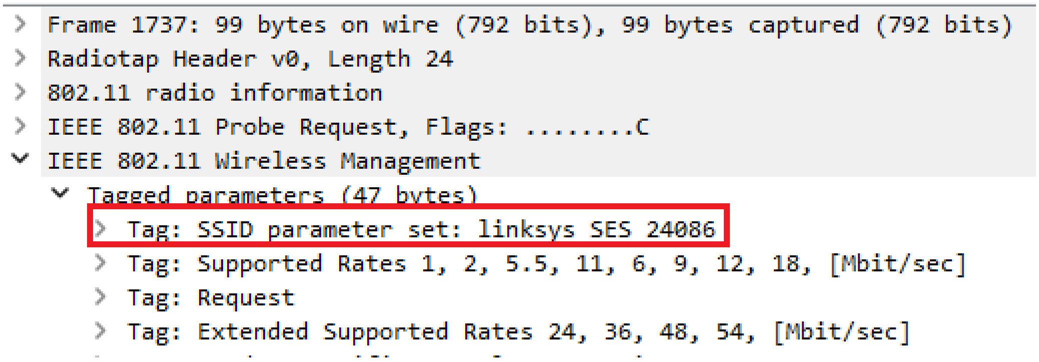
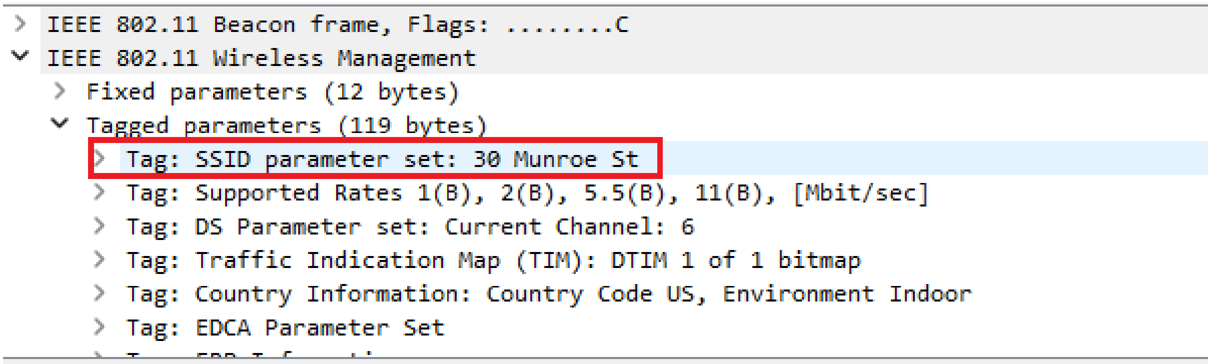
Lab_7_Wireshark_802.11_v8.0

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

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



```
> Frame 1737: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: ........C
v IEEE 802.11 Wireless Management
  v Tagged parameters (47 bytes)
    > Tag: SSID parameter set: linksys_SES_24086
    > Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    > Tag: Request
    > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
```

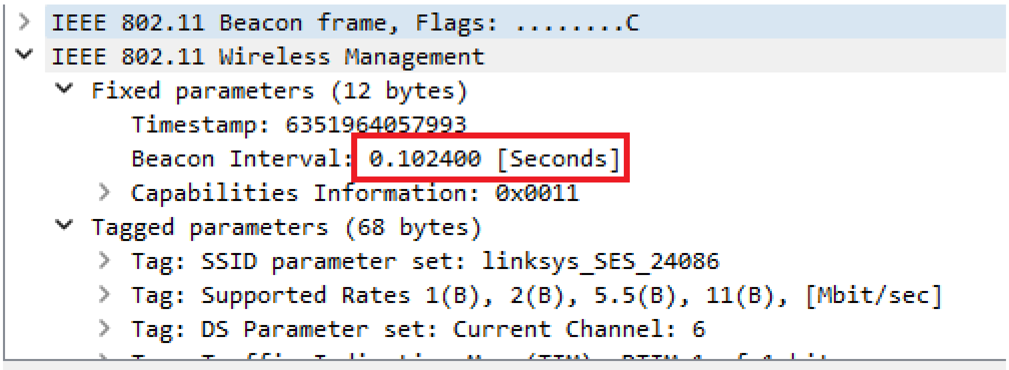


```
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (119 bytes)
    > Tag: SSID parameter set: 30 Munroe St
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Indoor
    > Tag: EDCA Parameter Set
```

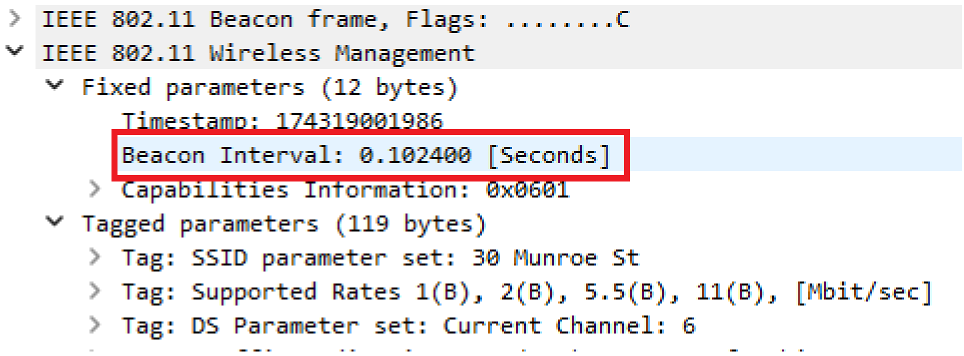
2.What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).

Answer:

- The intervals of time between the transmission of the beacon frames the linksys_ses_24086 is 0.102400
- The intervals of time between the transmission of the beacon frames the Munroe St is 0.102400 seconds
- Note that the 30 Munroe St AP beacon frames show up in the trace at this regularity, but the beacons from the linsys_SES_24086 AP do not.



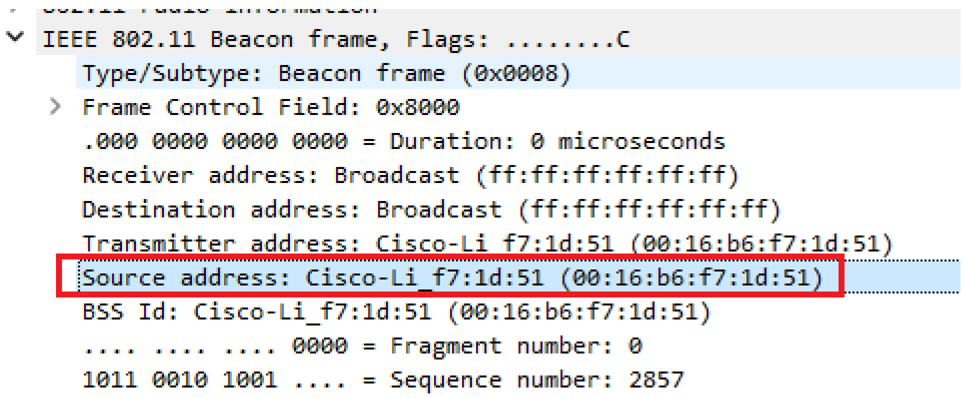
```
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
      Timestamp: 6351964057993
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0011
  v Tagged parameters (68 bytes)
    > Tag: SSID parameter set: linksys_SES_24086
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
```



```
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
      Timestamp: 174319001986
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  v Tagged parameters (119 bytes)
    > Tag: SSID parameter set: 30 Munroe St
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
```

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).

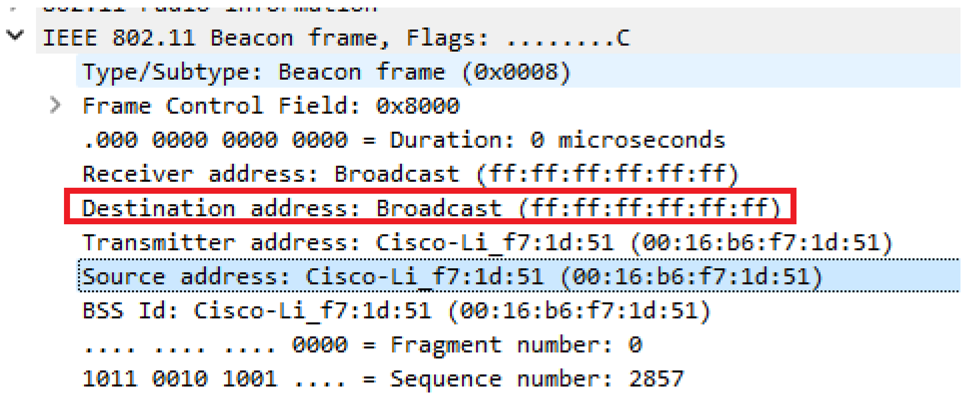
<u>Answer:</u> The source MAC address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51.



```
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 1001 .... = Sequence number: 2857
```

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

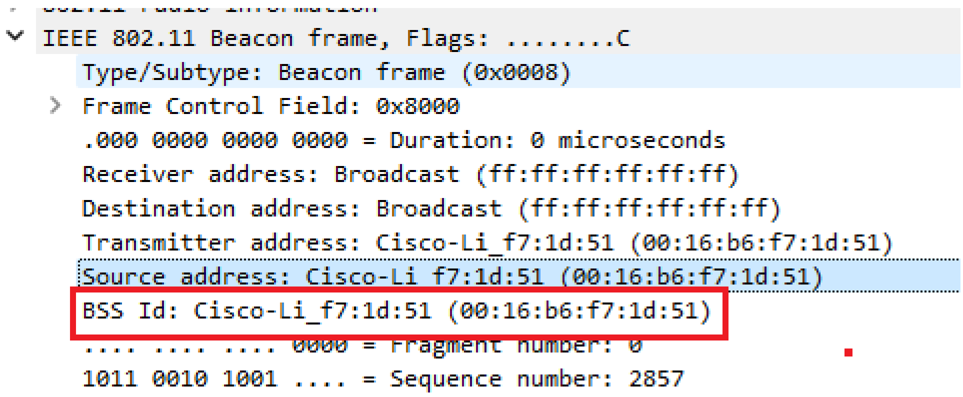
<u>Answer:</u> The destination MAC is for broadcast. The destination MAC is ff:ff:ff:ff:ff:ff.



```
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 1001 .... = Sequence number: 2857
```

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

<u>Answer:</u> The MAC BSS id on the beacon frame from the 30 Munroe St is 00:16:b6:f7:1d:51

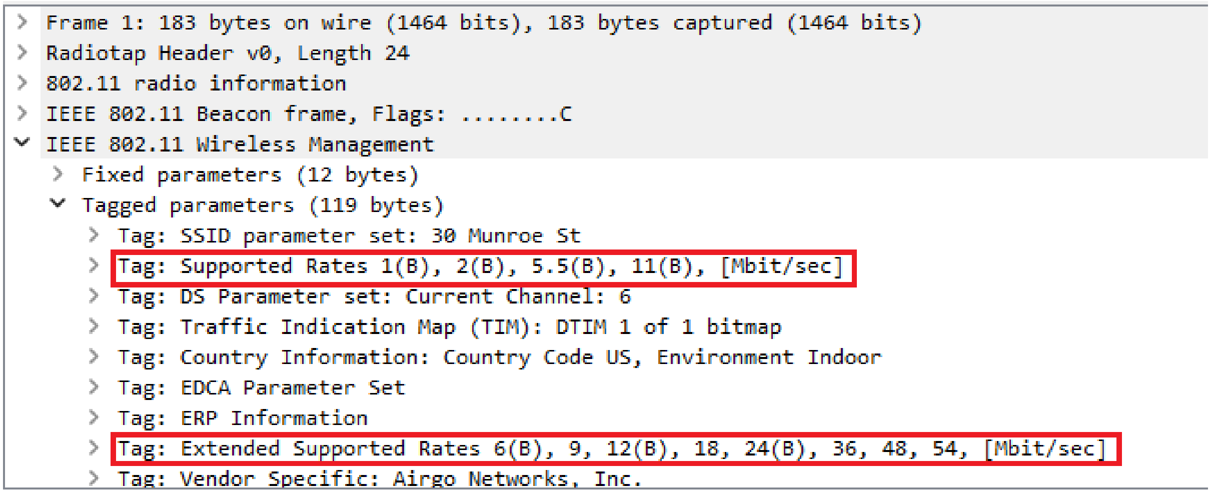


```
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    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 1001 .... = Sequence number: 2857
```

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

Answer:

- The supported rates are 1(B), 2(B), 5.5(B), 11(B) [Mbit/sec]
- The extended supported rate are 6(B), 9(B), 12(B), 18, 24(B), 36, 48, 54 [Mbit/sec]



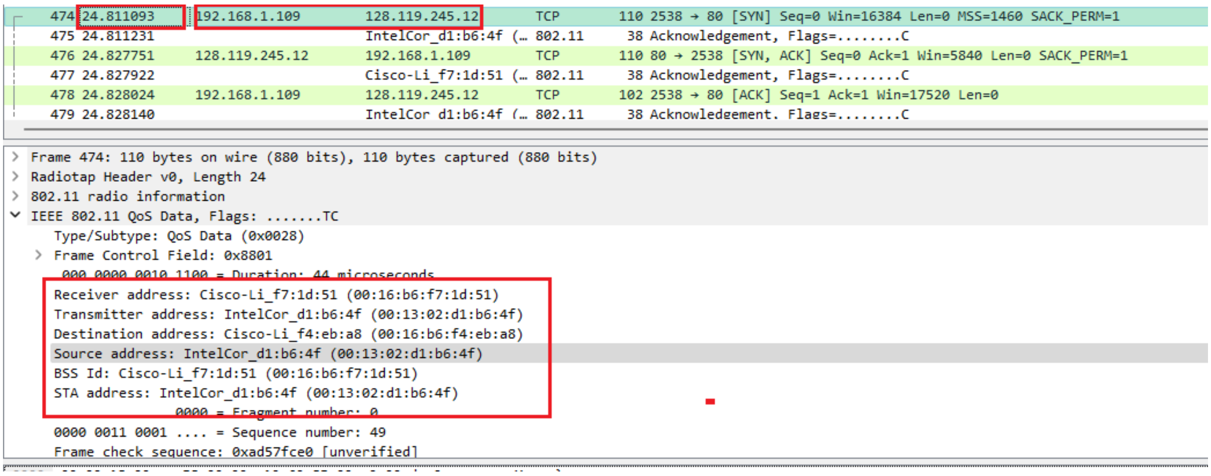
```
> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (119 bytes)
    > Tag: SSID parameter set: 30 Munroe St
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Indoor
    > Tag: EDCA Parameter Set
    > Tag: ERP Information
    > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Vendor Specific: Airgo Networks, Inc.
```

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 802.11frame? 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:

- Those MAC addresses are BSSid, source address and destination.
- 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 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.



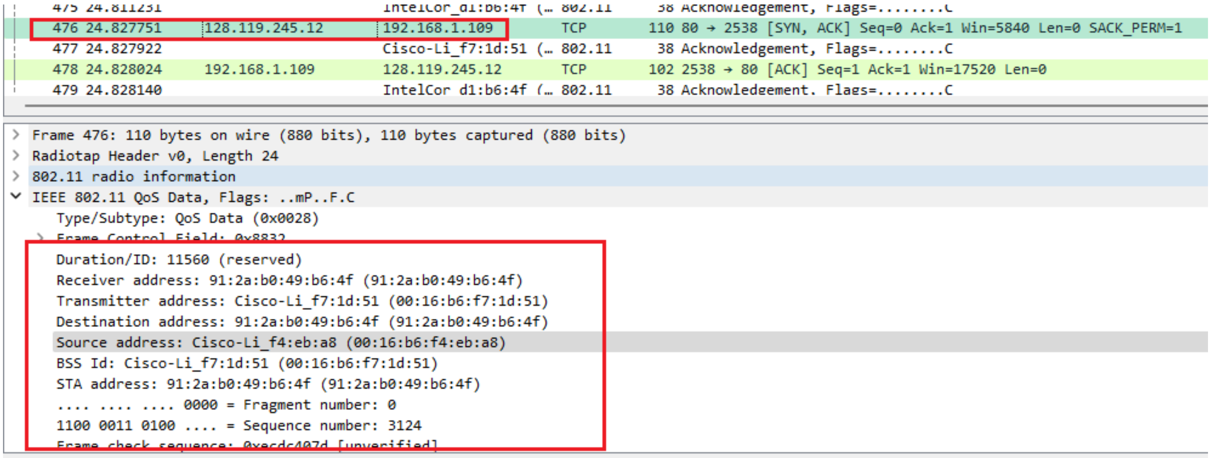
```
474 24.811093    192.168.1.109    128.119.245.12     TCP     110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
475 24.811231                     IntelCor_d1:b6:4f (… 802.11   38 Acknowledgement, Flags=........C
476 24.827751    128.119.245.12   192.168.1.109      TCP     110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477 24.827922                     Cisco-Li_f7:1d:51 (… 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 (… 802.11   38 Acknowledgement, Flags=........C

> Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
     .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
               .... .... .... 0000 = Fragment number: 0
    0000 0011 0001 .... = Sequence number: 49
    Frame check sequence: 0xad57fce0 [unverified]
```

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).

Answer:

- 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. 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).



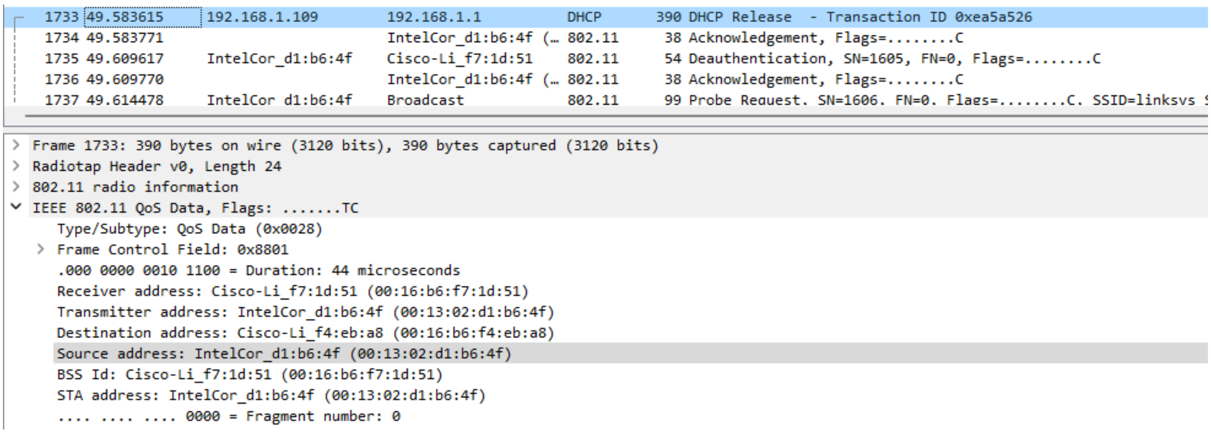
```
475 24.811231                          IntelCor_d1:b6:4f (… 802.11     38 Acknowledgement, Flags=........C
476 24.827751    128.119.245.12        192.168.1.109        TCP       110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477 24.827922                          Cisco-Li_f7:1d:51 (… 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 (… 802.11     38 Acknowledgement, Flags=........C

> Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v 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)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124
    Frame check sequence: 0xecdc407d [unverified]
```

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?

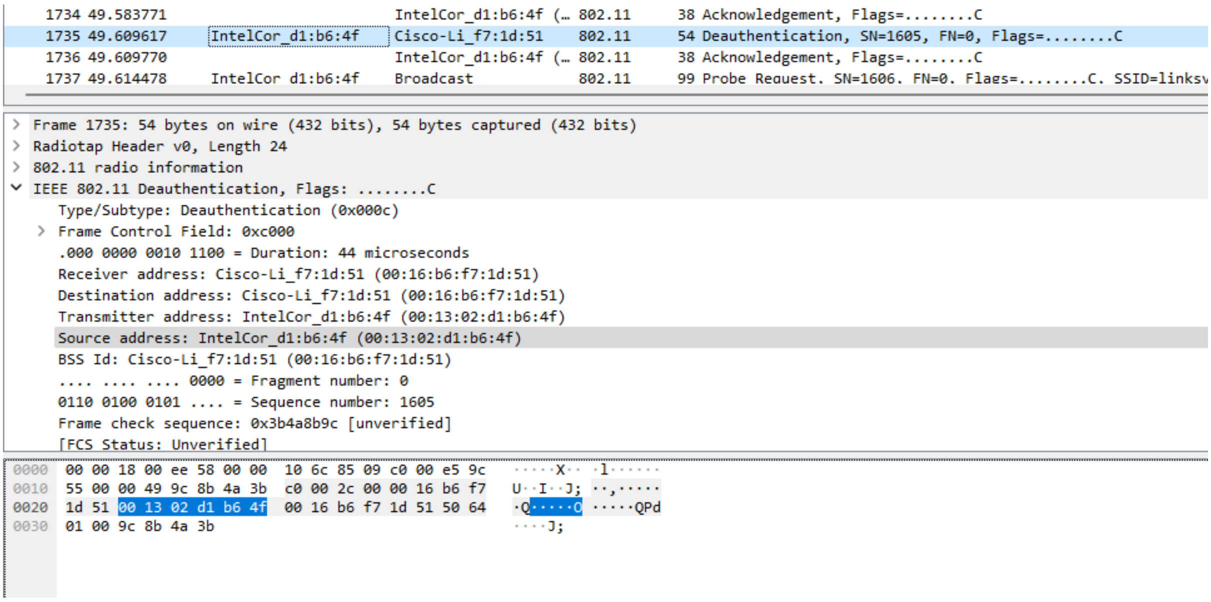
Answer:

- 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.



```
1733 49.583615   192.168.1.109       192.168.1.1          DHCP      390 DHCP Release  - Transaction ID 0xea5a526
1734 49.583771                       IntelCor_d1:b6:4f (… 802.11     38 Acknowledgement, Flags=........C
1735 49.609617   IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51    802.11     54 Deauthentication, SN=1605, FN=0, Flags=........C
1736 49.609770                       IntelCor_d1:b6:4f (… 802.11     38 Acknowledgement, Flags=........C
1737 49.614478   IntelCor_d1:b6:4f   Broadcast            802.11     99 Probe Request, SN=1606, FN=0, Flags=........C, SSID=linksys

> Frame 1733: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
```



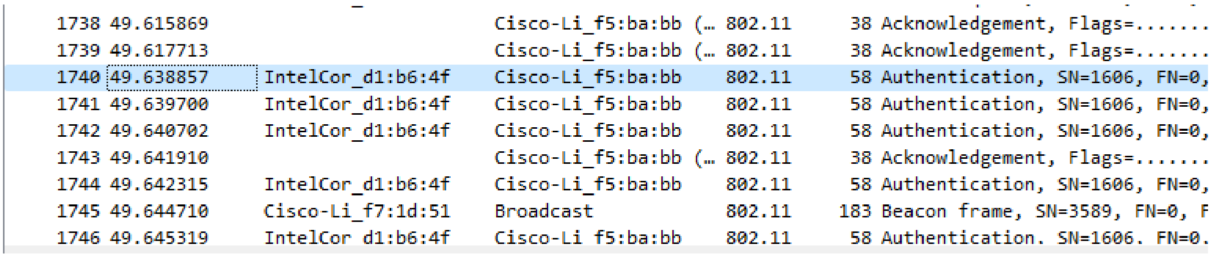
```
1734 49.583771                      IntelCor_d1:b6:4f (… 802.11    38 Acknowledgement, Flags=........C
1735 49.609617 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11    54 Deauthentication, SN=1605, FN=0, Flags=........C
1736 49.609770                      IntelCor_d1:b6:4f (… 802.11    38 Acknowledgement, Flags=........C
1737 49.614478 IntelCor_d1:b6:4f    Broadcast            802.11    99 Probe Request, SN=1606, FN=0, Flags=........C, SSID=linksy
```

```
> Frame 1735: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  > Frame Control Field: 0xc000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    0110 0100 0101 .... = Sequence number: 1605
    Frame check sequence: 0x3b4a8b9c [unverified]
    [FCS Status: Unverified]
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e5 9c   ·····X·· ·l······
0010  55 00 00 49 9c 8b 4a 3b  c0 00 2c 00 00 16 b6 f7   U··I··J; ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f7 1d 51 50 64   ·Q·····O ·····QPd
0030  01 00 9c 8b 4a 3b                                  ····J;
```

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? .

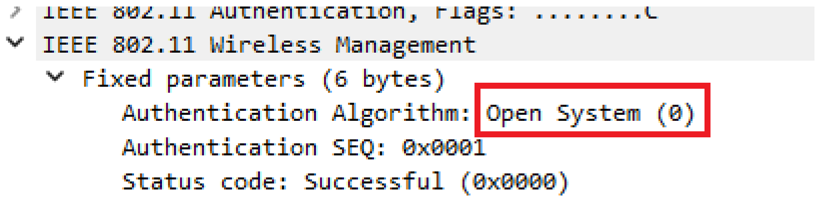
Answer: The first AUTHENTICATION from the host to the AP is at t = 49.638857.



```
1738 49.615869                      Cisco-Li_f5:ba:bb (… 802.11    38 Acknowledgement, Flags=.......
1739 49.617713                      Cisco-Li_f5:ba:bb (… 802.11    38 Acknowledgement, Flags=.......
1740 49.638857 IntelCor_d1:b6:4f    Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0,
1741 49.639700 IntelCor_d1:b6:4f    Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0,
1742 49.640702 IntelCor_d1:b6:4f    Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0,
1743 49.641910                      Cisco-Li_f5:ba:bb (… 802.11    38 Acknowledgement, Flags=.......
1744 49.642315 IntelCor_d1:b6:4f    Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0,
1745 49.644710 Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3589, FN=0, F
1746 49.645319 IntelCor_d1:b6:4f    Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0,
```

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

Answer: The host is requesting that the association be open



```
> IEEE 802.11 Authentication, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

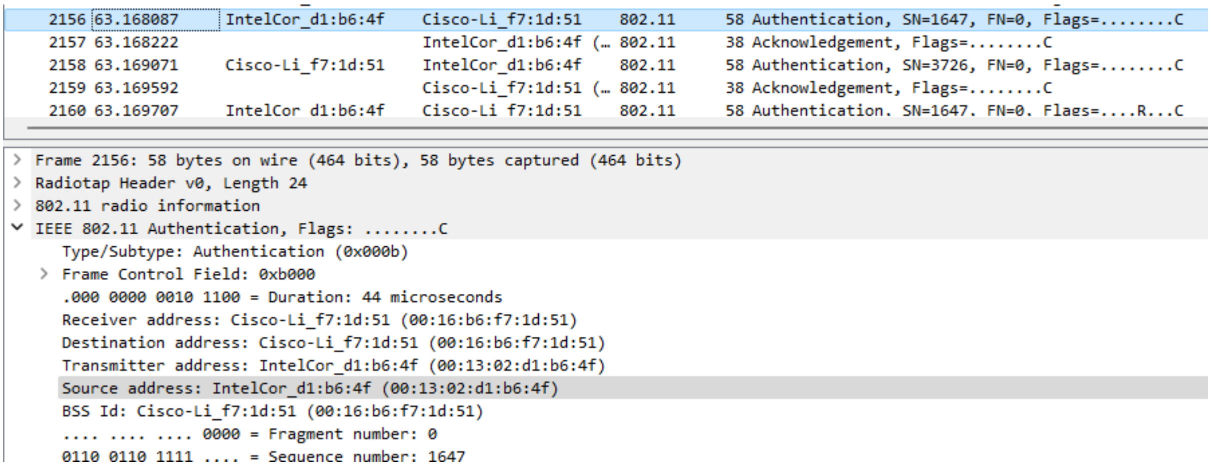
12.Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?

Answer: I can't find any reply from the AP. This is probably because the AP is configured to require a key when associating with that AP, so the AP is likely ignoring (i.e., not responding to) 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.)

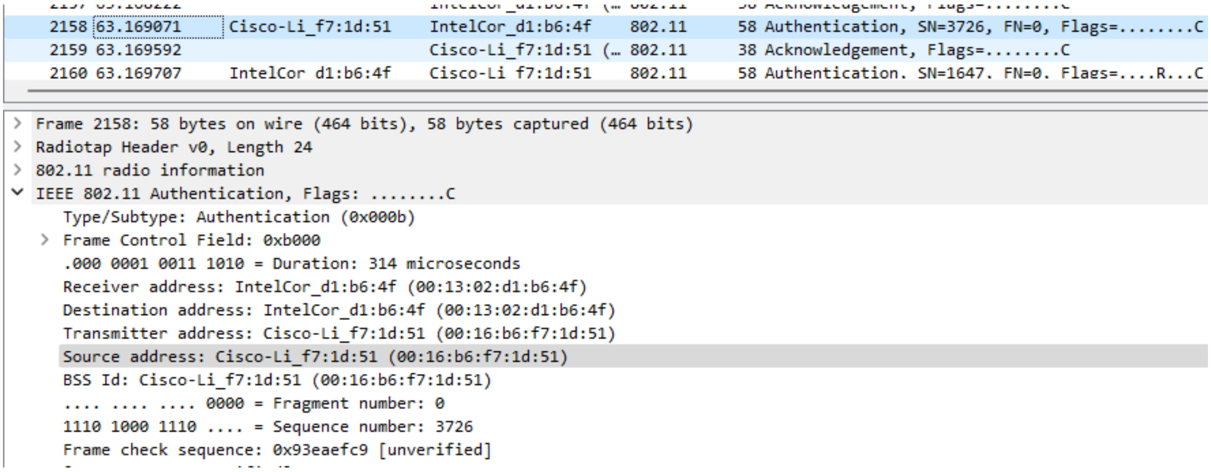
Answer:

- At t = 63.168087 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 = 63.169071 there is an AUTHENTICATION sent in the reverse direction from the BSS to the wireless host.



```
2156 63.168087   IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51    802.11     58 Authentication, SN=1647, FN=0, Flags=........C
2157 63.168222                       IntelCor_d1:b6:4f (… 802.11     38 Acknowledgement, Flags=........C
2158 63.169071   Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f    802.11     58 Authentication, SN=3726, FN=0, Flags=........C
2159 63.169592                       Cisco-Li_f7:1d:51 (… 802.11     38 Acknowledgement, 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

> Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    0110 0110 1111 .... = Sequence number: 1647
```



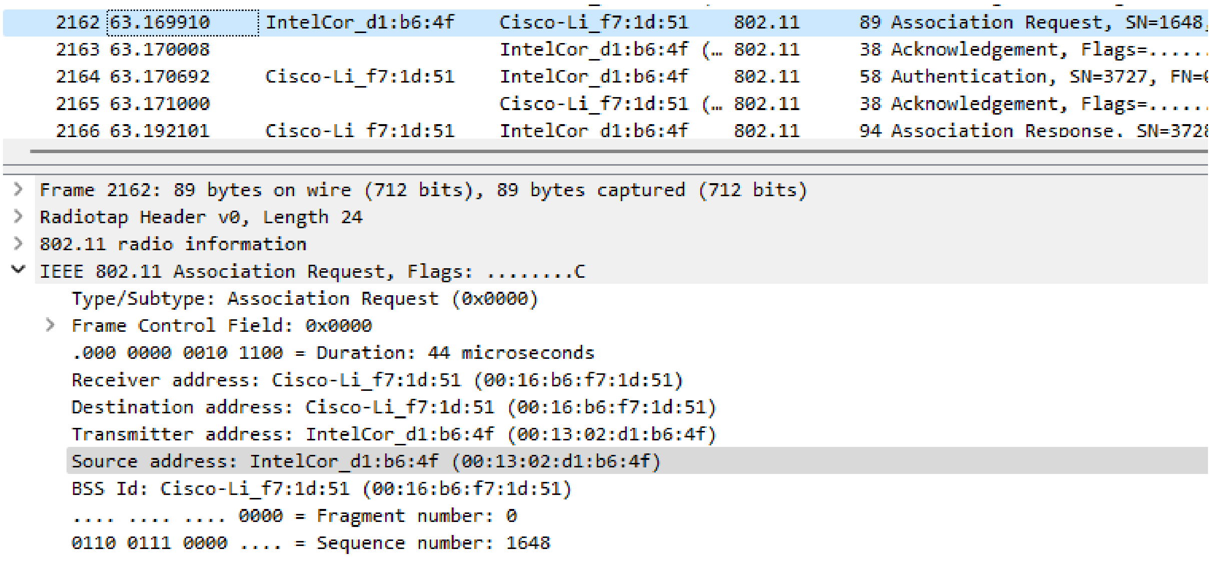
```
2158 63.169071   Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f    802.11     58 Authentication, SN=3726, FN=0, Flags=........C
2159 63.169592                       Cisco-Li_f7:1d:51 (… 802.11     38 Acknowledgement, Flags=........C
2160 63.169707   IntelCor d1:b6:4f   Cisco-Li f7:1d:51    802.11     58 Authentication. SN=1647. FN=0. Flags=....R...C

> Frame 2158: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    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
    1110 1000 1110 .... = Sequence number: 3726
    Frame check sequence: 0x93eaefc9 [unverified]
```

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.)

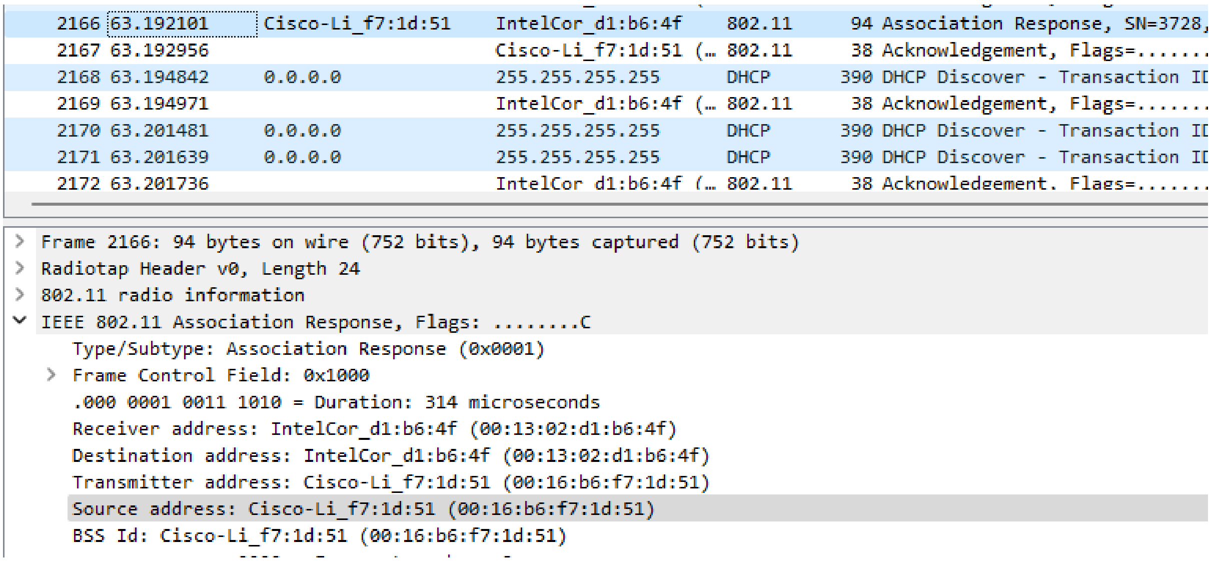
Answer:

- At t = 63.169910 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 = 63.192101 there is an ASSOCIATE RESPONSE sent in the reverse direction from the BSS to the wireless host.



```
2162 63.169910    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51      802.11    89 Association Request, SN=1648,
2163 63.170008                         IntelCor_d1:b6:4f (…  802.11    38 Acknowledgement, Flags=......
2164 63.170692    Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f      802.11    58 Authentication, SN=3727, FN=0
2165 63.171000                         Cisco-Li_f7:1d:51 (…  802.11    38 Acknowledgement, Flags=......
2166 63.192101    Cisco-Li f7:1d:51    IntelCor d1:b6:4f      802.11    94 Association Response. SN=3728

> Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  > Frame Control Field: 0x0000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    0110 0111 0000 .... = Sequence number: 1648
```



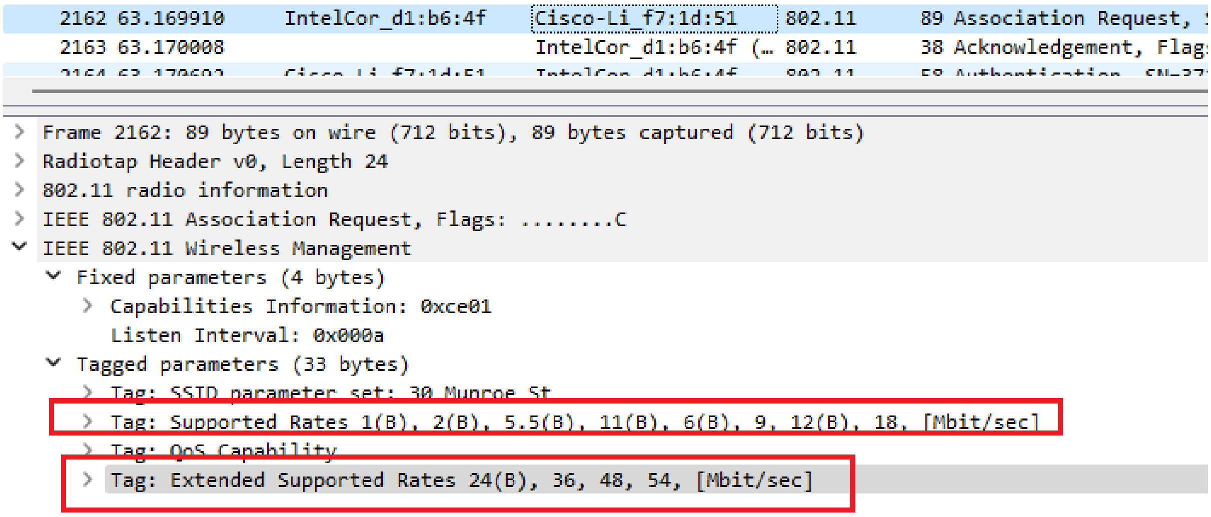
```
2166 63.192101    Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f      802.11    94 Association Response, SN=3728,
2167 63.192956                         Cisco-Li_f7:1d:51 (…  802.11    38 Acknowledgement, Flags=.......
2168 63.194842    0.0.0.0              255.255.255.255        DHCP     390 DHCP Discover - Transaction ID
2169 63.194971                         IntelCor_d1:b6:4f (…  802.11    38 Acknowledgement, Flags=.......
2170 63.201481    0.0.0.0              255.255.255.255        DHCP     390 DHCP Discover - Transaction ID
2171 63.201639    0.0.0.0              255.255.255.255        DHCP     390 DHCP Discover - Transaction ID
2172 63.201736                         IntelCor d1:b6:4f (…  802.11    38 Acknowledgement. Flags=.......

> Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Association Response, Flags: ........C
    Type/Subtype: Association Response (0x0001)
  > Frame Control Field: 0x1000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    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)
```

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.

Answer:

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



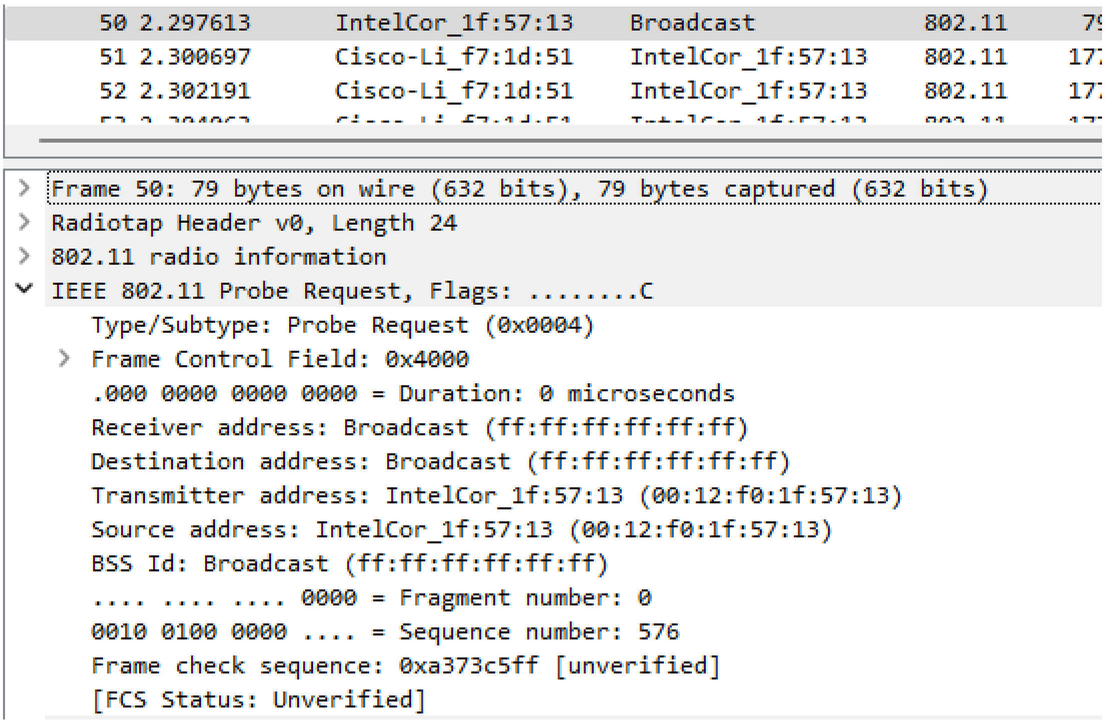
```
2162 63.169910    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11    89 Association Request, 
2163 63.170008                         IntelCor_d1:b6:4f (… 802.11    38 Acknowledgement, Flag
2164 63.170692    Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11    58 Authentication, SN=37

> Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (4 bytes)
    > Capabilities Information: 0xce01
      Listen Interval: 0x000a
  v Tagged parameters (33 bytes)
    > Tag: SSID parameter set: 30 Munroe St
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    > Tag: QoS Capability
    > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

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).

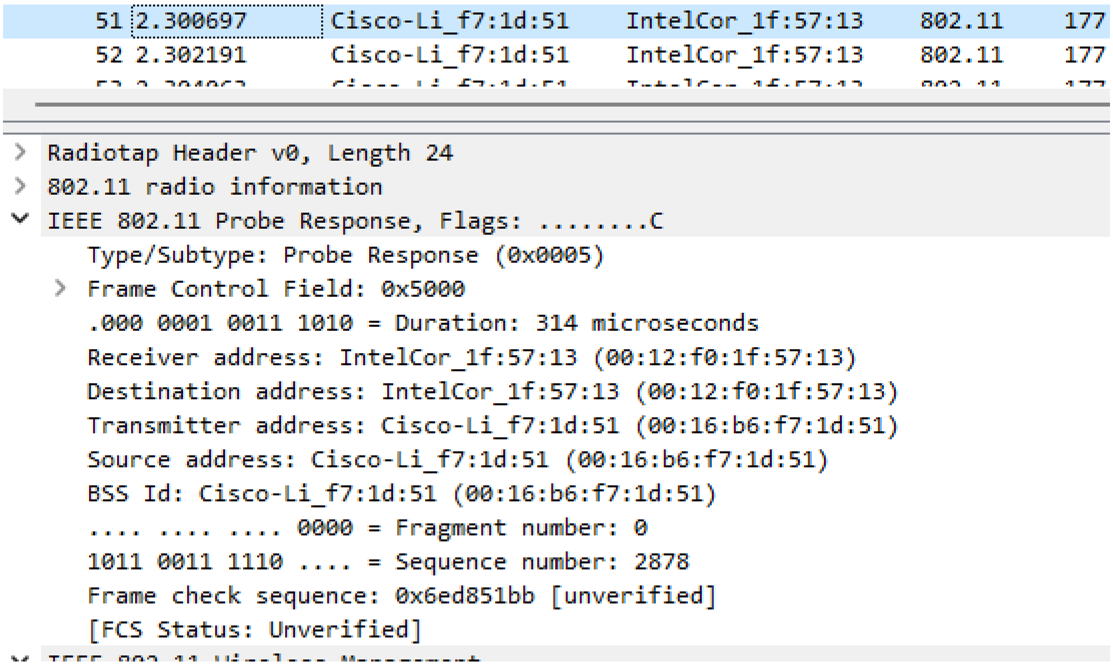
Answer:

- At t = 2.297613 there is a PROBE REQUEST sent with source 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, and a BSSID of ff:ff:ff:ff:ff:ff.
- At t = 2.300697 there is a PROBE RESPONSE sent with source: 00:16:b6:f7:1d:51, destination and a BSSID of 00:16:b6:f7:1d:51.



```
50 2.297613    IntelCor_1f:57:13    Broadcast            802.11    79
51 2.300697    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11    17
52 2.302191    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11    17
53 2.304063    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11    17

> Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  > Frame Control Field: 0x4000
    .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: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0010 0100 0000 .... = Sequence number: 576
    Frame check sequence: 0xa373c5ff [unverified]
    [FCS Status: Unverified]
```



```
     51 2.300697      Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11     177
     52 2.302191      Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11     177
     53 2.304063      Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11     177

>  Radiotap Header v0, Length 24
>  802.11 radio information
v  IEEE 802.11 Probe Response, Flags: ........C
      Type/Subtype: Probe Response (0x0005)
   >  Frame Control Field: 0x5000
      .000 0001 0011 1010 = Duration: 314 microseconds
      Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
      Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
      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 0011 1110 .... = Sequence number: 2878
      Frame check sequence: 0x6ed851bb [unverified]
      [FCS Status: Unverified]
v  IEEE 802.11 Wireless Management
```