CS315 : Computer Networks Lab

Assignment 12

Sourabh Bhosale (200010004)

March 28, 2023

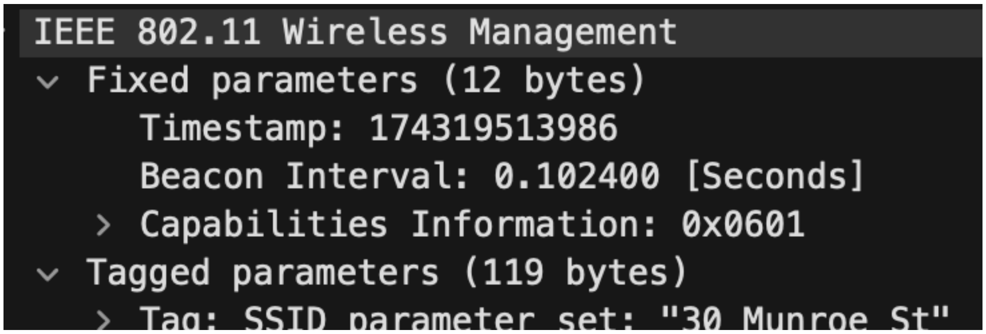
1 Part-1: Beacon Frames

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

30 Munroe St and linsys_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).

From the figure we can see that the beacon interval for both access points in reported in the Beacon Interval of the 802.11 wireless LAN Management frame as 0.1024 seconds.



```
IEEE 802.11 Wireless Management
 ⌄ Fixed parameters (12 bytes)
      Timestamp: 174319513986
      Beacon Interval: 0.102400 [Seconds]
    › Capabilities Information: 0x0601
 ⌄ Tagged parameters (119 bytes)
    › Tag: SSID parameter set: "30 Munroe St"
```

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).

Source MAC address : 00:16:b6:f7:1d:51

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

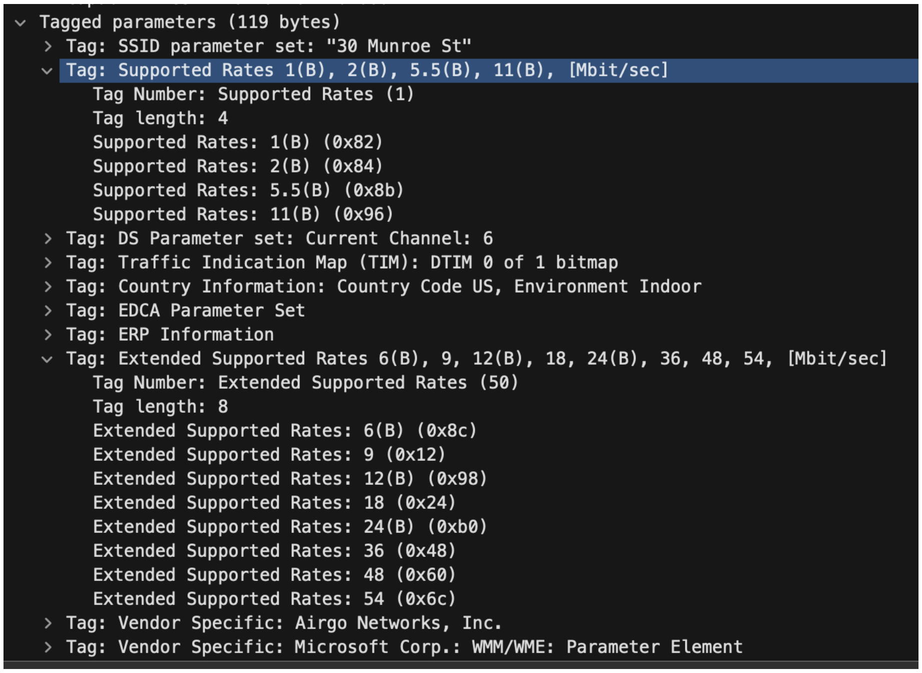
Destination MAC address : ff:ff:ff:ff:ff:ff (Ethernet broadcast address)

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

MAC BSS id : 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." What are these rates?

From the figure, we can say that the support rates are 1, 2, 5.5, 11 Mbps and the extended rates are 6, 9, 12, 18, 24, 36, 48 and 54 Mbps.

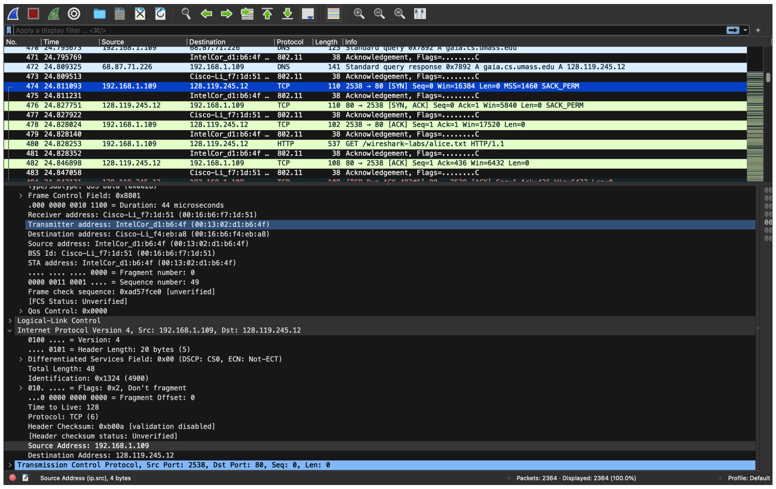


```
v Tagged parameters (119 bytes)
   > Tag: SSID parameter set: "30 Munroe St"
   v Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
         Tag Number: Supported Rates (1)
         Tag length: 4
         Supported Rates: 1(B) (0x82)
         Supported Rates: 2(B) (0x84)
         Supported 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: Country Information: Country Code US, Environment Indoor
   > Tag: EDCA Parameter Set
   > Tag: ERP Information
   v 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)
   > Tag: Vendor Specific: Airgo Networks, Inc.
   > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

2 Part-2: Data Transfer

1. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (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.
Source MAC address (for the host sending the TCP SYN) : 00:13:02:d1:b6:4f
Destination MAC address (the first hop router to which the host is connected) : 00:16:b6:f4:eb:a8
The MAC address for the BSS (access point): 00:16:b6:f7:1d:51
The IP address of the host sending the TCP SYN : 192.168.1.109
The destination IP address : 128.199.245.12.
This corresponds to the server gaia.cs.umass.edu. Also, 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.



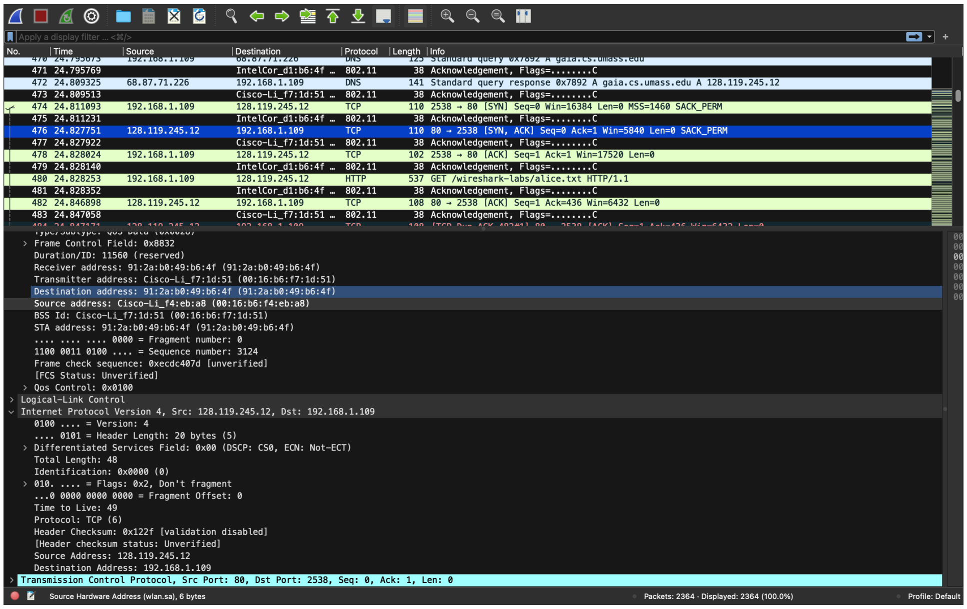
```
No.  Time       Source          Destination          Protocol Length Info
470  24.795673  192.168.1.109   68.87.71.226         DNS      125    Standard query 0x7892 A gaia.cs.umass.edu
471  24.795769                  IntelCor_d1:b6:4f …  802.11    38    Acknowledgement, Flags=........C
472  24.809325  68.87.71.226    192.168.1.109        DNS      141    Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
473  24.809513                  Cisco-Li_f7:1d:51 …  802.11    38    Acknowledgement, Flags=........C
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
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
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
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 …  802.11    38    Acknowledgement, Flags=........C
482  24.846898  128.119.245.12  192.168.1.109        TCP      108    80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
483  24.847058                  Cisco-Li_f7:1d:51 …  802.11    38    Acknowledgement, Flags=........C

    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]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
> Logical-Link Control
v 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)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xb00a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.109
    Destination Address: 128.119.245.12
> Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0

Source Address (ip.src), 4 bytes          Packets: 2364 · Displayed: 2364 (100.0%)          Profile: Default
```

2. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (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.
Source MAC address (for the sender of the 802.11 frame containing the TCP SYNACK segment which is the 1st hop router to which the host is attached) : 00:16:b6:f4:eb:a8
Destination MAC address (the host) : 91:2a:b0:49:b6:4f (this is different from the MAC address of the host used in the frame that sends the TCP SYN. The host wireless interface is behaving as if it has two interface addresses)
The MAC address for the BSS (access point): 00:16:b6:f7:1d:51
The IP address of the server sending the TCP SYNACK : 128.199.245.12 (gaia.cs.umass.edu)
The destination IP address : 192.168.1.109 (our wireless PC).



```
No.  Time       Source          Destination        Protocol Length Info
471  24.795769                  IntelCor_d1:b6:4f … 802.11    38 Acknowledgement, Flags=........C
472  24.809325  68.87.71.226    192.168.1.109      DNS      141 Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
473  24.809513                  Cisco-Li_f7:1d:51 … 802.11    38 Acknowledgement, Flags=........C
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
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
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
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 … 802.11    38 Acknowledgement, Flags=........C
482  24.846898  128.119.245.12  192.168.1.109      TCP      108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
483  24.847058                  Cisco-Li_f7:1d:51 … 802.11    38 Acknowledgement, Flags=........C
```

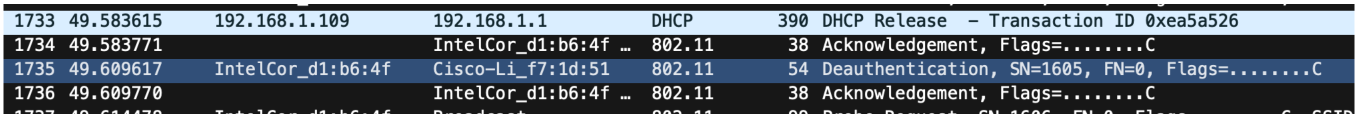
```
  > Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    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
v 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)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 49
    Protocol: TCP (6)
    Header Checksum: 0x122f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.1.109
> Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 0, Ack: 1, Len: 0
```

Source Hardware Address (wlan.sa), 6 bytes   Packets: 2364 · Displayed: 2364 (100.0%)   Profile: Default

3 Part-3: Association/Disassociation

1. What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (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?

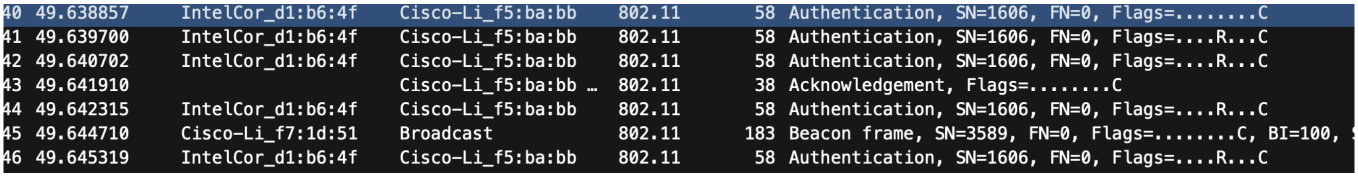
At t = 49.583615 a DHCP release is sent by the host to the DHCP server (whose IP address is 192.168.1.1) in the network that the host is leaving. At t = 49.609617, the host sends a DEAUTHENTICATION frame. One might have expected to see a DISASSOCIATION request to have been sent.



```
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
```

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

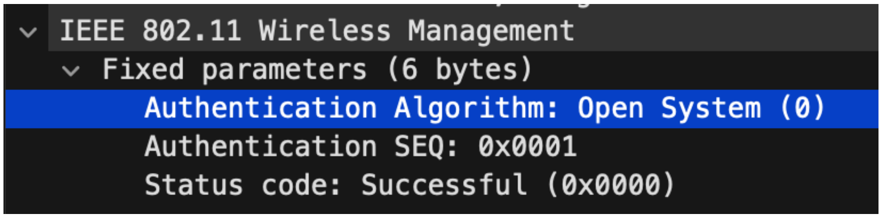
The first AUTHENTICATION from the host to the AP is at t = 49.638857. Total of 17 AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP.



```
40  49.638857     IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb    802.11       58  Authentication, SN=1606, FN=0, Flags=........C
41  49.639700     IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb    802.11       58  Authentication, SN=1606, FN=0, Flags=....R...C
42  49.640702     IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb    802.11       58  Authentication, SN=1606, FN=0, Flags=....R...C
43  49.641910                         Cisco-Li_f5:ba:bb …  802.11       38  Acknowledgement, Flags=........C
44  49.642315     IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb    802.11       58  Authentication, SN=1606, FN=0, Flags=....R...C
45  49.644710     Cisco-Li_f7:1d:51   Broadcast            802.11      183  Beacon frame, SN=3589, FN=0, Flags=........C, BI=100,
46  49.645319     IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb    802.11       58  Authentication, SN=1606, FN=0, Flags=....R...C
```

3. 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).



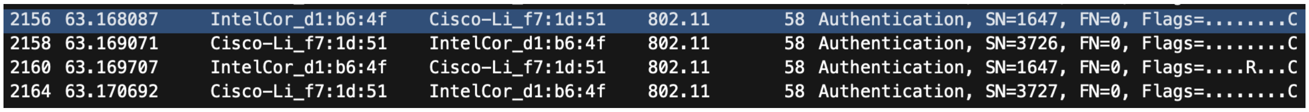
```
∨ IEEE 802.11 Wireless Management
  ∨ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

4. 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 (i.e., not responding to) requests for open access.

5. Now let's consider what happens as the host gives up trying to associate with the linksys_ses_24086 AP and now tries to associate with the 30 Munroe St AP. Look for AUTHENTICATION frames sent from the host to an AP and vice versa. 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 == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

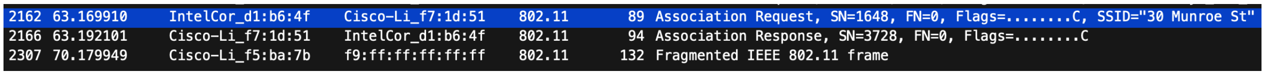
At t = 63.168087 there is a AUTHENTICATION frame sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS). At t = 63.169071 there is an AUTHENTICATION from sent in the reverse direction from the BSS to the wireless host.



```
2156  63.168087    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11        58 Authentication, SN=1647, FN=0, Flags=........C
2158  63.169071    Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11        58 Authentication, SN=3726, 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
2164  63.170692    Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11        58 Authentication, SN=3727, FN=0, Flags=........C
```

6. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to be associated with an AP. 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.)

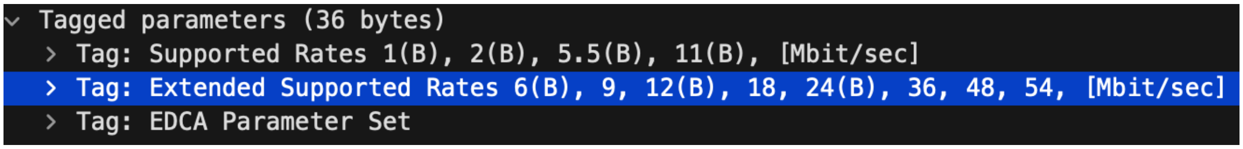
At t = 63.169910 there is a ASSOCIATE REQUEST frame sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS). At t = 63.192101 there is an ASSOCIATE RESPONSE from sent in the reverse direction from the BSS to the wireless host.



```
2162  63.169910    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11        89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
2166  63.192101    Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11        94 Association Response, SN=3728, FN=0, Flags=........C
2307  70.179949    Cisco-Li_f5:ba:7b    f9:ff:ff:ff:ff:ff    802.11       132 Fragmented IEEE 802.11 frame
```

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

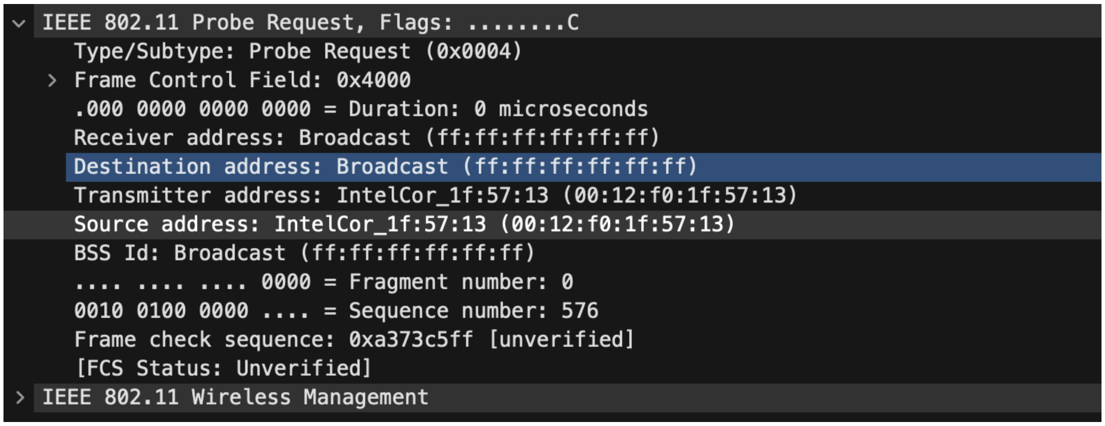
In the ASSOCIATION REQUEST frame the supported rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. The same rates are advertised in the ASSOCIATION RESPONSE.



```
⌄ 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
```

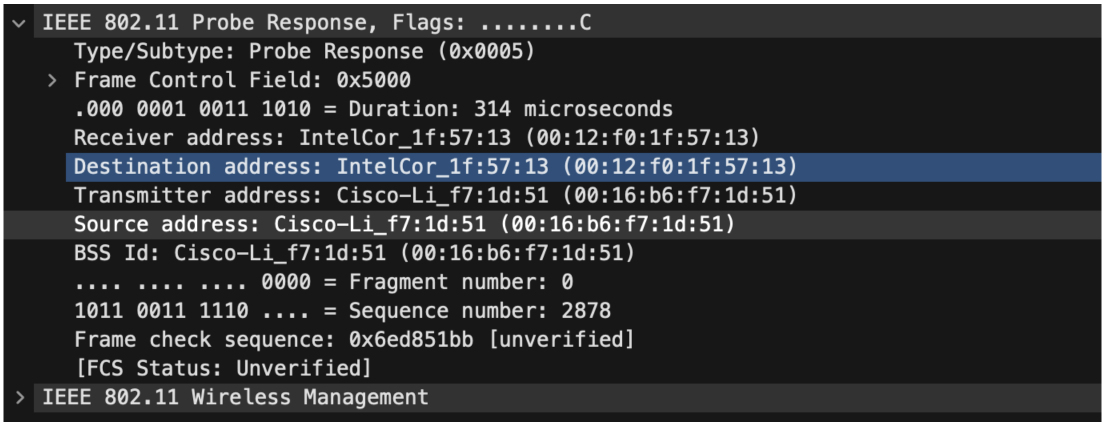
4 Part-4: Other Frame types

1. 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).



```
⌄ 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 = 2.297613 there is a PROBE REQUEST.
Source MAC address : 00:12:f0:1f:57:13
Destination MAC address : ff:ff:ff:ff:ff:ff
BSS ID : ff:ff:ff:ff:ff:ff.



```
⌄ 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
```

At t = 2.300697 there is a PROBE RESPONSE
Source MAC address : 00:16:b6:f7:1d:51
Destination MAC address : 00:12:f0:1f:57:13
BSS ID : 00:16:b6:f7:1d:51.

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.