Computer Networking Lab

Assignment No 05.

Date: 15/02/2023

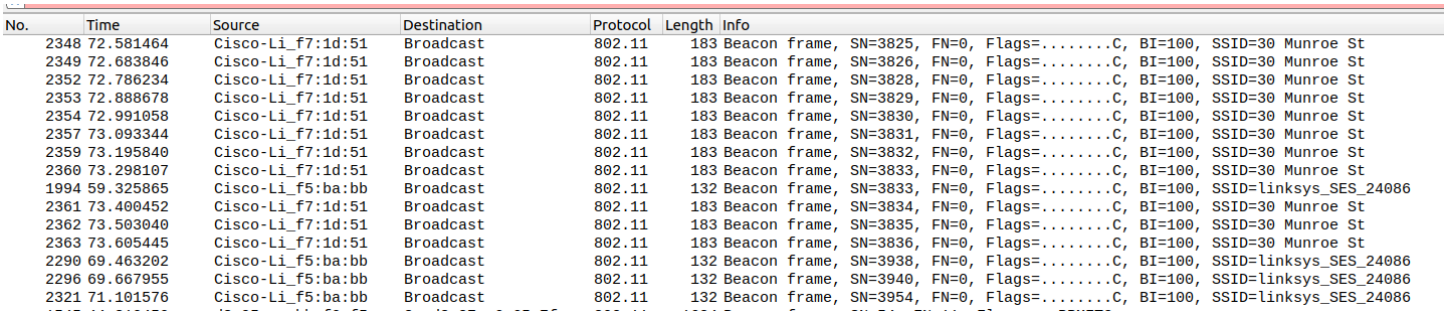
Name: Harshavardhan Anil Bamane PRN: 22510112

Wireshark Lab: 802.11

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

Ans: The SSIDs of the two access points that are issuing most of the beacon frames in this trace are 30 Munroe St and linsys_SES_24086.

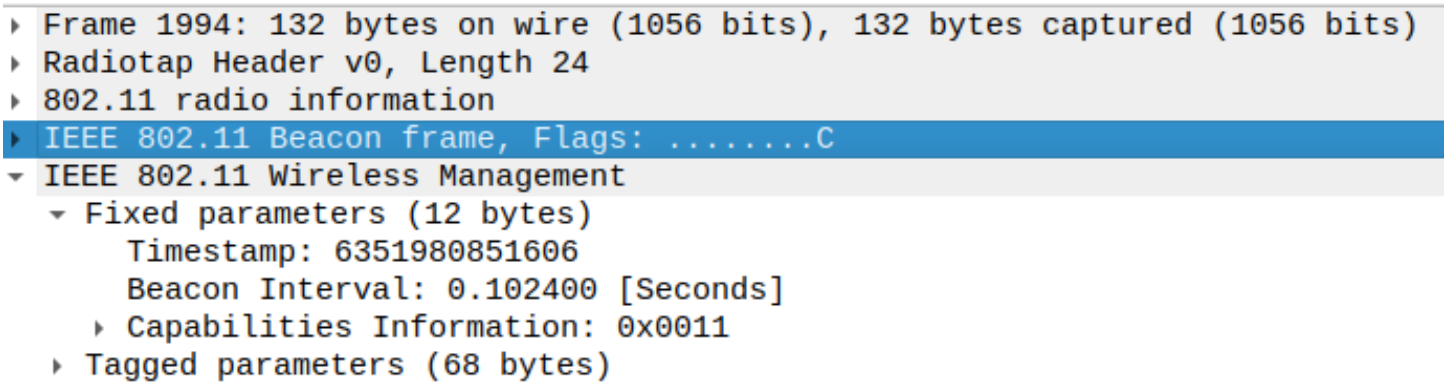
The two access points that are issuing most of the beacon frames have an SSID of 30 Munroe St and linsys_SES_24086.



No.	Time	Source	Destination	Protocol	Length	Info
2348	72.581464	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3825, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2349	72.683846	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3826, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2352	72.786234	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3828, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2353	72.888678	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3829, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2354	72.991058	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3830, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2357	73.093344	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3831, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2359	73.195840	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3832, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2360	73.298107	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3833, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1994	59.325865	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3833, FN=0, Flags=........C, BI=100, SSID=linksys_SES_24086
2361	73.400452	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3834, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2362	73.503040	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3835, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2363	73.605445	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3836, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2290	69.463202	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3938, FN=0, Flags=........C, BI=100, SSID=linksys_SES_24086
2296	69.667955	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3940, FN=0, Flags=........C, BI=100, SSID=linksys_SES_24086
2321	71.101576	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3954, FN=0, Flags=........C, BI=100, SSID=linksys_SES_24086

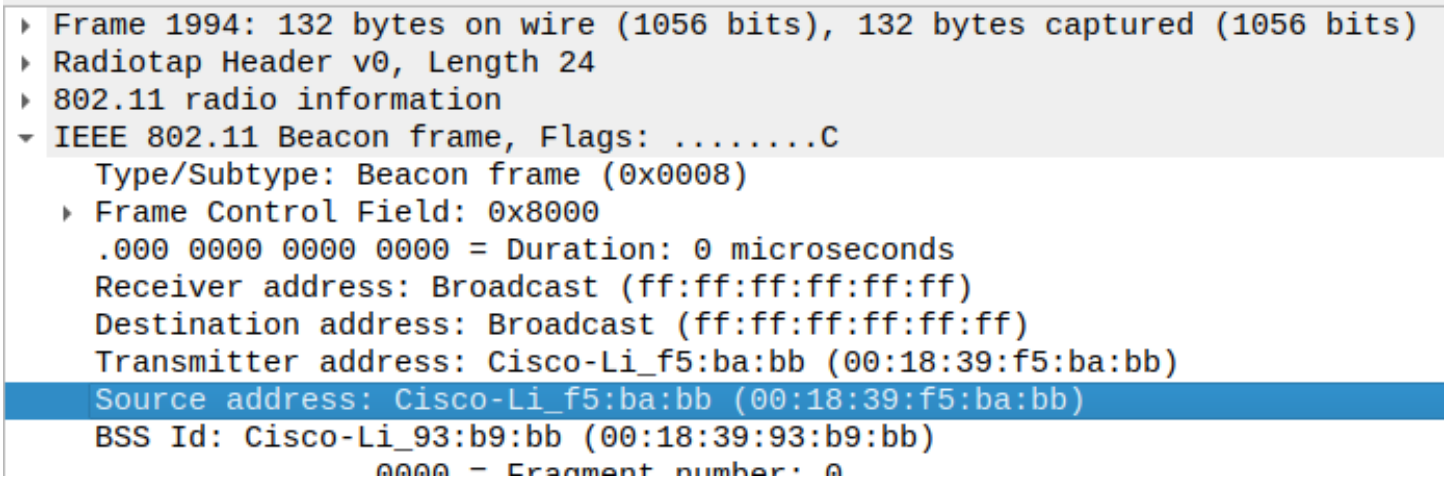
2. What are the intervals of time between the transmission of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).

Ans: intervals of time:0.1024 sec.



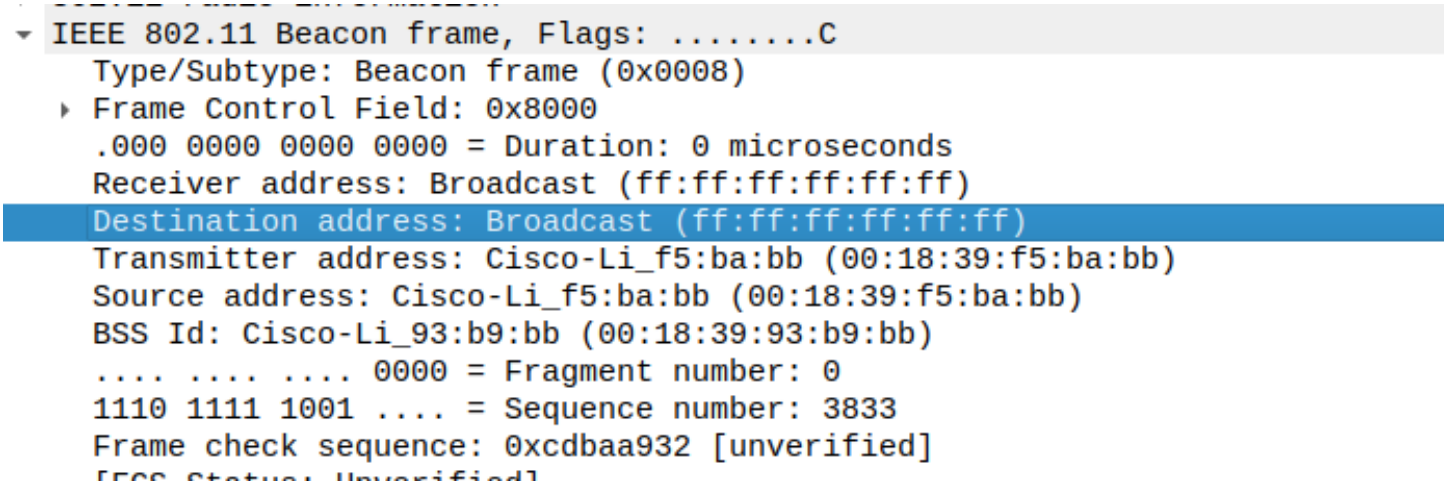
3. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 6.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).

Ans: The source MAC address on the 30 Munroe St, beacon frame is 00:18:39:f5:ba:bb.



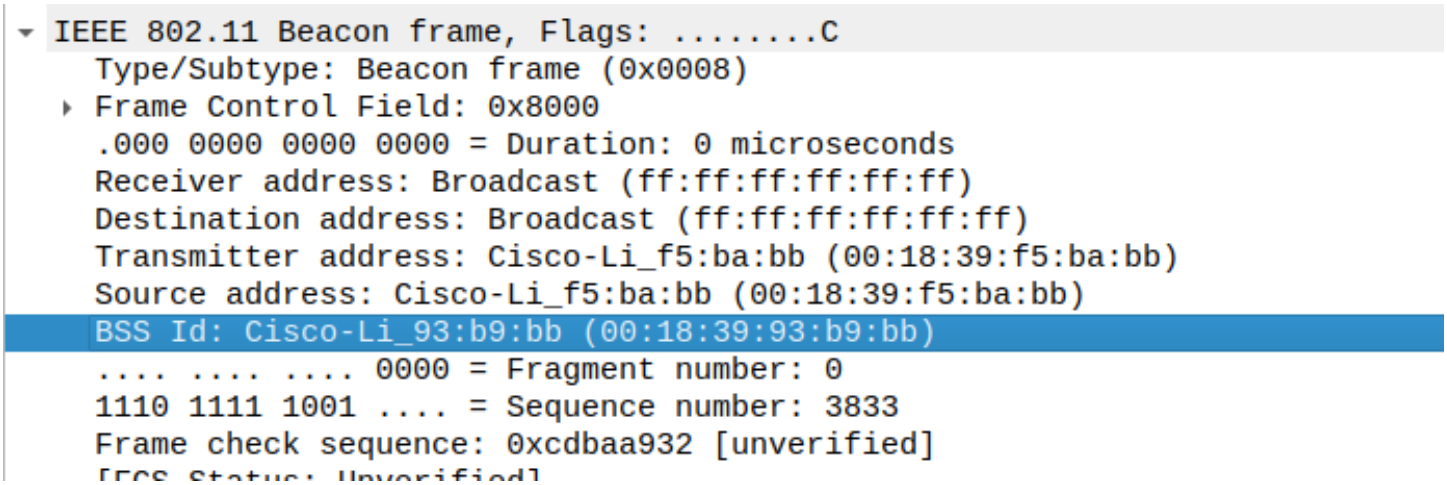
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??

Ans: The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff, i.e., the Ethernet broadcast address.



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

Ans: The MAC BSS ID address on the beacon frame from 30 Munroe St is 00:18:39:93:b9:bb.



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?

Ans:

```
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
  Tagged parameters (68 bytes)
    Tag: SSID parameter set: linksys_SES_24086
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
        Tag Number: Supported Rates (1)
        Tag length: 4
        Supported Rates: 1(B) (0x82)
        Supported Rates: 2(B) (0x84)
        Supported Rates: 5.5(B) (0x8b)
        Supported Rates: 11(B) (0x96)
    Tag: DS Parameter set: Current Channel: 6
    Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
```

```
Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 8
    Extended Supported Rates: 6(B) (0x8c)
    Extended Supported Rates: 9 (0x12)
    Extended Supported Rates: 12(B) (0x98)
    Extended Supported Rates: 18 (0x24)
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 36 (0x48)
    Extended Supported Rates: 48 (0x60)
    Extended Supported Rates: 54 (0x6c)
```

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). At what time is the TCP SYN sent? 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.

Ans:

The time TCP SYN sent is 24.811093 sec.

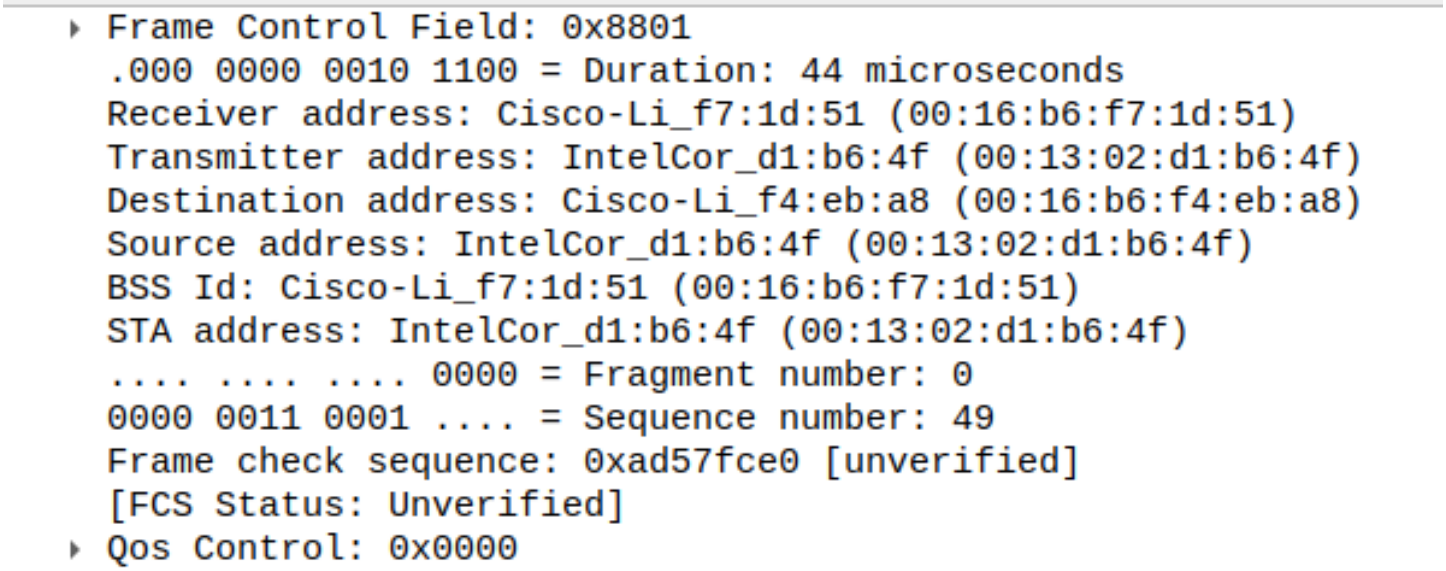
The MAC address for the host sending that transmitter's address to the TCP SYN is 00:13:02:d1:b6:4f.

The MAC address for the destination, which is 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.

The destination address is 00:16:b6:f4:eb:a8.



8. Find the 802.11 frame containing the SYNACK segment for this TCP session. At what time is the TCP SYNACK received? What are three MAC address fields in the 802.11 frame containing the SYNACK? 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?

Ans:

The time the TCP SYNACK received is 24.827751 seconds.

The MAC address for the sender of the 802.11 frame containing the TCP SYNACK segment is 00:16:b6:f4:eb:a8.

The MAC address for the destination, which is the host itself, is 91:2a:b0:49:b6:4f.

The MAC address for the Transmitter is 00:16:b6:f7:1d:51.

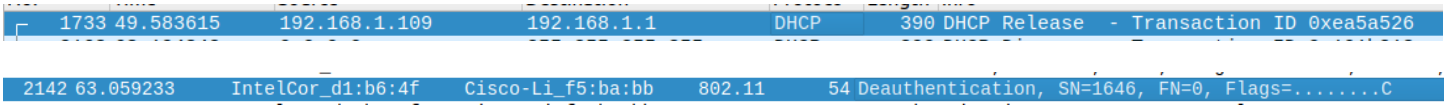
```
▾ IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  ▾ Frame Control Field: 0x8832
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ▸ Flags: 0x32
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
```

Association/Disassociation:

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, and at what times are these frames sent? (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?

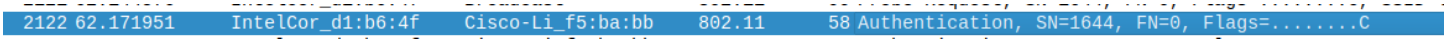
Ans: At t = 49.583615 a DHCP release is sent by the host to the DHCP server.

At t = 49.609617, the host sends a de-authentication frame



10. 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?

Ans: 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?

Ans: Yes.

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

Ans: No.

1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1612, FN=0, Flags=........C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=........C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=........C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58 Authentication, SN=1647, FN=0, Flags=........C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58 Authentication, SN=1647, FN=0, Flags=....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3726, FN=0, Flags=........C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, Flags=........C

13. Now let's consider what happens as the host gives up (sometime after t = 63.0) 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?

Ans: At t = 63.168087 there is a AUTHENTICATION frame sent.

At t = 63.169071, there is an AUTHENTICATION from sent in the reverse direction.

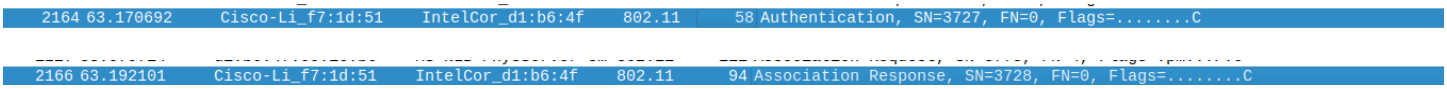
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58 Authentication, SN=1647, FN=0, Flags=........C

14. Let's continue on with the association between the wireless host and the 30 Munroe St AP that happens after t = 63.0. An ASSOCIATE 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 the host to 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent?

Ans: At t = 63.169910 there is a ASSOCIATE REQUEST frame sent.

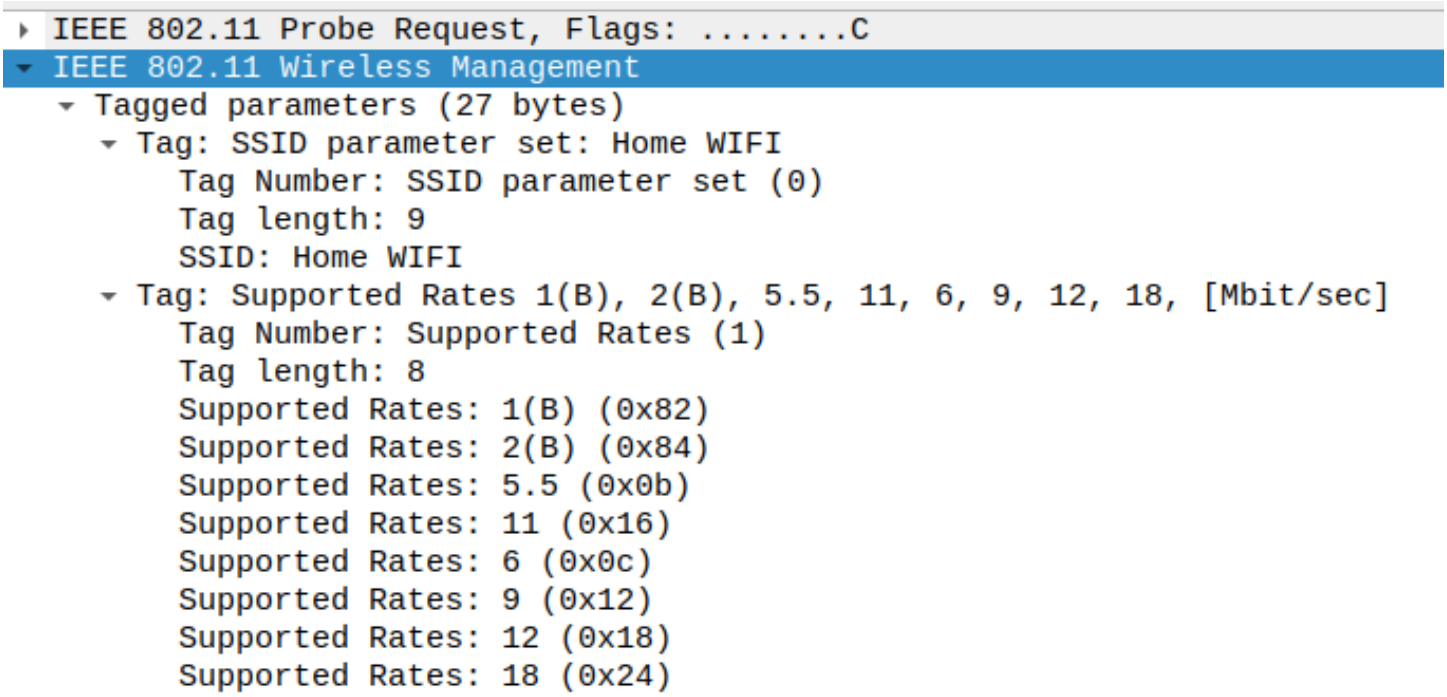
At t = 63.192101, there is an ASSOCIATE RESPONSE sent in the reverse direction.

2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89 Association Request, SN=1648, FN=0, Flags=........C, SSID=30 Munroe St



15. 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.

Ans:



16. Consider the first PROBE REQUEST and the soonest subsequent PROBE RESPONSE PAIR occurs after t = 2.0 seconds in the trace. When are these frames sent and what are the sender, receiver and BSS ID MAC addresses for these frames?

Ans: At t = 2.297613 there is a PROBE REQUEST sent with source. At t = 2.300697, there is a PROBE RESPONSE sent.