USC EE450 Fall 2020

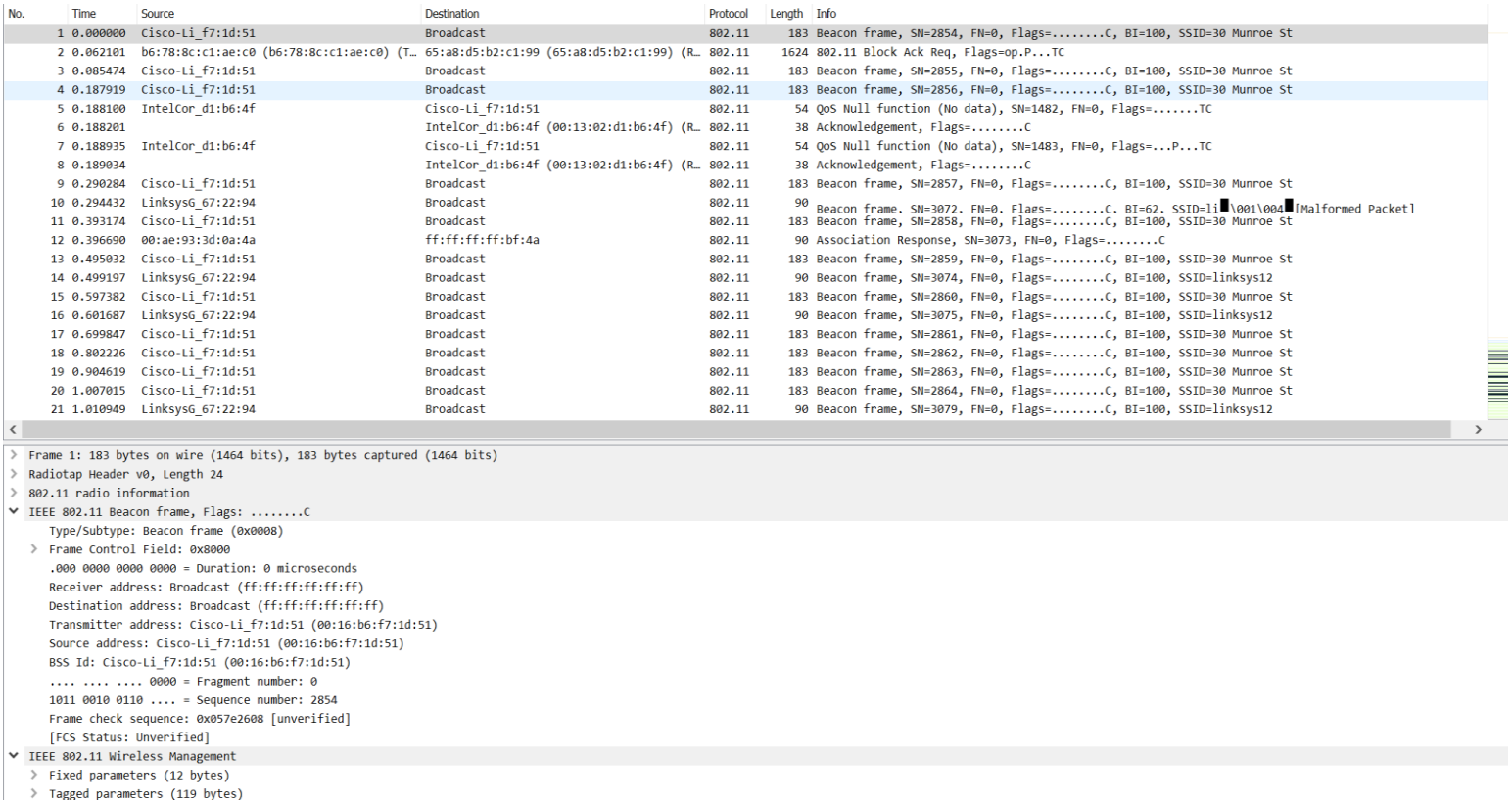
Lab #3 Report: WLANs

Zeyu Wang

Session 2

1. Abstract

In this lab, I examined and analyzed the 802.11 wireless network protocol using the given trace file, *Wireshark_802_11.pcap*. I demonstrated the details of the "IEEE 802.11" frame and its subfields such as SSIDs, Beacon frames, Time intervals, Basic Service Set ids, etc. Furthermore, I also illustrated the data transfer frames over an 802.11 with the access point, these specific frames, including TCP SYN/SYNACK, ASSOCIATE REQUEST/REPLY, and AUTHENTICATION between the host and the AP. Finally, I figured out the use of the PROBE REQUEST/RESPONSE frames, which are often used to scan the area for WLAN networks' availability.



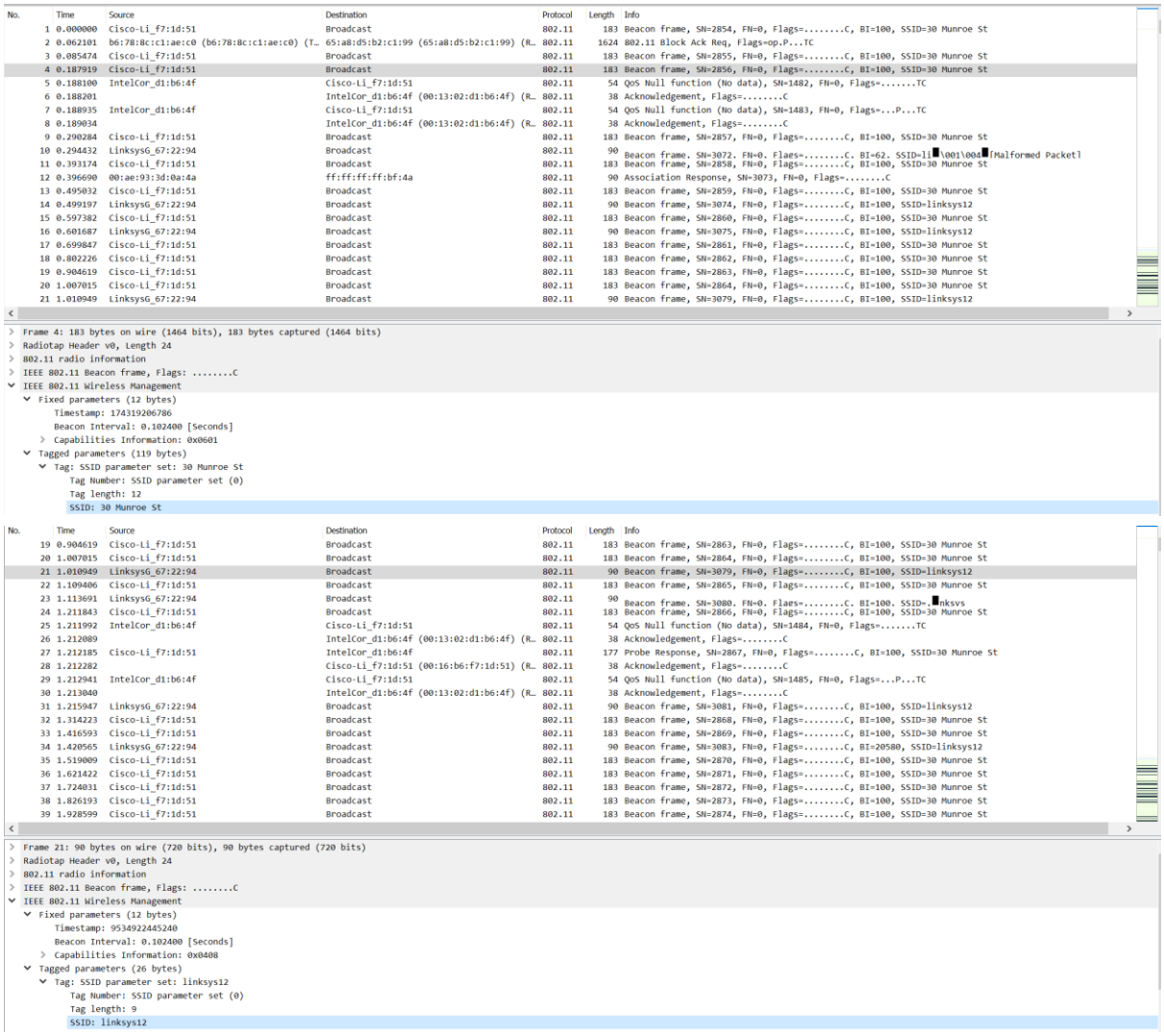
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2	0.062101	b6:78:8c:c1:ae:c0 (b6:78:8c:c1:ae:c0) (T…	65:a8:d5:b2:c1:99 (65:a8:d5:b2:c1:99) (R…	802.11	1624	802.11 Block Ack Req, Flags=op.P...TC
3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
4	0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
5	0.188100	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.......TC
6	0.188201		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (R…	802.11	38	Acknowledgement, Flags=........C
7	0.188935	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
8	0.189034		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (R…	802.11	38	Acknowledgement, Flags=........C
9	0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=li\001\004[Malformed Packet]
11	0.393174	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=........C
13	0.495032	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID=linksys12
15	0.597382	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID=linksys12
17	0.699847	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
18	0.802226	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
19	0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
20	1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
21	1.010949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID=linksys12

```
> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    1011 0010 0110 .... = Sequence number: 2854
    Frame check sequence: 0x057e2608 [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  > Tagged parameters (119 bytes)
```

2. Answers to questions in lab

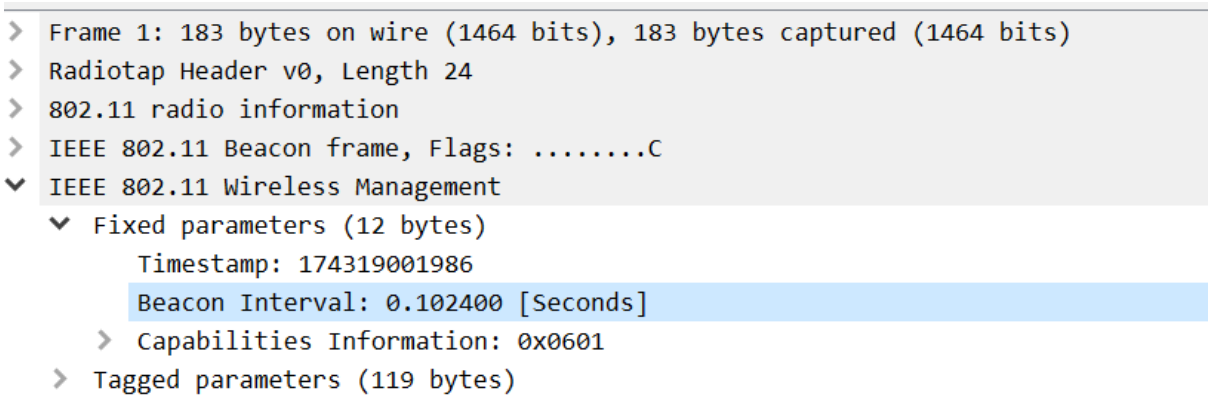
1) What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

   The two access points are 30 Munroe St and Linksys_SES_24086.



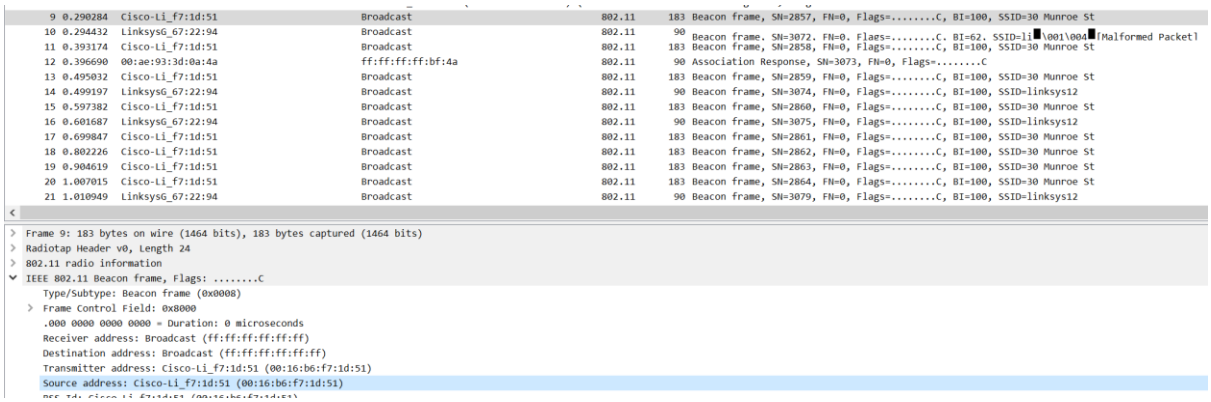
2) What are the intervals of time between the transmissions of the beacon frames the *linksys_ses_24086* access point? From the *30 Munroe St*. access point? (Hint: this interval of time is contained in the beacon frame itself)

The intervals of time between the transmissions of the beacon frames is 0.0124 seconds.



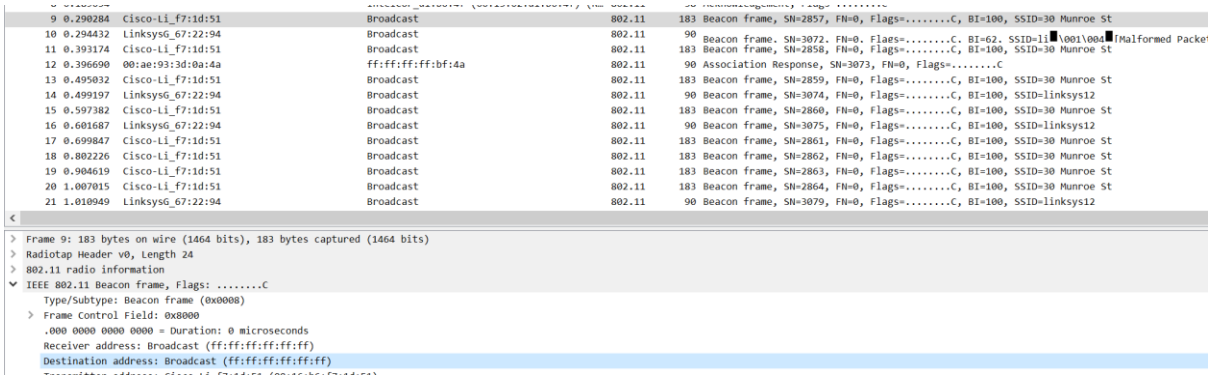
3) What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).

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



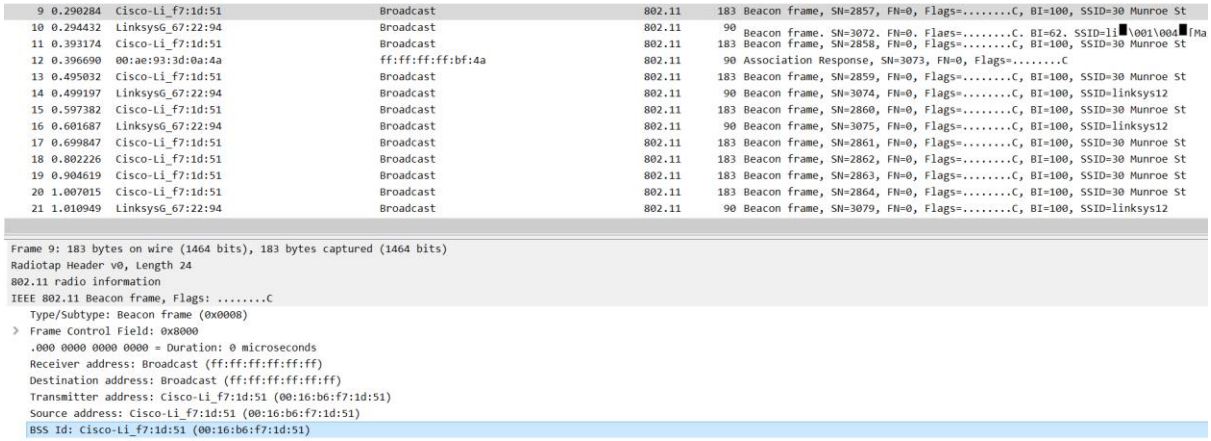
4) What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*?

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



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."

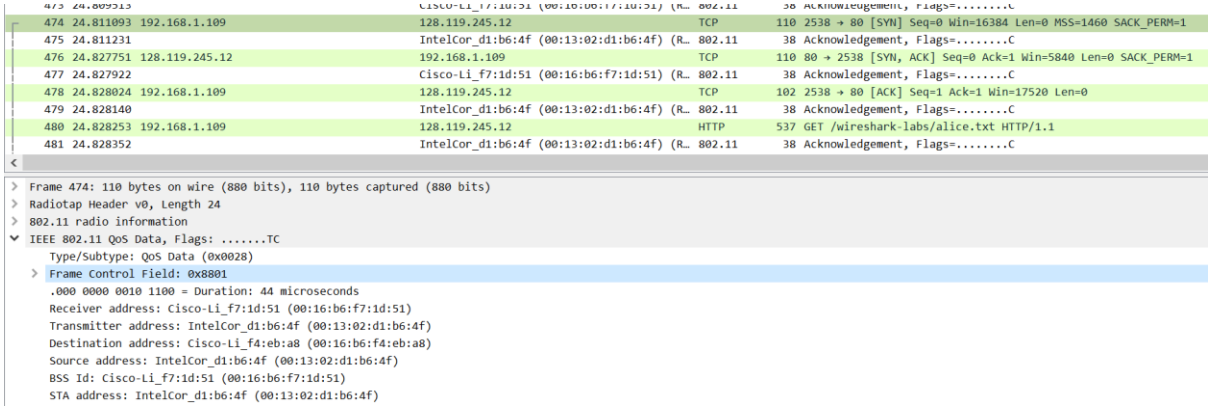
The support rates are 1, 2, 5.5, 11 Mbps. The extended rates are 6, 9, 12, 18, 24, 36, 48, 53 Mbps

```
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: 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). 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 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 IP address is 128.119.245.12. Yes, this destination IP address correspond to the host server gaia.cs.umass.edu because IP address of gaia.cs.umass.edu is 128.119.245.12 and the TCP port number is 80.



```
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x1324 (4900)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xb00a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.109
    Destination: 128.119.245.12
```

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? (Hint: review Figure 6.19 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).

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 first hop router to which the host is attached. The MAC address for the destination is 91:2a:b0:49:b6:4f, which is the host itself. The MAC address for BSS is 00:16:b6:f7:1d:51. The IP address of the server sending the TCP SYNACK is 128.119.245.12. The destination address is 192.168.1.109.

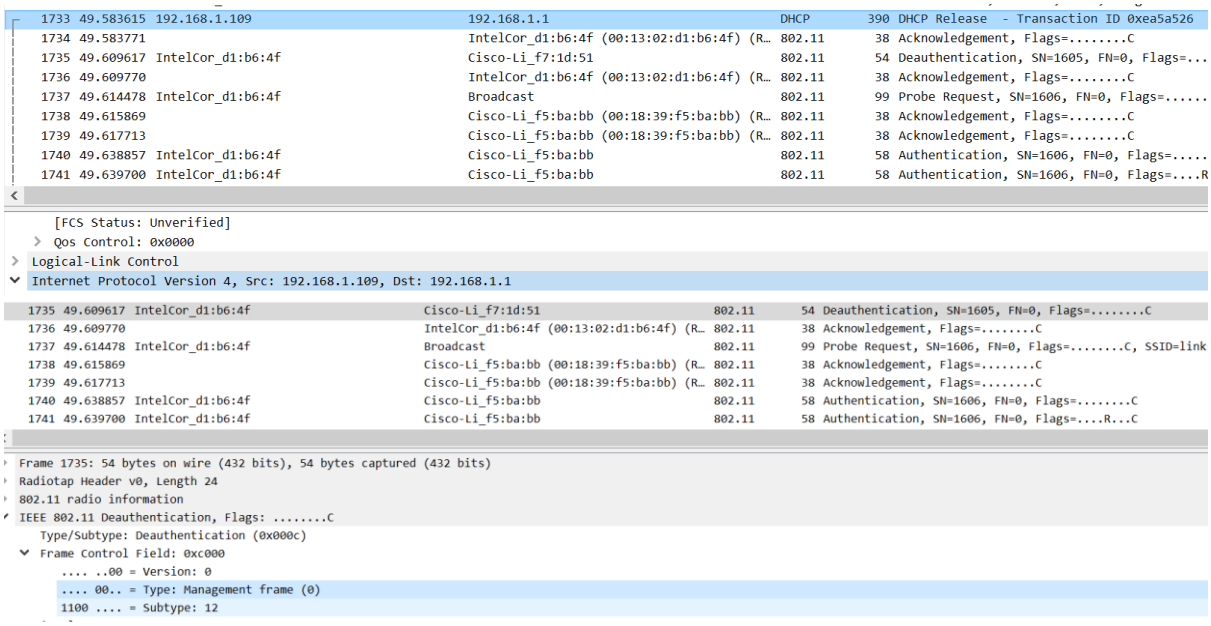
```
476 24.827751 128.119.245.12                192.168.1.109                TCP       110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477 24.827922                               Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) (R… 802.11     38 Acknowledgement, Flags=........C
478 24.828024 192.168.1.109                 128.119.245.12               TCP       102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
479 24.828140                               IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (R… 802.11     38 Acknowledgement, Flags=........C
480 24.828253 192.168.1.109                 128.119.245.12               HTTP      537 GET /wireshark-labs/alice.txt HTTP/1.1
481 24.828352                               IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (R… 802.11     38 Acknowledgement, Flags=........C

Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8832
    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)
```

```
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x0000 (0)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 49
    Protocol: TCP (6)
    Header checksum: 0x122f [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.109
```

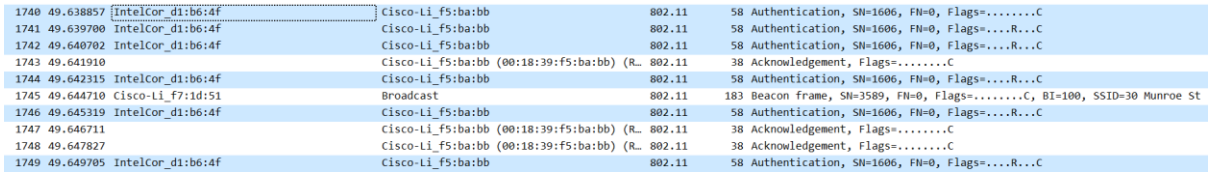
9) What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the *30 Munroe St* AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

DHCP release is sent by host to the DHCP server at t=49.583165, whose IP address is 192.168.1.1 in the network that the host is leaving. The host sends a DEAUTHENTICATION frame at t=49.609617, the Frametype = 00 [Management], the subframe type = 12 [Deauthentication]. I might have expected to see a DISASSOCIATION request to be sent, but don't see here.



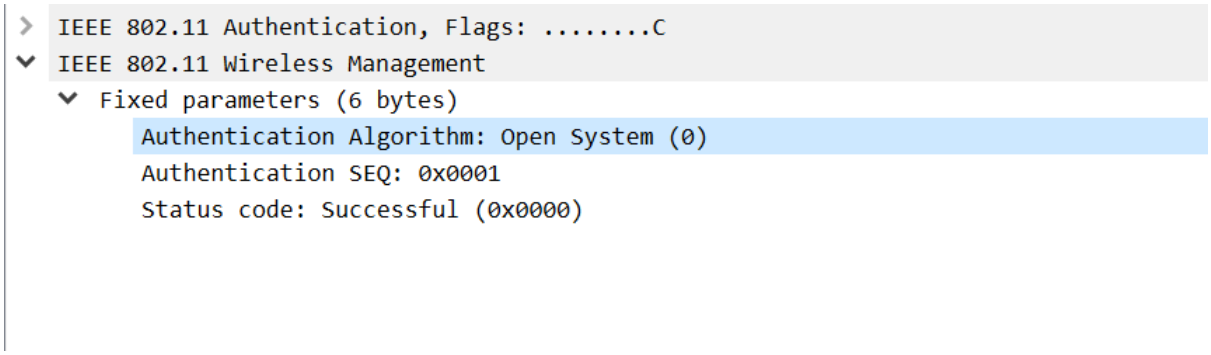
10) Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around t=49?

There're six AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP starting at t=49.638857.



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

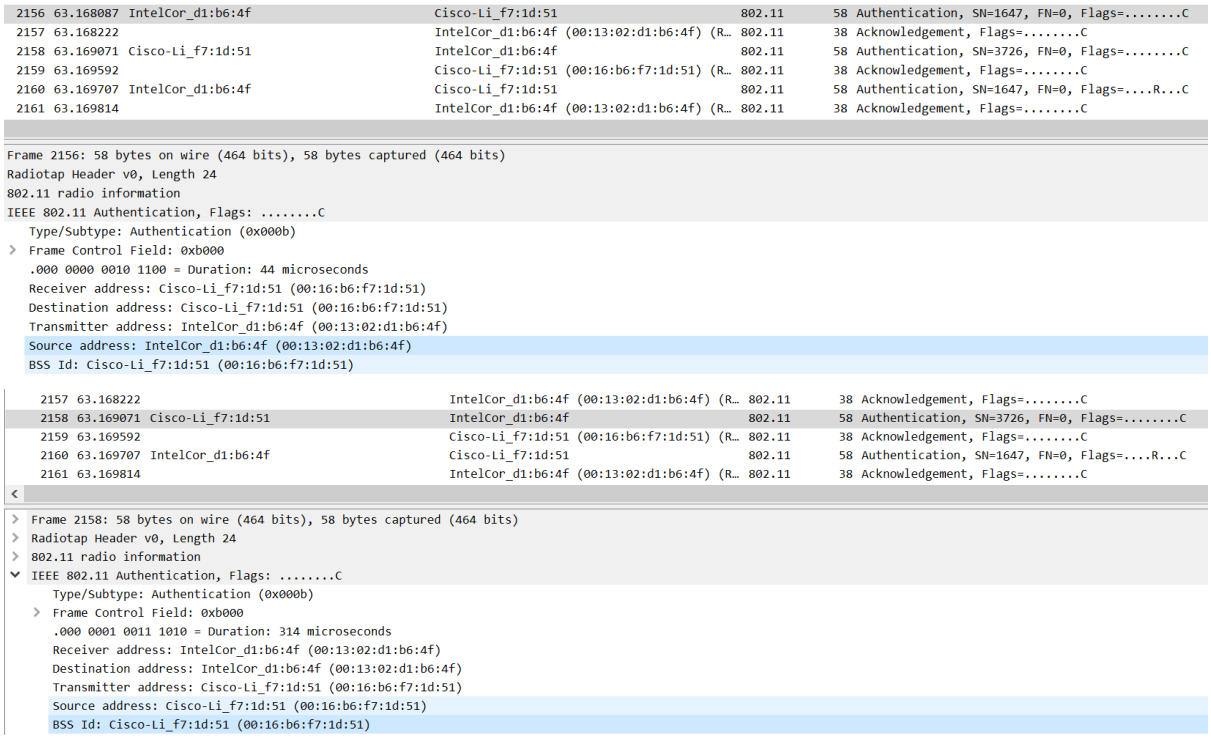
The host is requesting that the association be open. So it doesn't require a key.



12) Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?
No, I didn't. This is probably because the AP is configured to require a key when associating with that AP, so the AP is likely ignoring requests for open access.

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? (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.)

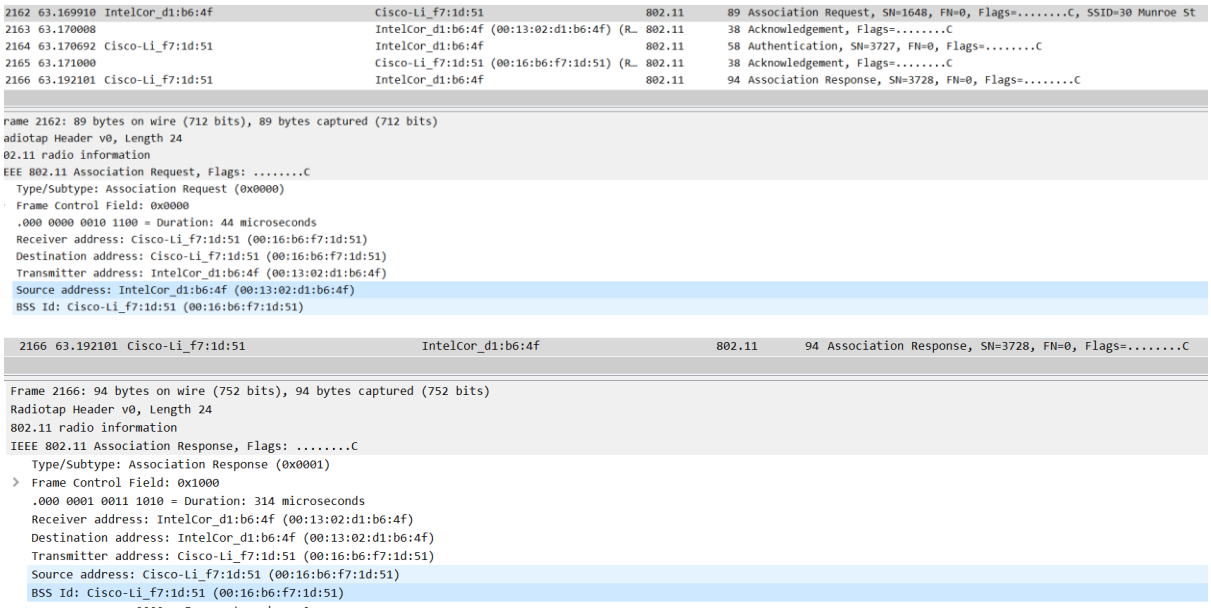
There is a AUTHENTICATION frame sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS) at t=63.168087. There is an AUTHENTICATION from sent in the reverse direction from the BSS to the wireless host at t=63.169071.



14) An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding

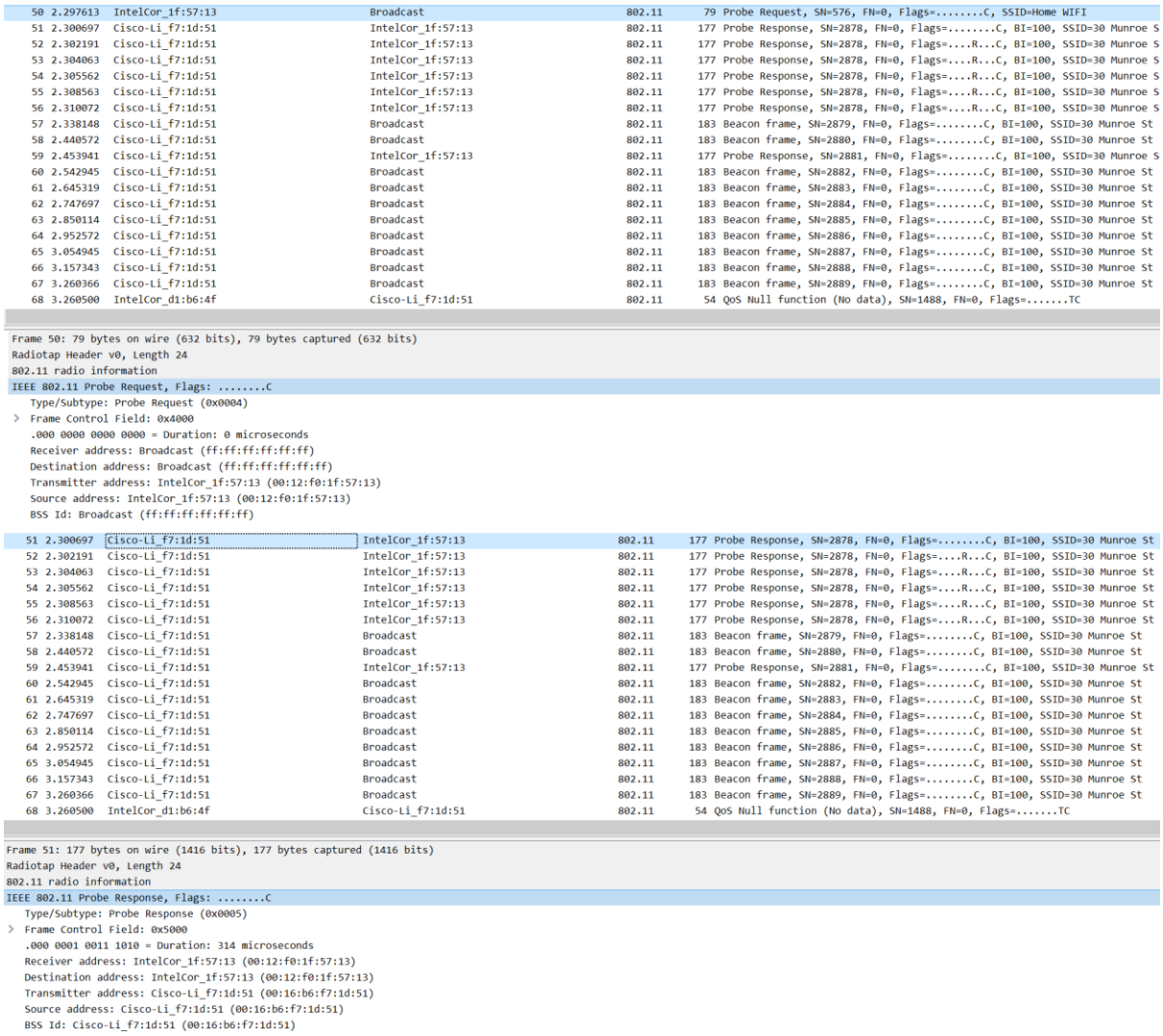
ASSOCIATE REPLY sent? (Note that you can use the filter expression "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

There is a ASSOCIATE REQUEST frame sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS) at t=63.169910. There is an ASSOCIATE RESPONSE from sent in the reverse direction from the BSS to the wireless host at t=63.192101.



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.
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 are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).
There is a PROBE REQUEST sent with source 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, and a BSS id: ff:ff:ff:ff:ff:ff at t=2.297613. There is a PROBE RESPONSE sent with source: 00:16:b6:f7:1d:51, destination: 00:12:f0:1f:57:13, and a BSS id: 00:16:b6:f7:1d:51 at t=2.300697. A PROBE REQUEST is used by a host in active scanning to find an Access Point. A PROBE RESPONSE is sent by the access point to the host sending the request.



3. Conclusion (Discussion of the result & Evaluation of the tool)

In this lab, I have studied IEEE 802.11 WLANs' characteristics over the infrastructure network (BSS with an AP), specifically, the frame exchange progress of Channel Association from host to AP. To find AP's name (SSID) and MAC address, I search through the channels via passive scanning in the 802.11 frames, perform association request/response, authentication, and run DHCP to obtain an IP address in AP's subnet. I also observed the active scanning and its associated frame, a more practical and modern method to find the AP than the passive scanning. Both passive and active scanning can co-exist within a network, complementing each other's capabilities.

As a packet analyzer, Wireshark are capable of capturing and decoding every packet that are currently-being-transmitted between clients and servers over a real-time network. It also provides practical functionalities such as timing datagram, flow graph, protocols filter, time display formatters, file I/O, and data import/export. On top of that, it's a human-friendly tool for network administrators due to its colorful GUI interface and other interactive built-in statistic toolboxes.