EE 450

Lab #3

Name: Shih-Ju Hsu

1. They are **30 Munroe St** and **linksys_SES_24086**.

```
No.     Time           Source                Destination           Protocol Length Info
   1994 59.325865      Cisco-Li_f5:ba:bb     Broadcast             802.11   132    Beacon
frame, SN=3833, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
Frame 1994: 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
No.     Time           Source                Destination           Protocol Length Info
   1995 59.372340      Cisco-Li_f7:1d:51     Broadcast             802.11   183    Beacon
frame, SN=3684, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
Frame 1995: 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
```

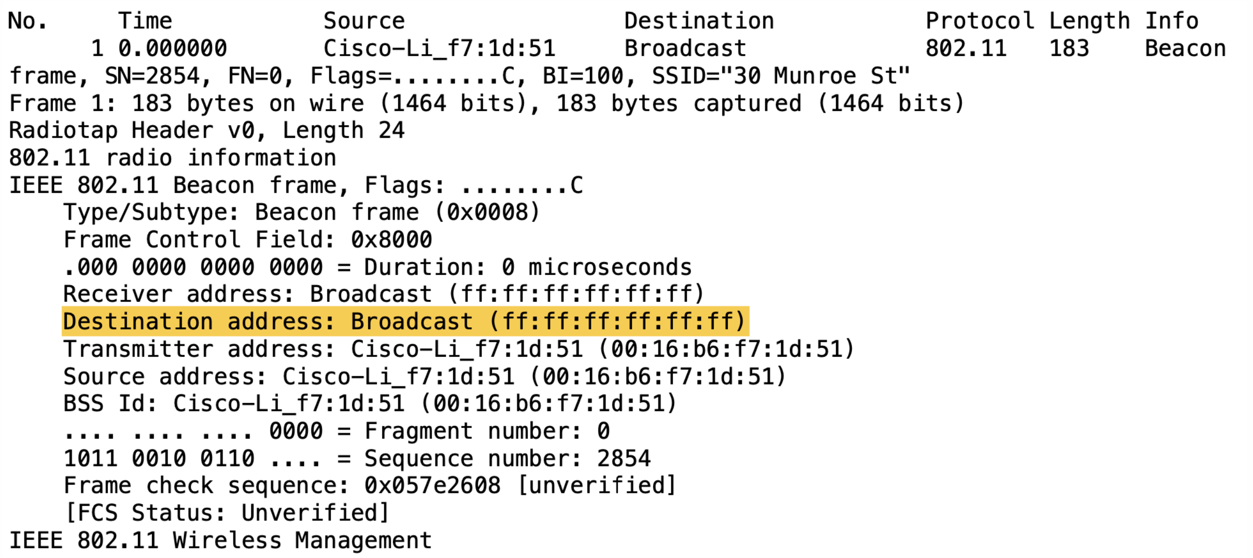
2. They are both **0.1024 seconds**.

```
No.     Time           Source                Destination           Protocol Length Info
     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"
Frame 13: 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: 174319513986
        Beacon Interval: 0.102400 [Seconds]
        Capabilities Information: 0x0601
    Tagged parameters (119 bytes)
No.     Time           Source                Destination           Protocol Length Info
   1527 43.658960      Cisco-Li_f5:ba:bb     Broadcast             802.11   132    Beacon
frame, SN=3651, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
Frame 1527: 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: 6351965184389
        Beacon Interval: 0.102400 [Seconds]
        Capabilities Information: 0x0011
    Tagged parameters (68 bytes)
```

3. It is **00:16:b6:f7:1d:51**.

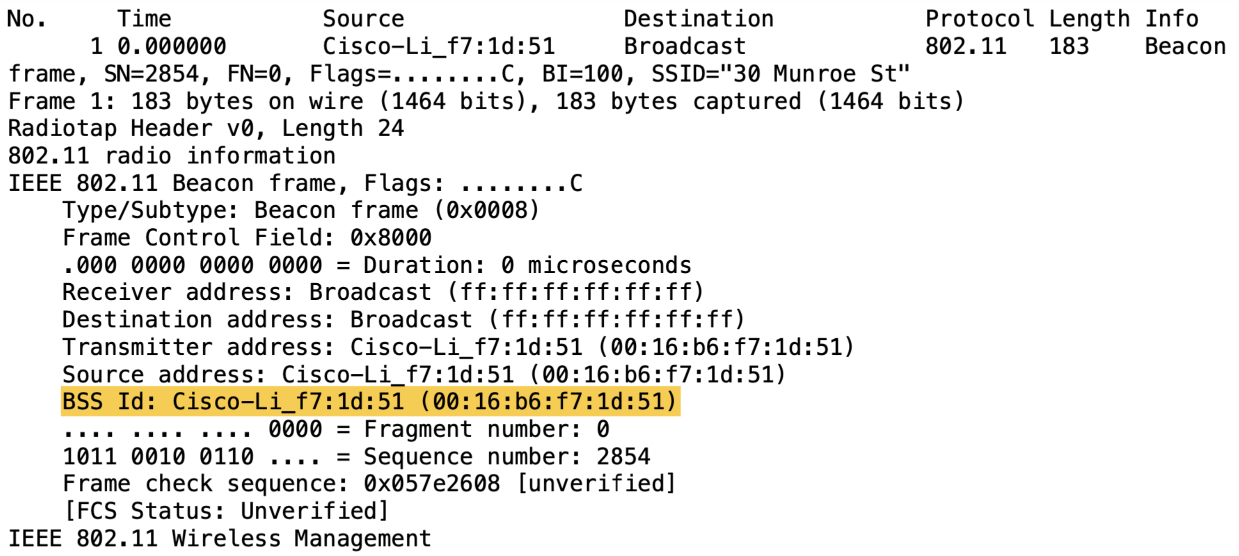
```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       Cisco-Li_f7:1d:51     Broadcast             802.11   183    Beacon
frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
    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]
IEEE 802.11 Wireless Management
```

4. It is **ff:ff:ff:ff:ff:ff** (broadcast).



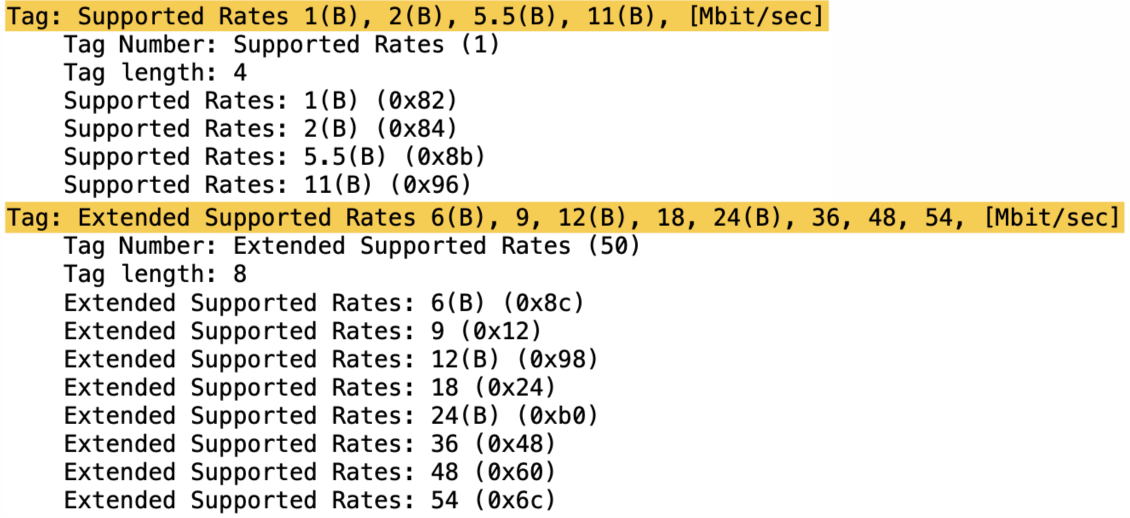
```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       Cisco-Li_f7:1d:51     Broadcast             802.11   183    Beacon
frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
    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]
IEEE 802.11 Wireless Management
```

5. It is **00:16:b6:f7:1d:51**.



```
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
    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]
IEEE 802.11 Wireless Management
```

6. Supported Rates: **1, 2, 5.5, 11 (Mbps)**. Extended Supported Rates: **6, 9, 12, 18, 24, 36, 48, 54 (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. Three MAC address fields are **destination address**, **source address** and **BSS Id**.

   MAC address corresponds to the wireless host: **00:13:02:d1:b6:4f** (source address)

MAC address corresponds to the access point: **00:16:b6:f7:1d:51** (BSS Id)

MAC address corresponds to the first-hop router: **00:16:b6:f4:eb:a8** (desination address)

IP address of the wireless host: **192.168.1.109**

Destination IP address: **128.119.245.12**

The destination IP address is the **IP address of gaia.cs.umass.edu** since it's the destination address of the IP packet.

```
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
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)
    .... .... .... 0000 = Fragment number: 0
    0000 0011 0001 .... = Sequence number: 49
    Frame check sequence: 0xad57fce0 [unverified]
    [FCS Status: Unverified]
    Qos Control: 0x0000
Logical-Link Control
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
```

8. Three MAC address fields are **destination address**, **source address** and **BSS Id**.

   MAC address corresponds to the host: **91:2a:b0:49:b6:4f** (destination address)

   MAC address corresponds to the access point: **00:16:b6:f7:1d:51** (BSS Id)

   MAC address corresponds to the first-hop router: **00:16:b6:f4:eb:a8** (source address)

   No. The IP address of the device that sent the TCP segment is **128.119.245.12**, which is the IP address of gaia.cs.umass.edu. The sender MAC address is **00:16:b6:f4:eb:a8**, which is the MAC address of the first-hop router.

```
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
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
    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
```

9.

(1) The host sent a DHCP release to the DHCP server.

(2) The host sent a deauthentication frame to the access point (30 Munroe St).

```
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
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)
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
IEEE 802.11 Wireless Management
    Fixed parameters (2 bytes)
```

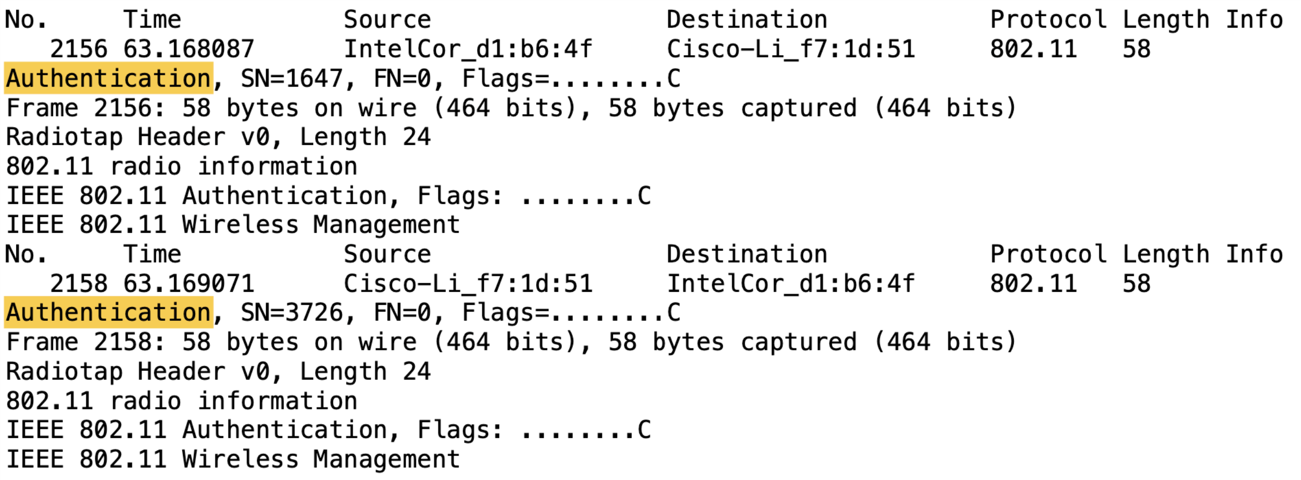
There should be a **disassociation** request to be sent but we don't see here.

10. There are **17** frames. They are frame 1740, 1741, 1742, 1744, 1746, 1749, 1750, 1751, 1821, 1822, 1921, 1922, 1923, 1924, 2122, 2123 and 2124.

11. **Yes.** The host wants the authentication to require a key or be open.

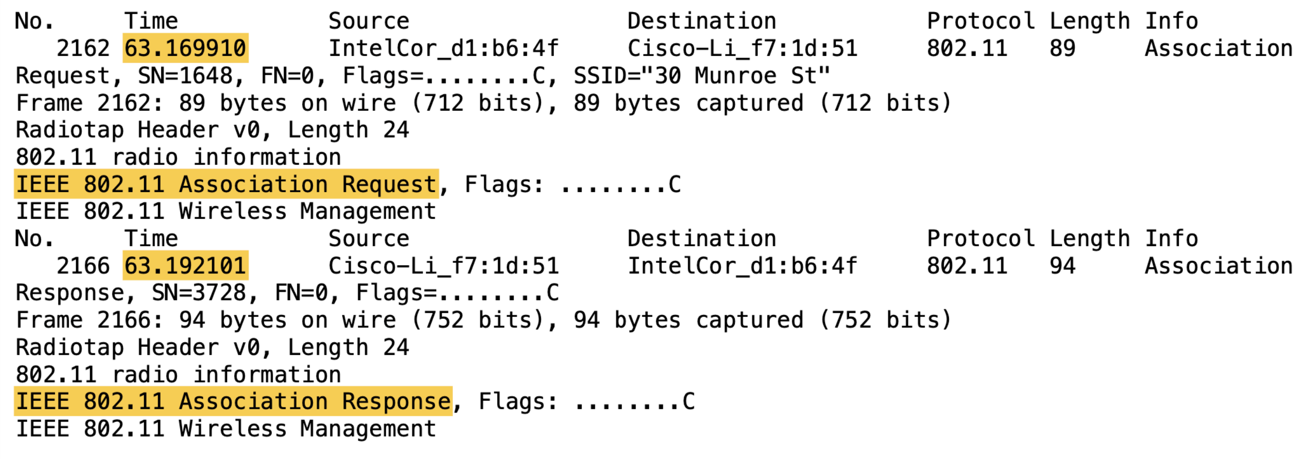
12. **No.** We can't find a reply authentication from the `linksys_ses_24086` AP in the trace.

13. At **63.168087**, the wireless host (00:13:02:d1:b6:4f) sent an authentication frame to the BSS (00:16:b6:f7:1d:51). At **63.169071**, the BSS sent an authentication frame back to the host.



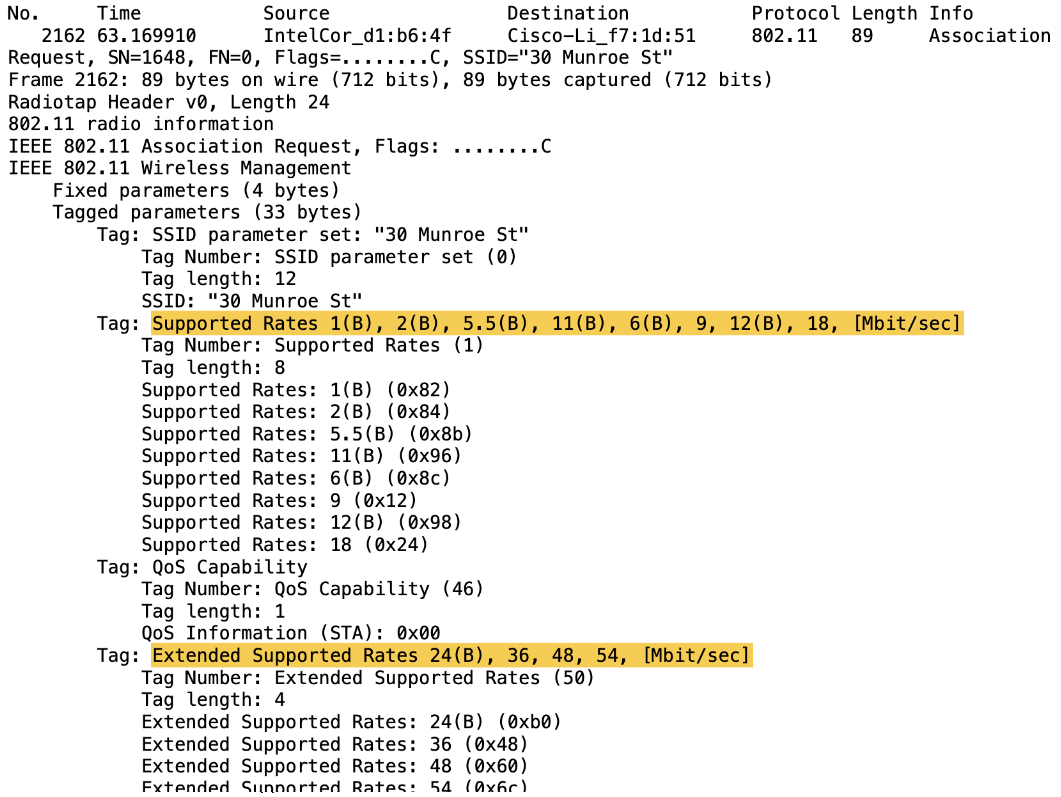
```
No.     Time           Source                Destination           Protocol Length Info
   2156 63.168087      IntelCor_d1:b6:4f     Cisco-Li_f7:1d:51     802.11   58
Authentication, SN=1647, FN=0, Flags=........C
Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Authentication, Flags: ........C
IEEE 802.11 Wireless Management
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
IEEE 802.11 Wireless Management
```

14. At **63.169910**, the host sent an association request. At **63.192101**, the *30 Munroe St* AP sent an association response.

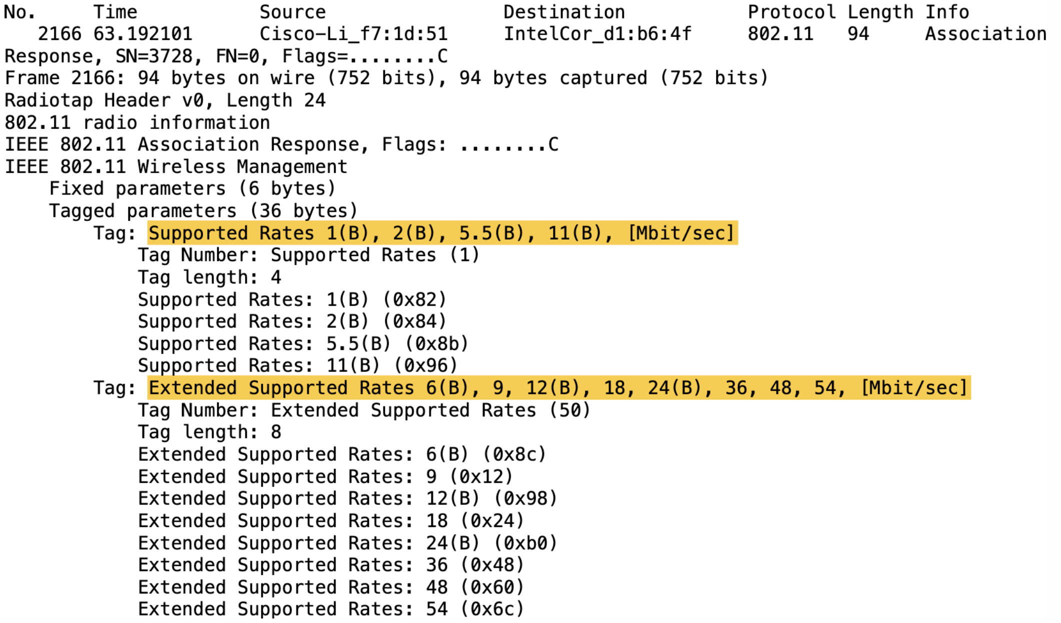


```
No.     Time           Source                Destination           Protocol Length Info
   2162 63.169910      IntelCor_d1:b6:4f     Cisco-Li_f7:1d:51     802.11   89     Association
Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Association Request, Flags: ........C
IEEE 802.11 Wireless Management
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
```

15. The supported rates are **1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 (Mbps)** for the host. The supported rates are the same for the AP.



```
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 Number: SSID parameter set (0)
            Tag length: 12
            SSID: "30 Munroe St"
        Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
            Tag Number: Supported Rates (1)
            Tag length: 8
            Supported Rates: 1(B) (0x82)
            Supported Rates: 2(B) (0x84)
            Supported Rates: 5.5(B) (0x8b)
            Supported Rates: 11(B) (0x96)
            Supported Rates: 6(B) (0x8c)
            Supported Rates: 9 (0x12)
            Supported Rates: 12(B) (0x98)
            Supported Rates: 18 (0x24)
        Tag: QoS Capability
            Tag Number: QoS Capability (46)
            Tag length: 1
            QoS Information (STA): 0x00
        Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
            Tag Number: Extended Supported Rates (50)
            Tag length: 4
            Extended Supported Rates: 24(B) (0xb0)
            Extended Supported Rates: 36 (0x48)
            Extended Supported Rates: 48 (0x60)
            Extended Supported Rates: 54 (0x6c)
```



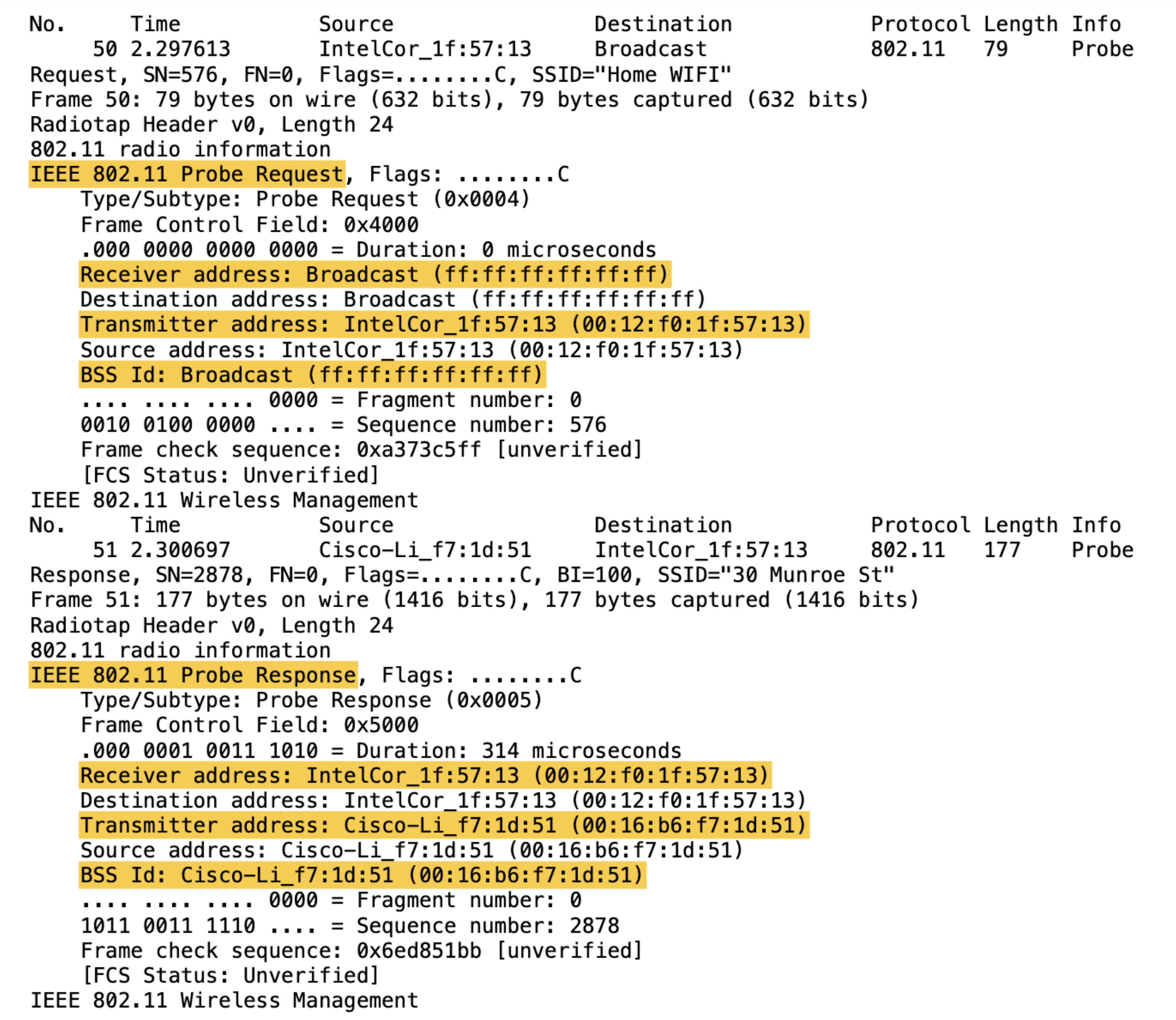
```
No.     Time           Source                Destination           Protocol Length Info
   2166 63.192101      Cisco-Li_f7:1d:51     IntelCor_d1:b6:4f     802.11   94     Association
Response, SN=3728, FN=0, Flags=........C
Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Radiotap 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 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)
```

16. Probe Request:

    - Receiver address: **ff:ff:ff:ff:ff:ff**
    - Transmitter(sender) address: **00:12:f0:1f:57:13**
    - BSS Id: **ff:ff:ff:ff:ff:ff**

    Probe Response:

    - Receiver address: **00:12:f0:1f:57:13**
    - Transmitter(sender) address: **00:16:b6:f7:1d:51**
    - BSS Id: **00:16:b6:f7:1d:51**



```
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
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 hosts to **actively find an access point**. A probe response is sent by the AP to **respond the host**.

Conclusion

In this lab, we use Wireshark to examine 802.11 frames for exploring various aspects of 802.11, including the MAC addresses of senders, receivers, BSS and the role of beacons and probes. We also observe the process of authentication, association, and disassociation between wireless devices and access points. All in all, the lab helps us in understanding the mechanism of wireless communication by analyzing the frames.