Wireshark Lab: 802.11 Wi-Fi

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 that are issuing most of the beacon frames have an SSID of "30 Munroe St" and "linksys12". They are highlighted in the prints below;

```
No.     Time       Source              Destination         Protocol Length Info
  1499 42.532596   Cisco-Li_f5:ba:bb   Broadcast           802.11   132    Beacon frame, SN=3640, FN=0, Flags=........C, BI=100,
SSID=linksys_SES_24086
Frame 1499: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
IEEE 802.11 Wireless Management
   Fixed parameters (12 bytes)
   Tagged parameters (68 bytes)
      Tag: SSID parameter set: linksys_SES_24086
         Tag Number: SSID parameter set (0)
```

```
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
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
IEEE 802.11 Wireless Management
   Fixed parameters (12 bytes)
   Tagged parameters (119 bytes)
      Tag: SSID parameter set: 30 Munroe St
         Tag Number: SSID parameter set (0)
         Tag length: 12
```

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 beacon interval for both access points in reported in the Beacon Interval of the 802.11 wireless management frame as 0.1024 seconds.

Interval of time is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
  1499 42.532596   Cisco-Li_f5:ba:bb     Broadcast             802.11   132    Beacon frame, SN=3640, FN=0, Flags=........C, BI=100,
SSID=linksys_SES_24086
Frame 1499: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
IEEE 802.11 Wireless Management
   Fixed parameters (12 bytes)
      Timestamp: 6351964057993
      Beacon Interval: 0.102400 [Seconds]
      Capabilities Information: 0x0011
   Tagged parameters (68 bytes)
```

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 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51 which is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   1491 42.170027   Cisco-Li_f7:1d:51     Broadcast             802.11   183    Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID=30
Munroe St
Frame 1491: 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
    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
    1101 1010 1100 .... = Sequence number: 3500
    Frame check sequence: 0x786ac857 [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

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

The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff, i.e., the Ethernet broadcast address. It is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   1491 42.170027   Cisco-Li_f7:1d:51     Broadcast             802.11   183    Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID=30
Munroe St
Frame 1491: 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
    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
    1101 1010 1100 .... = Sequence number: 3500
    Frame check sequence: 0x786ac857 [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

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

The MAC BSS ID address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51. This is the same as for the source address (since this is a beacon frame). It is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   1491 42.170027   Cisco-Li_f7:1d:51     Broadcast             802.11   183    Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID=30
Munroe St
Frame 1491: 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
    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
    1101 1010 1100 .... = Sequence number: 3500
    Frame check sequence: 0x786ac857 [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

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 support rates are 1.0, 2.0, 5.5, 11.0 Mbps. The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 Mbps. Extended and support rates are highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   1491 42.170027   Cisco-Li_f7:1d:51     Broadcast             802.11   183    Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID=30
Munroe St
Frame 1491: 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
IEEE 802.11 Wireless Management
    Fixed parameters (12 bytes)
        Timestamp: 174361190786
        Beacon Interval: 0.102400 [Seconds]
        Capabilities Information: 0x0601
    Tagged parameters (119 bytes)
        Tag: SSID parameter set: 30 Munroe St
            Tag Number: SSID parameter set (0)
            Tag length: 12
            SSID: 30 Munroe St
        Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
            Tag Number: Supported Rates (1)
            Tag length: 4
  Tag: ERP Information
      Tag Number: ERP Information (42)
      Tag length: 1
      ERP Information: 0x00
  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 is connected, is 00:16:b6:f4:eb:a8. The MAC address for corresponding to the access point is 00:16:b6:f7:1d:51 which is BSS.

The IP address of the host sending the TCP SYN is 192.168.1.109. Note that this is a NATed address. The destination address is 128.199.245.12. This corresponds to the server gaia.cs.umass.edu. The destination MAC address of the frame containing the SYN, is different

from the destination IP address of the IP packet contained within this frame.Information described above is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
    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
Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Radiotap Header v0, Length 24
802.11 radio information
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)
```

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 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 corresponding to the access point is 00:16:b6:f7:1d:51 which is BSS. The IP address of the server sending the TCP SYNACK is 128.199.245.12. Information described above is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
    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
Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
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)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124
    Frame check sequence: 0xecdc407d [unverified]
    [FCS Status: Unverified]
    Qos Control: 0x0100
Logical-Link Control
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 0, Ack: 1, Len: 0
```

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?

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. The information is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   1733 49.583615   192.168.1.109         192.168.1.1           DHCP     390    DHCP Release  - Transaction ID 0xea5a526
Frame 1733: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits)
Radiotap Header v0, Length 24
802.11 radio information
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 1011 1000 .... = Sequence number: 184
    Frame check sequence: 0x90381791 [unverified]
    [FCS Status: Unverified]
    Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Release)
```

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. The information is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   1735 49.609617   IntelCor_d1:b6:4f     Cisco-Li_f7:1d:51     802.11   54     Deauthentication, SN=1605, FN=0, Flags=........C
Frame 1735: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Radiotap Header v0, Length 24
802.11 radio information
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]
IEEE 802.11 Wireless Management
    Fixed parameters (2 bytes)
        Reason code: Unspecified reason (0x0001)
```

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?

The first AUTHENTICATION from the host to the AP is at t = 49.638857 and 6 AUTHENTICATION messages are sent from wireless host to the linksys_ses_24086 AP starting at around t=49. The first AUTHENTICATION messages starting at around t=49 is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   1740 49.638857   IntelCor_d1:b6:4f     Cisco-Li_f5:ba:bb     802.11   58     Authentication, SN=1606, FN=0, Flags=........C
Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 28, 2007 21:05:56.711314000 Central Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1183082756.711314000 seconds
    [Time delta from previous captured frame: 0.021144000 seconds]
    [Time delta from previous displayed frame: 0.021144000 seconds]
    [Time since reference or first frame: 49.638857000 seconds]
    Frame Number: 1740
    Frame Length: 58 bytes (464 bits)
    Capture Length: 58 bytes (464 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Authentication, Flags: ........C
IEEE 802.11 Wireless Management
```

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

The host is requesting that the association be open (by specifying Authentication Algorithm: Open System). It is shown in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   1740 49.638857   IntelCor_d1:b6:4f     Cisco-Li_f5:ba:bb     802.11   58     Authentication, SN=1606, FN=0, Flags=........C
Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Authentication, Flags: ........C
IEEE 802.11 Wireless Management
    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?

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 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.)

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). The information described is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   2156 63.168087   IntelCor_d1:b6:4f     Cisco-Li_f7:1d:51     802.11   58     Authentication, SN=1647, FN=0, Flags=........C
Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
    Frame Control Field: 0xb000
        .... ..00 = Version: 0
        .... 00.. = Type: Management frame (0)
        1011 .... = Subtype: 11
        Flags: 0x00
    .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
    Frame check sequence: 0x47e8cbe0 [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

At t = 63.169071 there is an AUTHENTICATION from sent in the reverse direction from the BSS to the wireless host. The information described is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
   2158 63.169071   Cisco-Li_f7:1d:51     IntelCor_d1:b6:4f     802.11   58     Authentication, SN=3726, FN=0, Flags=........C
Frame 2158: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Radiotap Header v0, Length 24
802.11 radio information
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]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

14. An ASSOCIATE REQUEST 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 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.)

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). The information described is highlighted in the print below;

```
No.     Time       Source              Destination         Protocol Length Info
   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
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
    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
    Frame check sequence: 0xfe3badc6 [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

At t = 63.192101 there is an ASSOCIATE RESPONSE from sent in the reverse direction from the BSS to the wireless host. The information described is highlighted in the print below;

```
No.     Time       Source              Destination         Protocol Length Info
   2166 63.192101  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f   802.11   94     Association Response, SN=3728, FN=0, Flags=........C
Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Radiotap Header v0, Length 24
802.11 radio information
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)
    .... .... .... 0000 = Fragment number: 0
    1110 1001 0000 .... = Sequence number: 3728
    Frame check sequence: 0x37f2ab2b [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

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

In the ASSOCIATION REQUEST frame the supported and extended rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. The AP is Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51). The information described is highlighted in the print below;

```
No.     Time        Source              Destination         Protocol Length Info
   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
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
IEEE 802.11 Wireless Management
    Fixed parameters (4 bytes)
    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]
```

In the ASSOCIATION RESPONSE frame the supported and extended rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. The AP is IntelCor_d1:b6:4f (00:13:02:d1:b6:4f). The information described is highlighted in the print below;

```
No.     Time        Source              Destination         Protocol Length Info
   2166 63.192101   Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f   802.11   94     Association Response, SN=3728, FN=0, Flags=........C
Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Association Response, Flags: ........C
IEEE 802.11 Wireless Management
    Fixed parameters (6 bytes)
    Tagged parameters (36 bytes)
        Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
        Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
        Tag: EDCA Parameter Set
```

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).

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. The information described is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
     50 2.297613    IntelCor_1f:57:13     Broadcast             802.11   79     Probe Request, SN=576, FN=0, Flags=........C, SSID=Home WIFI
Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
Radiotap Header v0, Length 24
802.11 radio information
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]
IEEE 802.11 Wireless Management
```

At t = 2.300697 there is a PROBE RESPONSE sent with source: 00:16:b6:f7:1d:51, destination: 00:12:f0:1f:57:13 and a BSSID of 00:16:b6:f7:1d:51. The information described is highlighted in the print below;

```
No.     Time        Source                Destination           Protocol Length Info
     51 2.300697    Cisco-Li_f7:1d:51     IntelCor_1f:57:13     802.11   177    Probe Response, SN=2878, FN=0, Flags=........C, BI=100, SSID=30
Munroe St
Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
Radiotap Header v0, Length 24
802.11 radio information
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]
IEEE 802.11 Wireless Management
```

A PROBE REQUEST is used by a host in active scanning to find an Access Point (see Figure 6.9 on page 531 in the text). A PROBE RESPONSE is sent by the access point to the host sending the request.