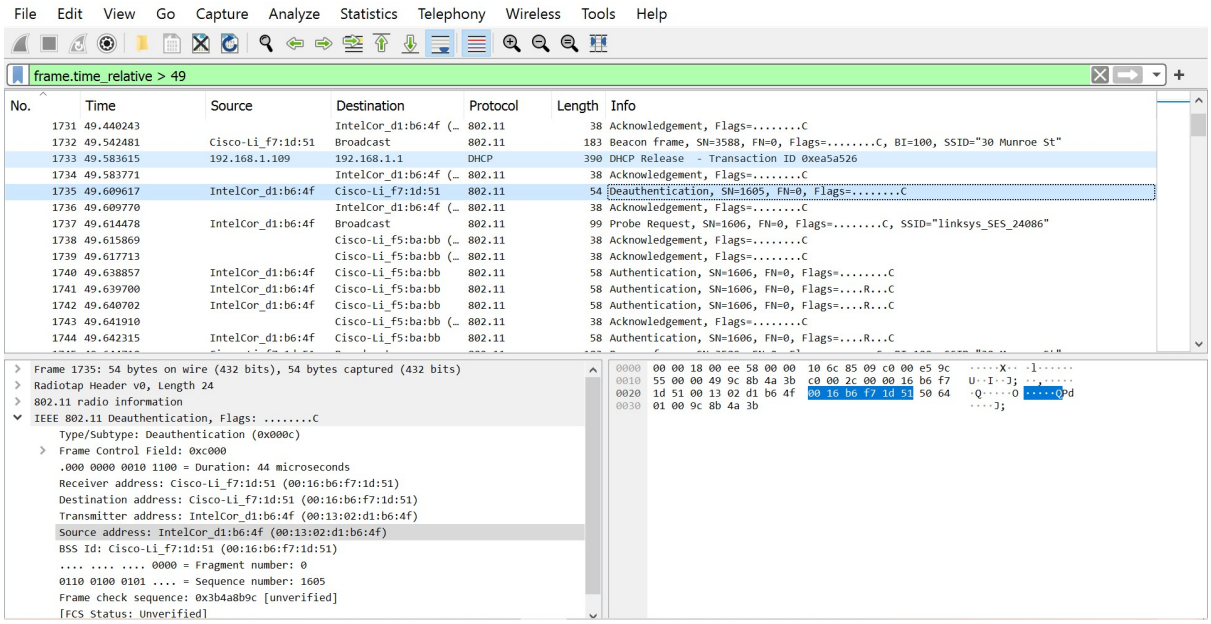

Figure 11: Actions taken to end association with 30 Munroe St

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

After $t = 49$, the following actions are taken to end the association with the 30 Munroe St:

- At $t = 49.583615$, DHCP Release is done. The host is releasing its IP address back to the DHCP server, and is exiting the network.
- At $t = 49.609617$, Deauthentication is done, to terminate a Wi-Fi connection.

One would expect a DISASSOCIATION request, but that is not observed here.

(2) Examine the trace file and look for AUTHENTICATION 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?

As seen in Figure (12), there are `6` AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086.
Note that the first AUTHENTICATION frame sent out successfully was observed to be at time $t = 49.649705$ (We don't consider the ones before this since they seem to have been unsuccessful, and required retransmissions, as observed in the flags.)

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

Based on Figure (13), the host wants the authentication to be `Open` .

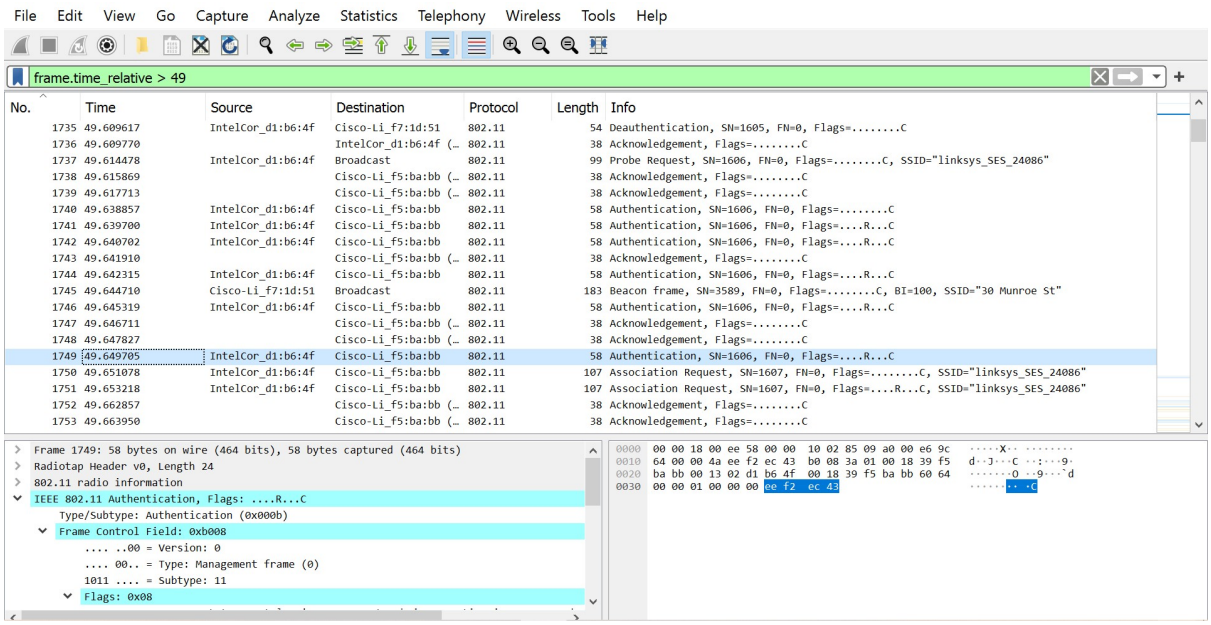

Figure 12: AUTHENTICATION messages

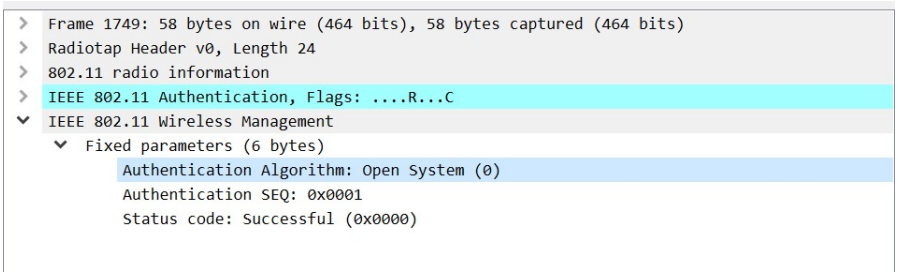

Figure 13: AUTHENTICATION algorithm

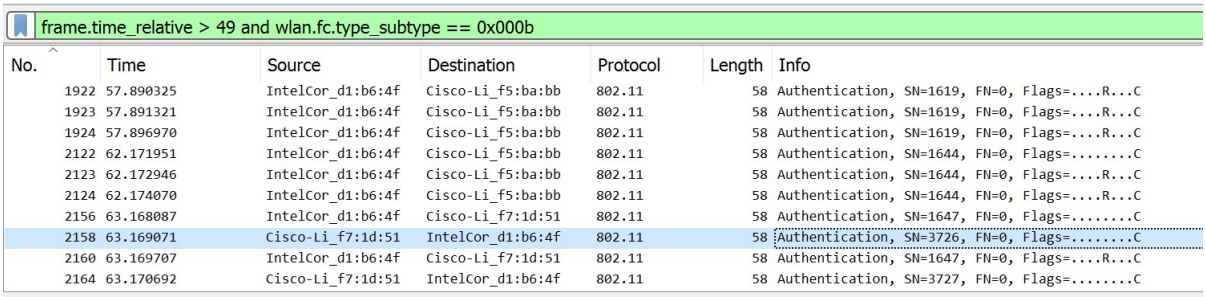

Figure 14: AUTHENTICATION messages

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

There is `no` reply AUTHENTICATION. There seems to be some kind of response in Frames 2158 and 2164, though these are at around $t = 63$, which is too long after the AUTHENTICATION messages that we have observed are sent in the previous question. Hence, we may not conclude that these are the required replies from the linksys host. (These late replies may help us in later questions, perhaps!)

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 an AP and vice versa. (Also, 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.)

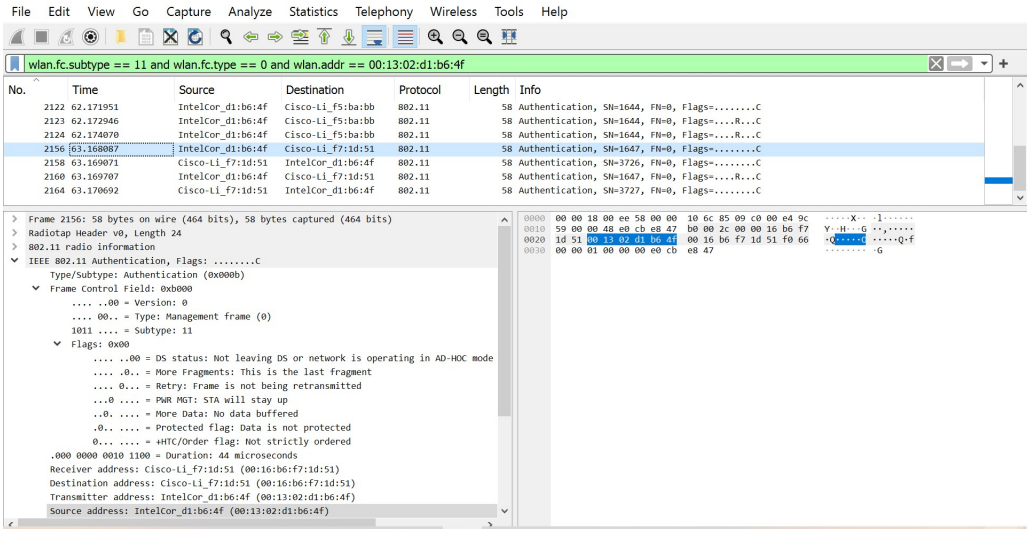

Figure 15: AUTHENTICATION frames

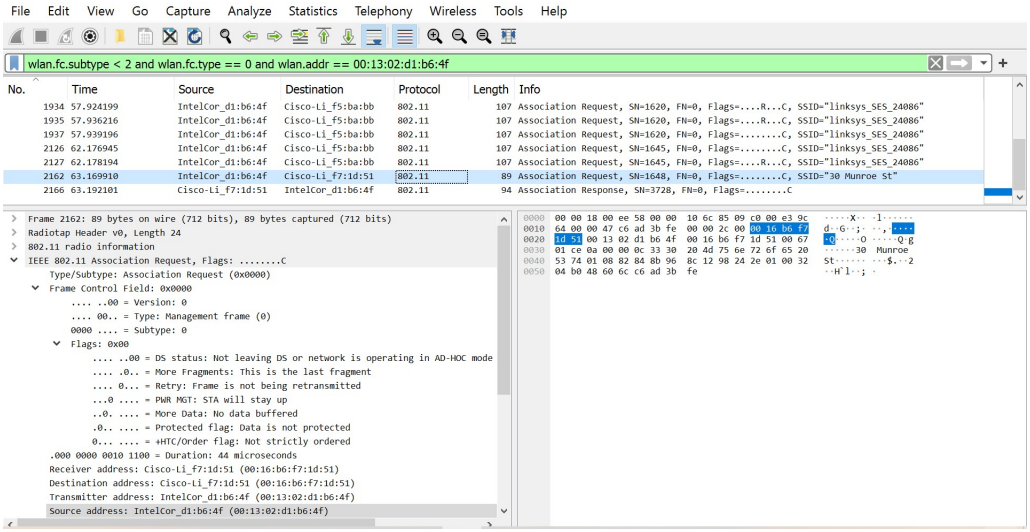

Figure 16: ASSOCIATE REQUEST frames

(5) At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP (access point), and when is there a reply AUTHENTICATION sent from that AP to the host in reply?

Using `wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == 00:13:02:d1:b6:4f` filter, as shown in Figure (15), we observe that:

- AUTHENTICATION frame is sent from the host to the 30 Munroe St AP at time $t = 63.168087$.
- Reply AUTHENTICATION is sent from that AP to the host in reply at time $t = 63.169071$.

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

Using `wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == 00:13:02:d1:b6:4f` filter, as shown in Figure (16), we observe that:

- An ASSOCIATION REQUEST (i.e., the ASSOCIATE REQUEST) is sent from host to the 30 Munroe St AP at time $t = 63.169910$.
- An ASSOCIATION RESPONSE (i.e., the ASSOCIATE REPLY) is sent from that AP to the host at time $t = 63.192101$.

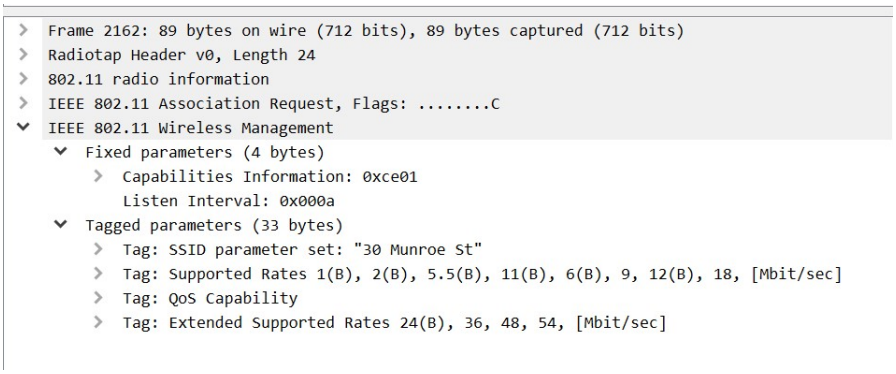

Figure 17: Rates advertised in request

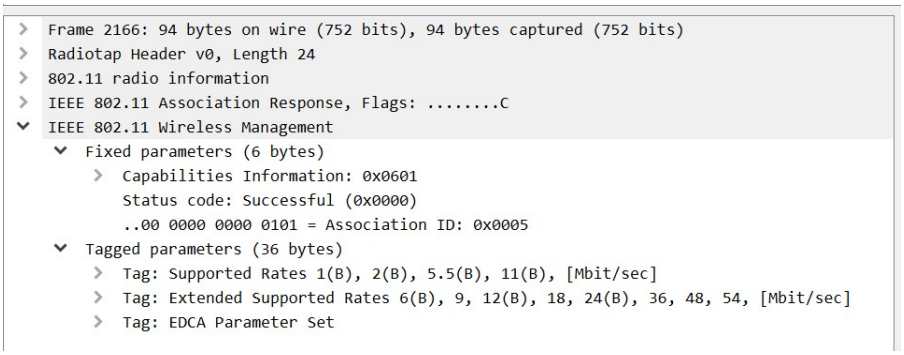

Figure 18: Rates advertised in response

(7) 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.

The host is willing to use the rates that are listed in Figure (17), which are:

- Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
- Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

The exact same rates are observed in the response, as seen in Figure (18), the only difference being that 6, 9, 12, and 18 are in the 'extended supported rates' field of the AP's request message.

4 Answers to Part 4: Other Frame Types

(1) Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?

Consider the first PROBE REQUEST at time $t = 2.297613$, as seen in Figure (19), The required info is as follows:

- Sender MAC address: `00:12:f0:1f:57:13` , which is the source address.
- Receiver MAC address: `ff:ff:ff:ff:ff:ff` , which is the Ethernet broadcast address.
- BSS ID MAC address: `ff:ff:ff:ff:ff:ff` , which is the Ethernet broadcast address.

Consider the PROBE RESPONSE that appears to be a reply to the above request, at time $t = 2.300697$, as seen in Figure (20), The required info is as follows:

- Sender MAC address: `00:16:b6:f7:1d:51` , which is the source address.
- Receiver MAC address: `00:12:f0:1f:57:13` , which is as seen in the Receiver Address field of Figure (20).
- BSS ID MAC address: `00:16:b6:f7:1d:51` , which is the as seen in the BSS ID field of Figure (20).

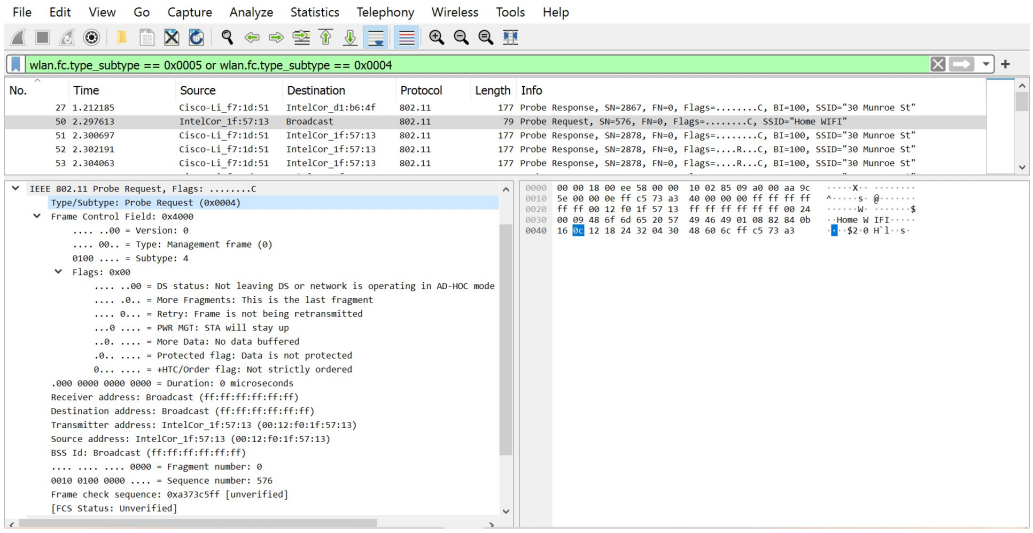

Figure 19: PROBE REQUEST

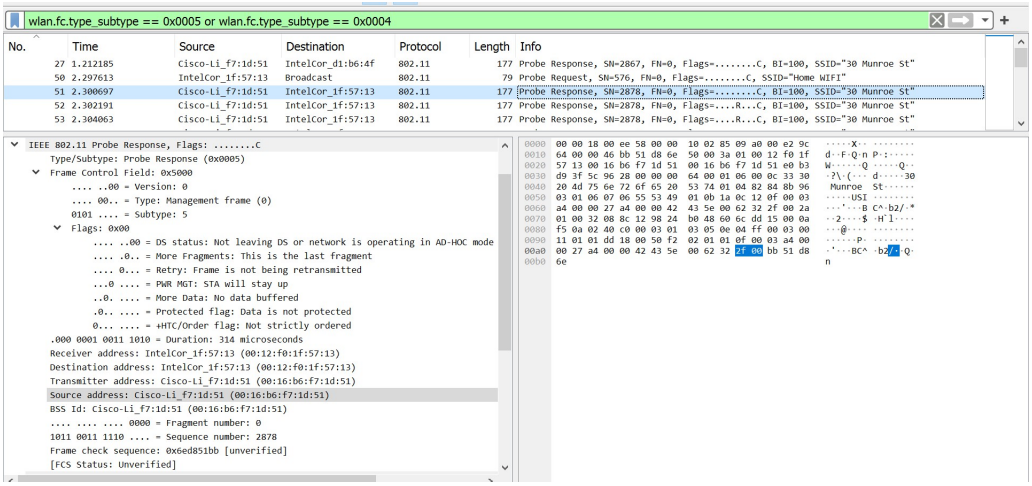

Figure 20: PROBE RESPONSE