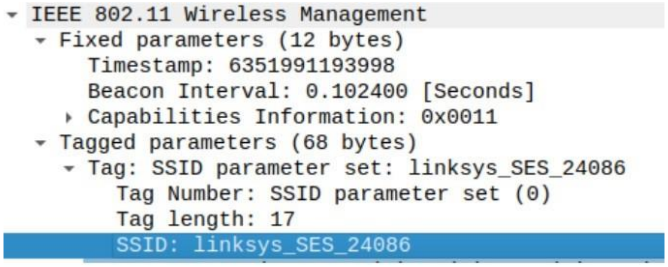
Computer Networks Lab

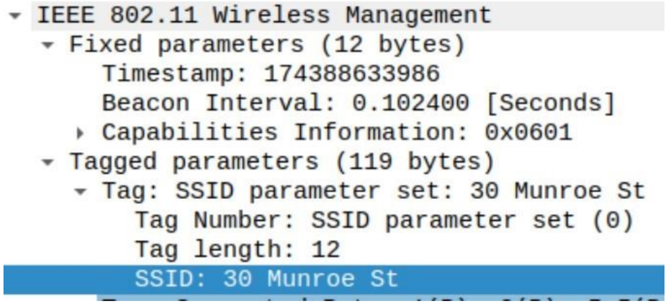
ASSIGNMENT – 12

Rahul Cheryala, 210010012

PART – 1:

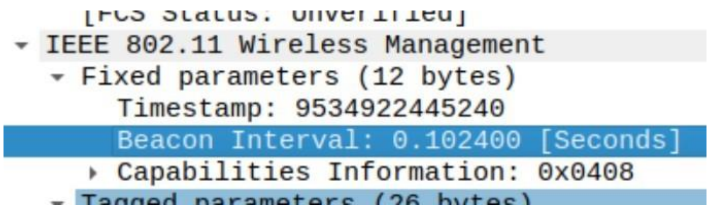


```
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 6351991193998
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0011
  ▾ Tagged parameters (68 bytes)
    ▾ Tag: SSID parameter set: linksys_SES_24086
        Tag Number: SSID parameter set (0)
        Tag length: 17
        SSID: linksys_SES_24086
```



```
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 174388633986
      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
```

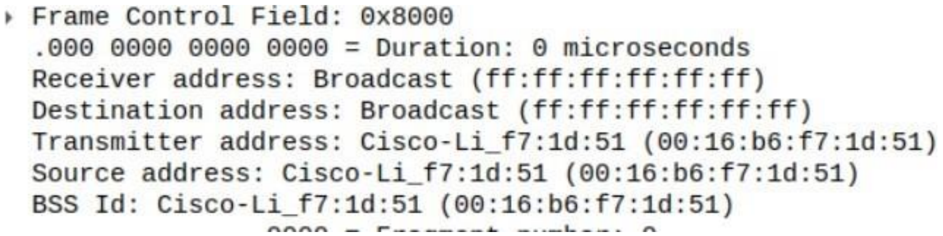
1. The two access points issuing most beacon frames have an SSID of “30 Munroe St” and “linsys_SES_24086.”



```
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 9534922445240
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0408
  ▾ Tagged parameters (26 bytes)
```

2. The beacon interval for both access points is reported in the Beacon Interval of the 802.11 wireless LAN Management frame as 0.102400

seconds.

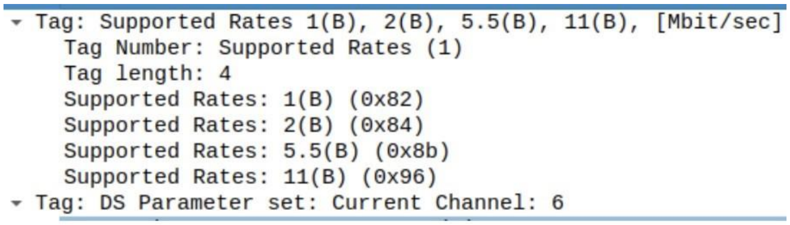


```
▸ Frame Control Field: 0x8000
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
                  0000 = Fragment number: 0
```

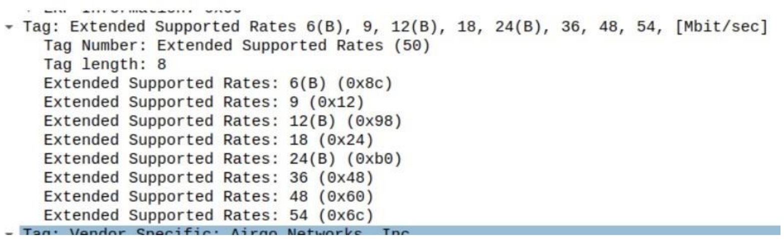
3. The source MAC address on the 30 Munroe St beacon frame is 00:16:b6:f7:1d:51.

4. The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff, i.e., the Ethernet broadcast address.

5. The MAC BSS ID address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51.



```
▾ 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
```

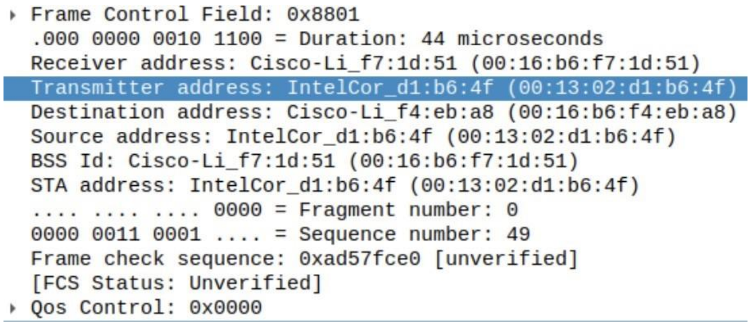


```
▸ ERP Information: 0x00
▾ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 8
    Extended Supported Rates: 6(B) (0x8c)
    Extended Supported Rates: 9 (0x12)
    Extended Supported Rates: 12(B) (0x98)
    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)
▸ Tag: Vendor Specific: Airgo Networks, Inc.
```

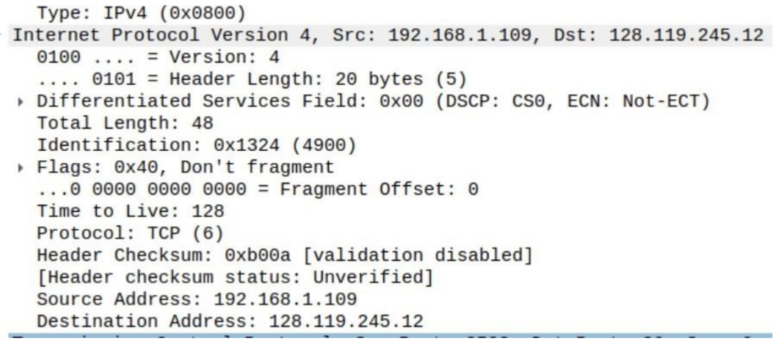
6. The support rates are 1.0, 2.0, 5.5, and 11.0 Mbps. The extended

speeds are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 Mbps.

PART – 2

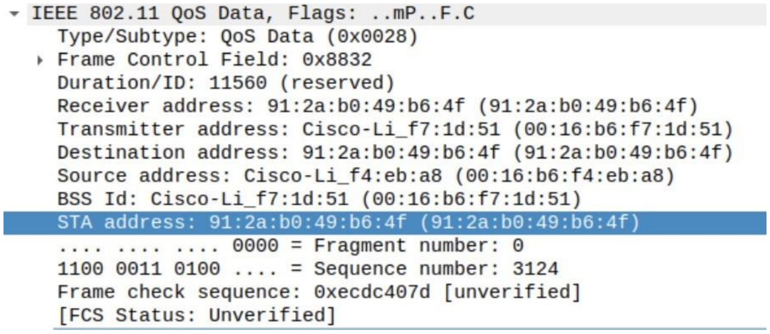


```
▸ Frame Control Field: 0x8801
  .000 0000 0010 1100 = Duration: 44 microseconds
  Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
  Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
  Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
  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
```

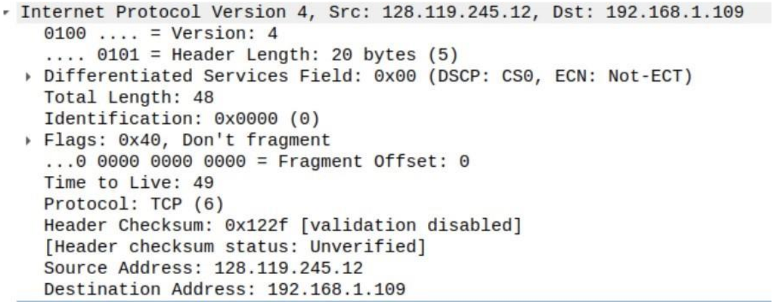


```
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 48
  Identification: 0x1324 (4900)
▸ Flags: 0x40, Don't fragment
  ...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
```

1. 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 is 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 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. It is essential to understand that the destination MAC address of the frame containing the SYN differs from the destination IP address of the IP packet contained within this frame.



```
▾ 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]
```



```
▾ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x0000 (0)
  ▸ Flags: 0x40, 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
```

2. The TCP SYN ACK is received at t = 24.827751 seconds into the trace. The MAC address for the sender of the 802.11 frames 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 is the host itself, is 91:2a:b0:49:b6:4f. (Curiously, this differs from the host's MAC address used in the frame that sends the TCP SYN. The host wireless interface behaves like it has two interface addresses). 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).

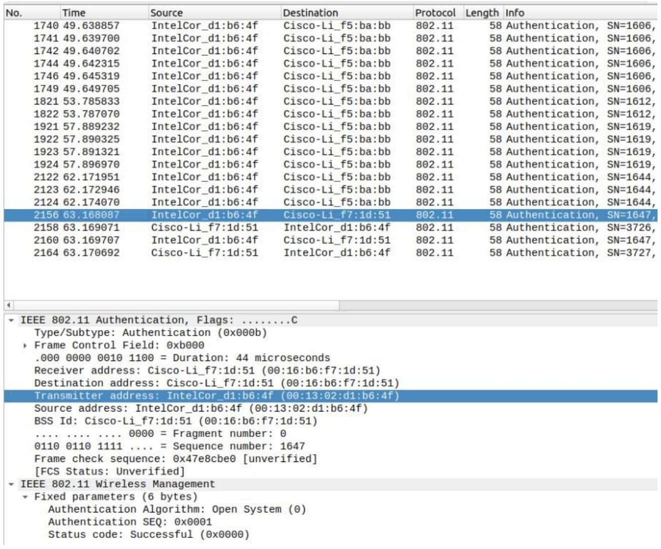
PART – 3

1) At t = 49.583615, the host sends a DHCP release to the DHCP server (whose IP address is 192.168.1.1) in the network 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.

2) The first AUTHENTICATION from the host to the AP is at t = 49.638857.
Around 6 authentication requests were sent to the requested access point.

3) The host requests that the association be open (by specifying Authentication Algorithm: Open System).

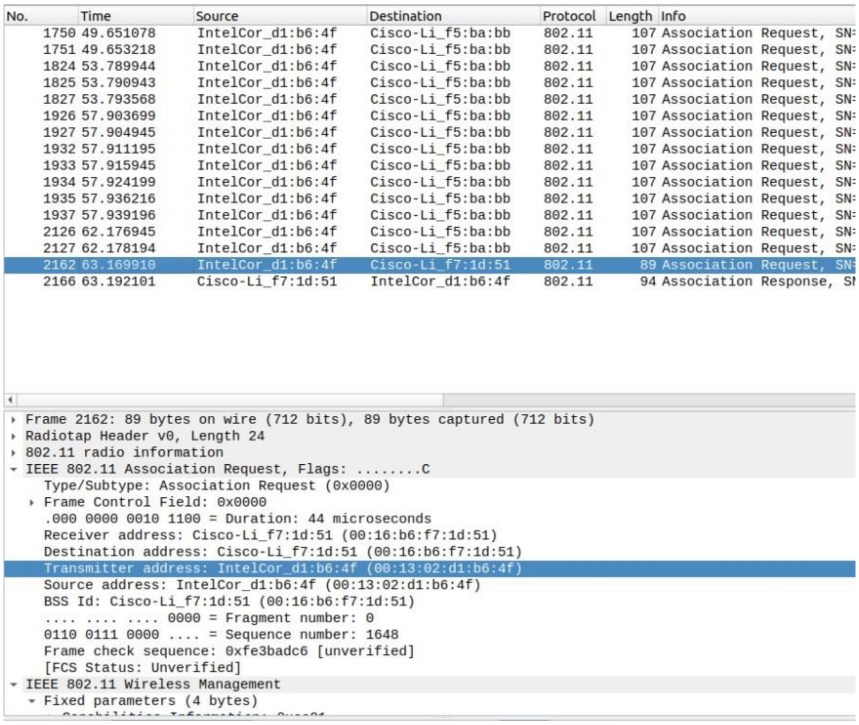
4) I can't find any reply from the AP. This is probably because the AP is configured to require a key when associating with that AP, so the AP is likely ignoring (i.e., not responding to) requests for open access



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,
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612,
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612,
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619,
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619,
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619,
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619,
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644,
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644,
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644,
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647,
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726,
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647,
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727,

```
▾ 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
    Frame check sequence: 0x47e8cbe0 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

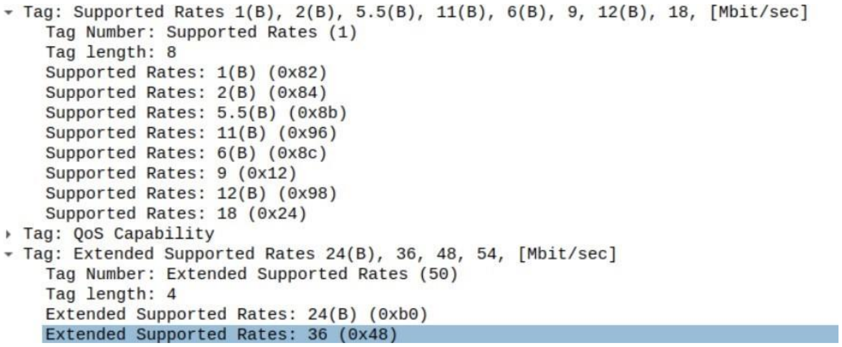
5) At t = 63.168087, an AUTHENTICATION frame was sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS). At t = 63.169071, an AUTHENTICATION is forwarded in the reverse direction from the BSS to the wireless host.



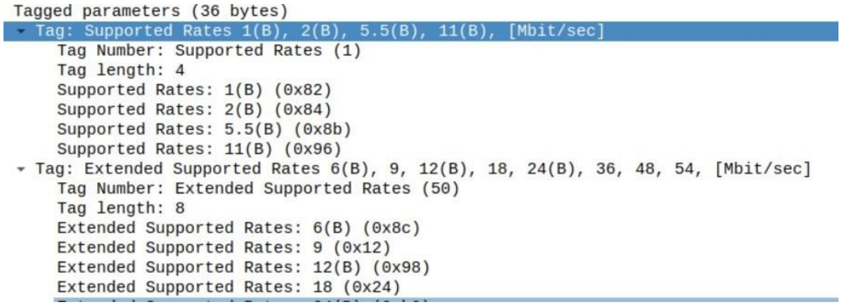
```
No.      Time       Source             Destination        Protocol Length Info
    1750 49.651078  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1751 49.653218  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1824 53.789944  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1825 53.790943  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1827 53.793568  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1926 57.903699  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1927 57.904945  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1932 57.911195  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1933 57.915945  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1934 57.924199  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1935 57.936216  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    1937 57.939196  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    2126 62.176945  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    2127 62.178194  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11     107 Association Request, SN=
    2162 63.169910  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51  802.11      89 Association Request, SN=
    2166 63.192101  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f  802.11      94 Association Response, SN
```

```
▸ 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
  ▾ Fixed parameters (4 bytes)
```

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



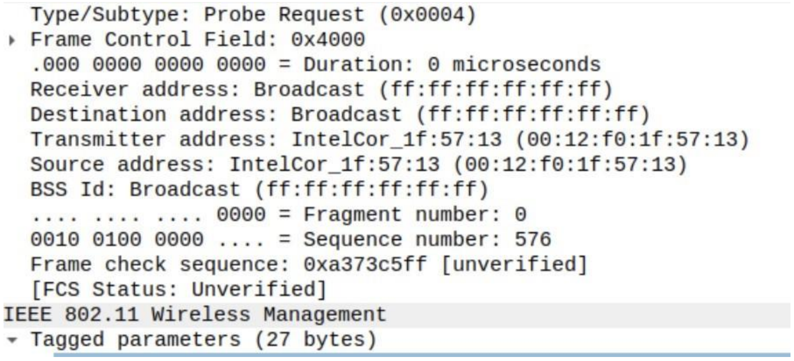
```
▾ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 8
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 11(B) (0x96)
    Supported Rates: 6(B) (0x8c)
    Supported Rates: 9 (0x12)
    Supported Rates: 12(B) (0x98)
    Supported Rates: 18 (0x24)
▸ Tag: QoS Capability
▾ Tag: 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)
```



```
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)
```

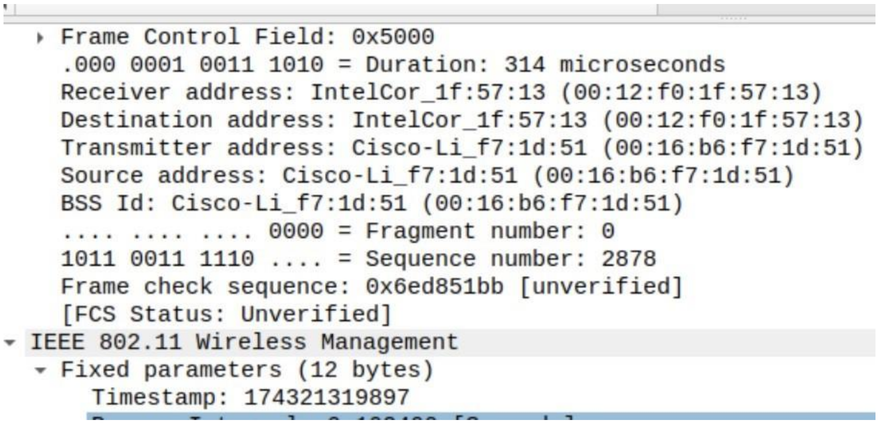
7) The supported rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps in the ASSOCIATION REQUEST frame. The same rates are advertised in the ASSOCIATION RESPONSE.

PART – 4



```
  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
▾ Tagged parameters (27 bytes)
```

1) 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, a PROBE RESPONSE was sent with source: 00:16:b6:f7:1d:51, destination and a BSSID of 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.



```
  ▸ 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
  ▾ Fixed parameters (12 bytes)
      Timestamp: 174321319897
```