Assignment 12: Wireshark Lab: 802.11 WiFi

210010020

Part1:

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

   A] .The two access points that are issuing most of the beacon frame have an SSID of “linksys12” and “30 Munroe St”.

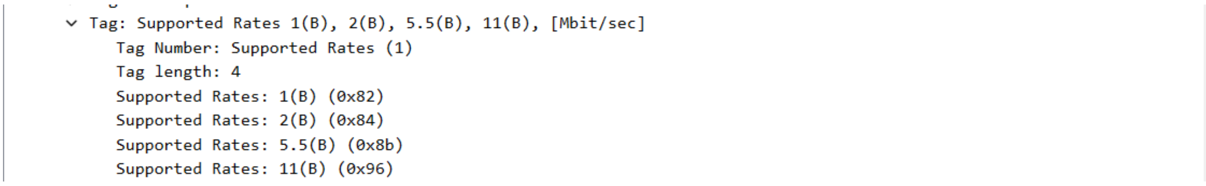
2. What are the beacon intervals in the *linksys_ses_24086* access point and the *30 Munroe St.* access point?
   A] Beacon Interval of the 802.11 wireless LAN Management frame as.**102400 seconds** for both the mentioned access points.

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).
   A] Source 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*??
   A] ff:ff:ff:ff:ff:ff this is the broadcast MAC Address of the beacon frame.

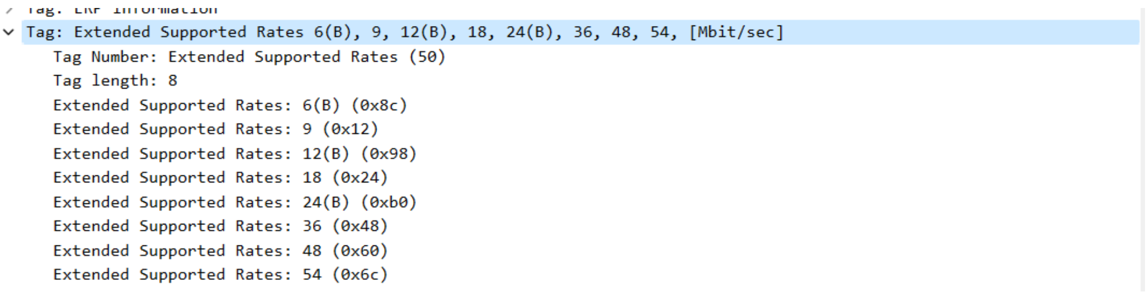
5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *30 Munroe St*?
   A] BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) same as the source address.

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?
   A]
   Data rates:



```
  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)
```

Extended supported rates:



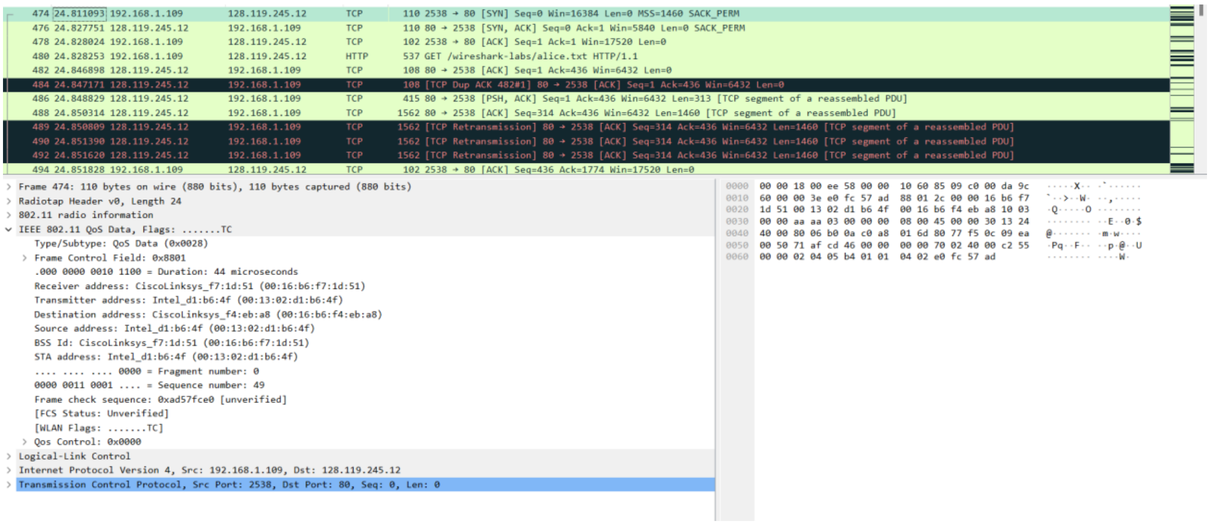
```
> Tag: ERP Information
v Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 8
    Extended Supported Rates: 6(B) (0x8c)
    Extended Supported Rates: 9 (0x12)
    Extended Supported Rates: 12(B) (0x98)
    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)
```

Part 2

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?

   A] The TCP SYN is sent at 24.81s. There are three addresses in the 802.11 frame: The

   - Transmitter address = **00:13:02:d1:b6:4f** this is the source address.
   - Receiver address = **00:16:b6:f7:1d:51**
   - MAC address for the destination, which the first hop router to which the host is connected, is **00:16:b6:f4:eb:a8.**
   - The MAC address for the BSS is 00:16:b6:f7:1d:51. The IP address of the host sending the TCP SYN is 192.168.1.109.
   - The IP address of wireless host sending TCP segment is 192.168.1.109 and that f destination is 128.119.245.12.



```
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
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
478 24.828024 192.168.1.109   128.119.245.12  TCP   102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
480 24.828253 192.168.1.109   128.119.245.12  HTTP  537 GET /wireshark-labs/alice.txt HTTP/1.1
482 24.846898 128.119.245.12  192.168.1.109   TCP   108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
484 24.847171 128.119.245.12  192.168.1.109   TCP   108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
486 24.848829 128.119.245.12  192.168.1.109   TCP   415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
488 24.850314 128.119.245.12  192.168.1.109   TCP  1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
489 24.850809 128.119.245.12  192.168.1.109   TCP  1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
490 24.851390 128.119.245.12  192.168.1.109   TCP  1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
492 24.851620 128.119.245.12  192.168.1.109   TCP  1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
494 24.851828 192.168.1.109   128.119.245.12  TCP   102 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
```

```
> Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: Intel_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]
    [WLAN Flags: .......TC]
  > Qos Control: 0x0000
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 00 18 00 ee 58 00 00  10 60 85 09 c0 00 da 9c   ·····X·· ·`······
0010  60 00 00 3e e0 fc 57 ad  88 01 2c 00 00 16 b6 f7   `··>··W· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 10 03   ·Q·····O ········
0030  00 00 aa aa 03 00 00 00  08 00 45 00 00 30 13 24   ········ ··E··0·$
0040  40 00 80 06 b0 0a c0 a8  01 6d 80 77 f5 0c 09 ea   @······· ·m·w····
0050  00 50 71 af cd 46 00 00  00 00 70 02 40 00 c2 55   ·Pq··F·· ··p·@··U
0060  00 00 02 04 05 b4 01 01  04 02 e0 fc 57 ad         ········ ····W·
```

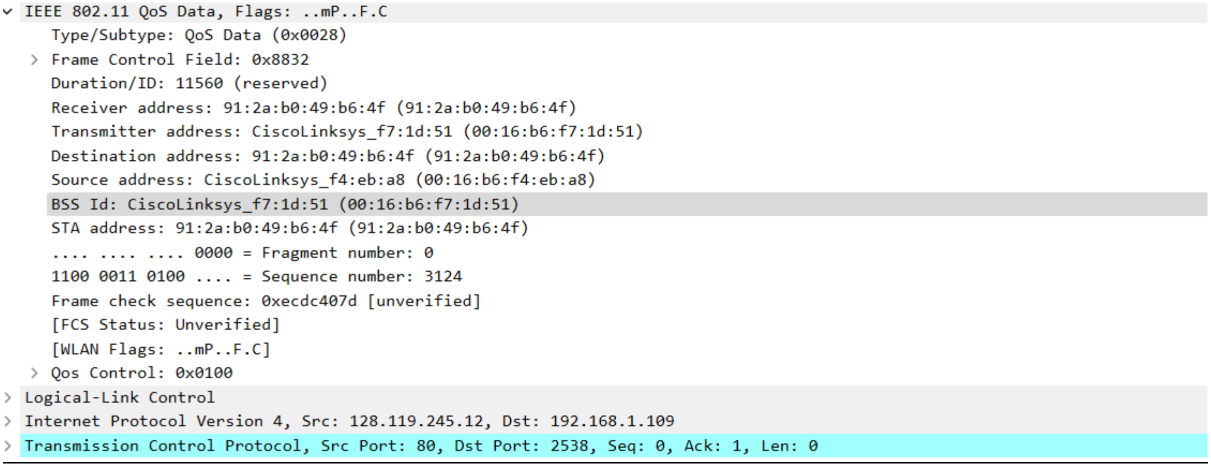
2. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which of these are the MAC addresses corresponding to the host sending SYNACK, destination and BSS? What is the IP address of the server sending the TCP SYNACK?

   A]

   - Sending address / source address : 00:16:b6:f4:eb:a8. Mac address of first hop router.

- destination address / receiver address : 91:2a:b0:49:b6:4f.
- BSS Id & Transmitter address: 00:16:b6:f7:1d:51

  IP address of server sending TCP SYN ACK: 128.119.245.12

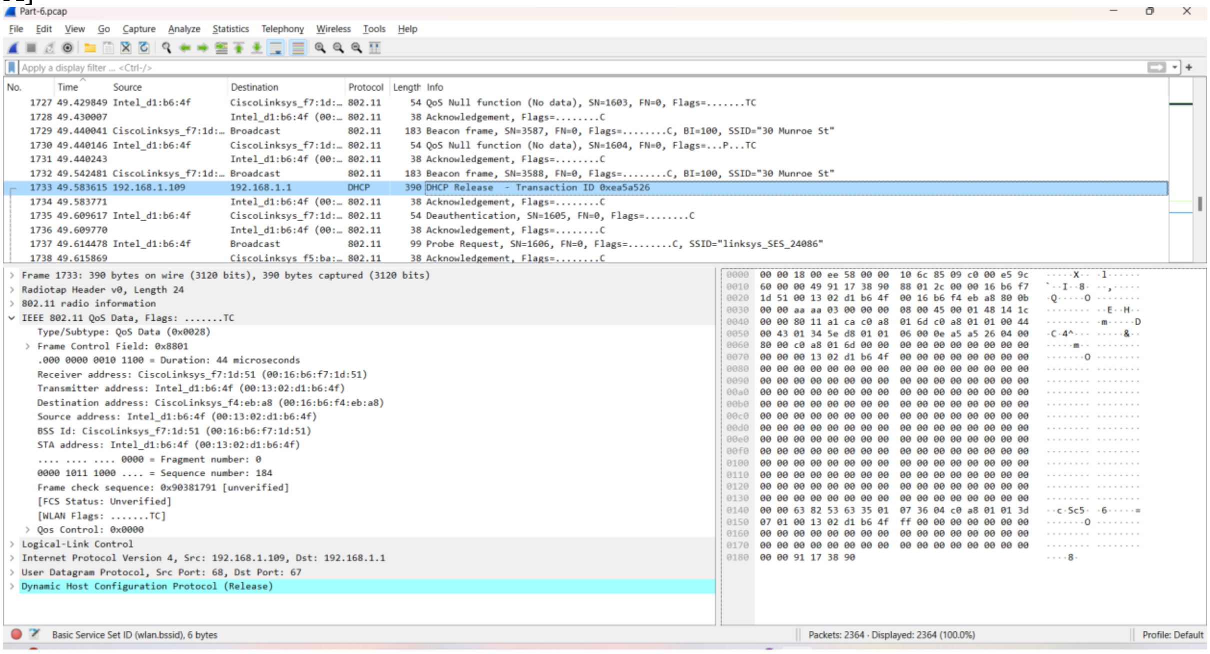


```
⌄ IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  › Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: CiscoLinksys_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]
    [WLAN Flags: ..mP..F.C]
  › 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
```

Part3:

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?

   A]



Part-6.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source                Destination           Protocol Length Info
 1727 49.429849 Intel_d1:b6:4f        CiscoLinksys_f7:1d:… 802.11    54 QoS Null function (No data), SN=1603, FN=0, Flags=.......TC
 1728 49.430007                       Intel_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=........C
 1729 49.440041 CiscoLinksys_f7:1d:… Broadcast             802.11   183 Beacon frame, SN=3587, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1730 49.440146 Intel_d1:b6:4f        CiscoLinksys_f7:1d:… 802.11    54 QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
 1731 49.440243                       Intel_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=........C
 1732 49.542481 CiscoLinksys_f7:1d:… Broadcast             802.11   183 Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1733 49.583615 192.168.1.109         192.168.1.1           DHCP     390 DHCP Release  - Transaction ID 0xea5a526
 1734 49.583771                       Intel_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=........C
 1735 49.609617 Intel_d1:b6:4f        CiscoLinksys_f7:1d:… 802.11    54 Deauthentication, SN=1605, FN=0, Flags=........C
 1736 49.609770                       Intel_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=........C
 1737 49.614478 Intel_d1:b6:4f        Broadcast             802.11    99 Probe Request, SN=1606, FN=0, Flags=........C, SSID="linksys_SES_24086"
 1738 49.615869                       CiscoLinksys_f5:ba:… 802.11    38 Acknowledgement, Flags=........C
```

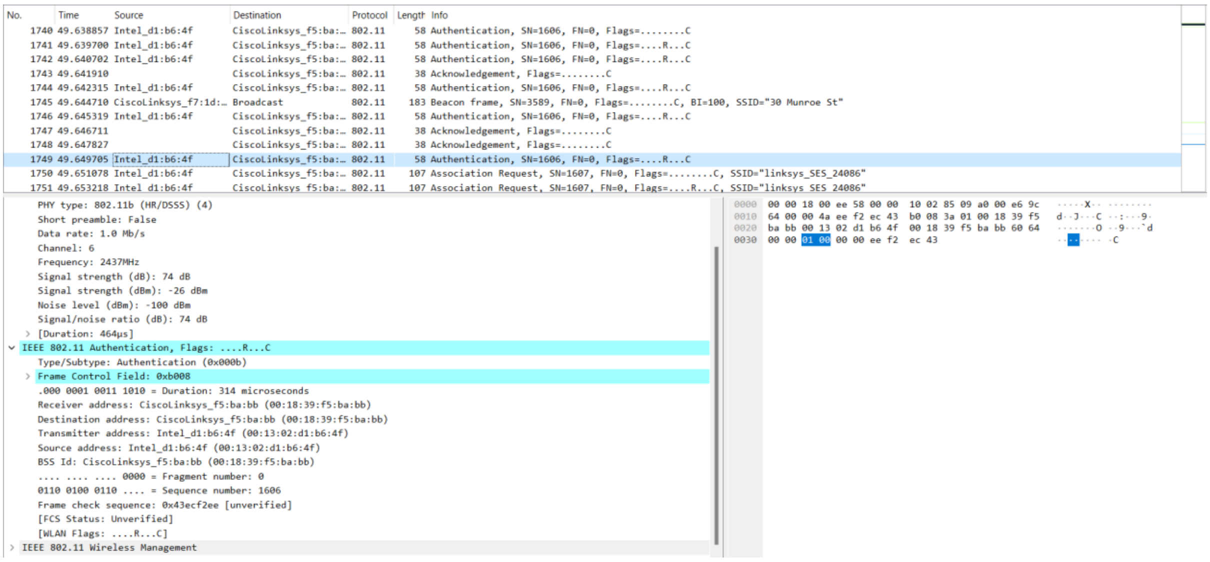
```
› Frame 1733: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits)
› Radiotap Header v0, Length 24
› 802.11 radio information
⌄ IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  › Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: Intel_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]
    [WLAN Flags: .......TC]
  › 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)
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e5 9c   .....X.. .l......
0010  60 00 00 49 91 17 38 90  88 01 2c 00 00 16 b6 f7   `..I..8. ..,.....
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 80 0b   .Q.....O ........
0030  00 00 aa aa 03 00 00 00  08 00 45 00 01 48 14 1c   ........ ..E..H..
0040  00 00 80 11 a1 ca c0 a8  01 6d c0 a8 01 01 00 44   ........ .m.....D
0050  00 43 01 34 5e d8 01 01  06 00 0e a5 a5 26 04 00   .C.4^... .....&..
0060  80 00 c0 a8 01 6d 00 00  00 00 00 00 00 00 00 00   .....m.. ........
0070  00 00 00 13 02 d1 b6 4f  00 00 00 00 00 00 00 00   .......O ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0140  00 00 63 82 53 63 35 01  07 36 04 c0 a8 01 01 3d   ..c.Sc5. .6.....=
0150  07 01 00 13 02 d1 b6 4f  ff 00 00 00 00 00 00 00   .......O ........
0160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0180  00 00 91 17 38 90                                  ....8.
```

Basic Service Set ID (wlan.bssid), 6 bytes | Packets: 2364 · Displayed: 2364 (100.0%) | Profile: Default

- At t=49.58 a DHCP release message is sent with an option as end to the server with IP address as can be seen in the UDP Dst: 192.168.1.1. The host is releasing its IP address back to the DHCP server, and is exiting the network.
- At t=49.609617, Deauthentication is done, to terminate a Wi-Fi Connection.
- Expected to observe a DISASSOCIATION request, but that is not observed here

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?*
   A] There are 6 AUTHENTICATION messages are sent from the wireless host to the linksys ses_24086. Note that the first AUTHENTICATION frame sent out successfully was observed to be at time t = 49.639705

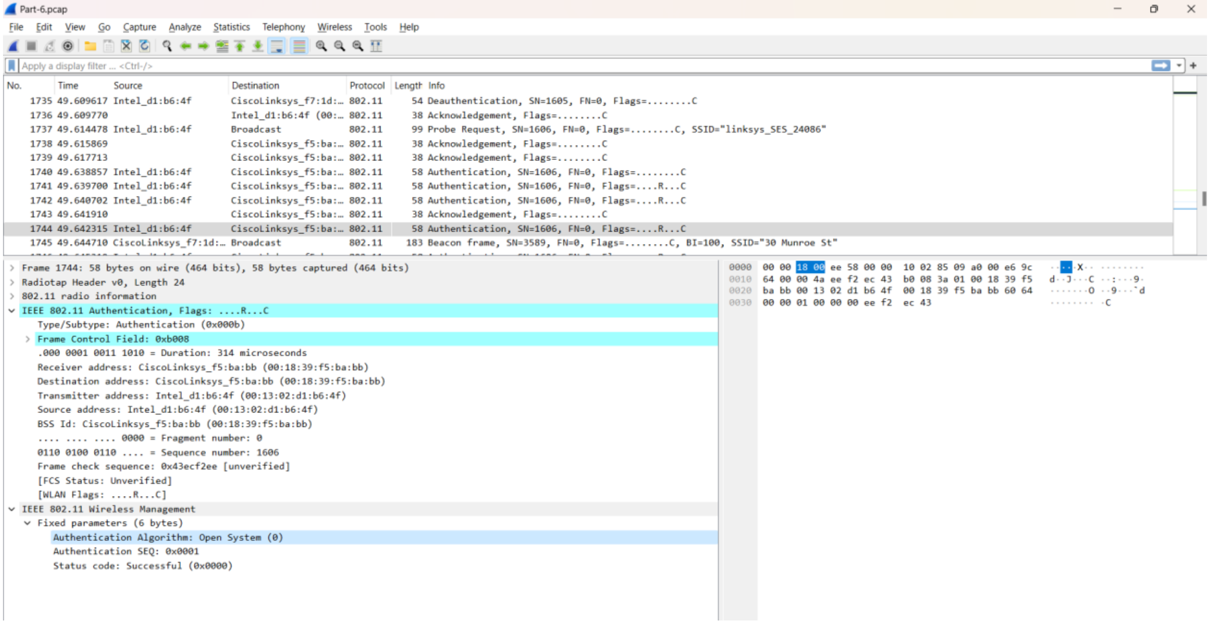


```
No.   Time      Source                Destination            Protocol Length Info
 1740 49.638857 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=........C
 1741 49.639700 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=....R...C
 1742 49.640702 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=....R...C
 1743 49.641910                       CiscoLinksys_f5:ba:…   802.11     38 Acknowledgement, Flags=........C
 1744 49.642315 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=....R...C
 1745 49.644710 CiscoLinksys_f7:1d:…  Broadcast              802.11    183 Beacon frame, SN=3589, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1746 49.645319 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=....R...C
 1747 49.646711                       CiscoLinksys_f5:ba:…   802.11     38 Acknowledgement, Flags=........C
 1748 49.647827                       CiscoLinksys_f5:ba:…   802.11     38 Acknowledgement, Flags=........C
 1749 49.649705 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=....R...C
 1750 49.651078 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11    107 Association Request, SN=1607, FN=0, Flags=........C, SSID="linksys_SES_24086"
 1751 49.653218 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11    107 Association Request, SN=1607, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
```

```
    PHY type: 802.11b (HR/DSSS) (4)
    Short preamble: False
    Data rate: 1.0 Mb/s
    Channel: 6
    Frequency: 2437MHz
    Signal strength (dB): 74 dB
    Signal strength (dBm): -26 dBm
    Noise level (dBm): -100 dBm
    Signal/noise ratio (dB): 74 dB
  > [Duration: 464µs]
v IEEE 802.11 Authentication, Flags: ....R...C
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb008
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    Destination address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    .... .... .... 0000 = Fragment number: 0
    0110 0100 0110 .... = Sequence number: 1606
    Frame check sequence: 0x43ecf2ee [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ....R...C]
> IEEE 802.11 Wireless Management
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e6 9c   ·····X·· ········
0010  64 00 00 4a ee f2 ec 43  b0 08 3a 01 00 18 39 f5   d··J···C ··:···9·
0020  ba bb 00 13 02 d1 b6 4f  00 18 39 f5 ba bb 60 64   ·······O ··9···`d
0030  00 00 01 00 00 00 ee f2  ec 43                     ········ ·C
```

3. Does the host want the authentication to require a key or be open?
   A] The host does not require any authentication key as it is open.



Part-6.pcap

```
No.   Time      Source                Destination            Protocol Length Info
 1735 49.609617 Intel_d1:b6:4f        CiscoLinksys_f7:1d:…   802.11     54 Deauthentication, SN=1605, FN=0, Flags=........C
 1736 49.609770                       Intel_d1:b6:4f (00:…   802.11     38 Acknowledgement, Flags=........C
 1737 49.614478 Intel_d1:b6:4f        Broadcast              802.11     99 Probe Request, SN=1606, FN=0, Flags=........C, SSID="linksys_SES_24086"
 1738 49.615869                       CiscoLinksys_f5:ba:…   802.11     38 Acknowledgement, Flags=........C
 1739 49.617713                       CiscoLinksys_f5:ba:…   802.11     38 Acknowledgement, Flags=........C
 1740 49.638857 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=........C
 1741 49.639700 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=....R...C
 1742 49.640702 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=....R...C
 1743 49.641910                       CiscoLinksys_f5:ba:…   802.11     38 Acknowledgement, Flags=........C
 1744 49.642315 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…   802.11     58 Authentication, SN=1606, FN=0, Flags=....R...C
 1745 49.644710 CiscoLinksys_f7:1d:…  Broadcast              802.11    183 Beacon frame, SN=3589, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
```

```
> Frame 1744: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Authentication, Flags: ....R...C
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb008
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    Destination address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    .... .... .... 0000 = Fragment number: 0
    0110 0100 0110 .... = Sequence number: 1606
    Frame check sequence: 0x43ecf2ee [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ....R...C]
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

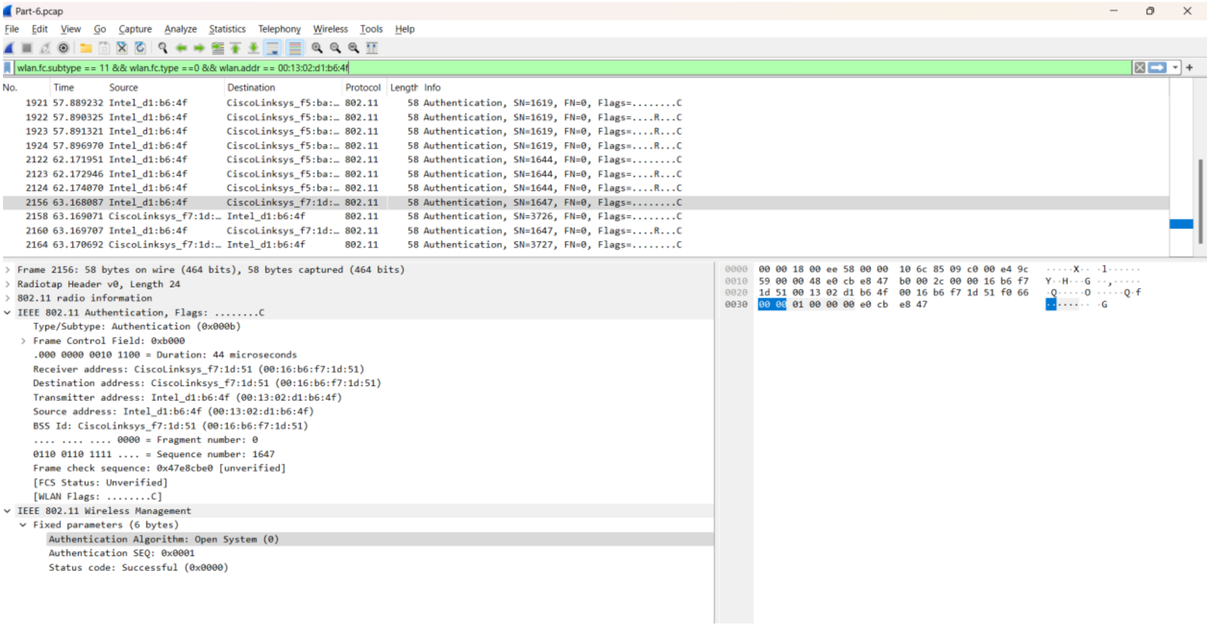
```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e6 9c   ·····X·· ········
0010  64 00 00 4a ee f2 ec 43  b0 08 3a 01 00 18 39 f5   d··J···C ··:···9·
0020  ba bb 00 13 02 d1 b6 4f  00 18 39 f5 ba bb 60 64   ·······O ··9···`d
0030  00 00 01 00 00 00 ee f2  ec 43                     ········ ·C
```

4. Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?
   A] No there is no reply that can be seen.

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 is there an AUTHENTICATION frame from the host to 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host reply? (Note that you can use the filter expression "wlan.fc.subtype == 11 && wlan.fc.type == 0 && wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

A]



```
wlan.fc.subtype == 11 && wlan.fc.type ==0 && wlan.addr == 00:13:02:d1:b6:4f
```

```
No.    Time      Source                Destination           Protocol Length Info
  1921 57.889232 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…  802.11     58 Authentication, SN=1619, FN=0, Flags=........C
  1922 57.890325 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…  802.11     58 Authentication, SN=1619, FN=0, Flags=....R...C
  1923 57.891321 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…  802.11     58 Authentication, SN=1619, FN=0, Flags=....R...C
  1924 57.896970 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…  802.11     58 Authentication, SN=1619, FN=0, Flags=....R...C
  2122 62.171951 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…  802.11     58 Authentication, SN=1644, FN=0, Flags=........C
  2123 62.172946 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…  802.11     58 Authentication, SN=1644, FN=0, Flags=....R...C
  2124 62.174070 Intel_d1:b6:4f        CiscoLinksys_f5:ba:…  802.11     58 Authentication, SN=1644, FN=0, Flags=....R...C
  2156 63.168087 Intel_d1:b6:4f        CiscoLinksys_f7:1d:…  802.11     58 Authentication, SN=1647, FN=0, Flags=........C
  2158 63.169071 CiscoLinksys_f7:1d:…  Intel_d1:b6:4f        802.11     58 Authentication, SN=3726, FN=0, Flags=........C
  2160 63.169707 Intel_d1:b6:4f        CiscoLinksys_f7:1d:…  802.11     58 Authentication, SN=1647, FN=0, Flags=....R...C
  2164 63.170692 CiscoLinksys_f7:1d:…  Intel_d1:b6:4f        802.11     58 Authentication, SN=3727, 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
v IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_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]
    [WLAN Flags: ........C]
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

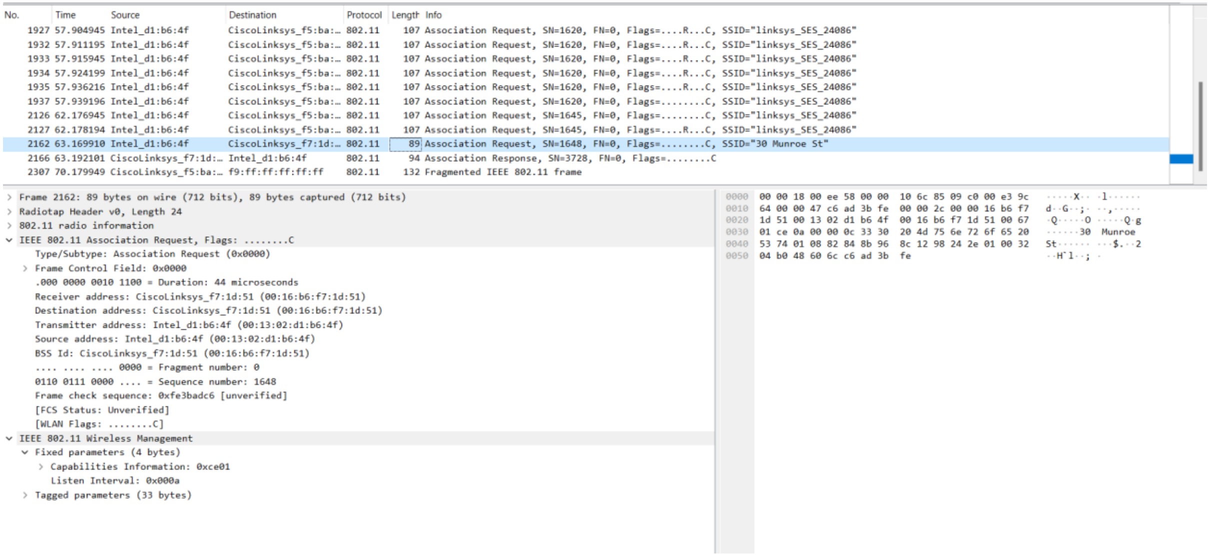
```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e4 9c   ·····X·· ·l······
0010  59 00 00 48 e0 cb e8 47  b0 00 2c 00 00 16 b6 f7   Y··H···G ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f7 1d 51 f0 66   ·Q·····O ·····Q·f
0030  00 00 01 00 00 00 e0 cb  e8 47                     ········ ·G
```

By using wlan.fc.subtype == 11 && wlan.fc.type ==0 && wlan.addr == 00:13:02:d1:b6:4f we can find that

- T = 63.169071s Authentication is sent from Host to 30 Munroe ST
- T = 63.1697007s Authentication comes from 30 Munroe St to Host

6. An ASSOCIATE REQUEST from the host to AP and a corresponding ASSOCIATE RESPONSE frame from AP to the host is used for the host to be associated with an AP. At what time is there an ASSOCIATE REQUEST from the host to 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression "wlan.fc.subtype < 2 && wlan.fc.type == 0 && wlan.addr == IntelCor_d1:b6:4f" to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

   A] 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.

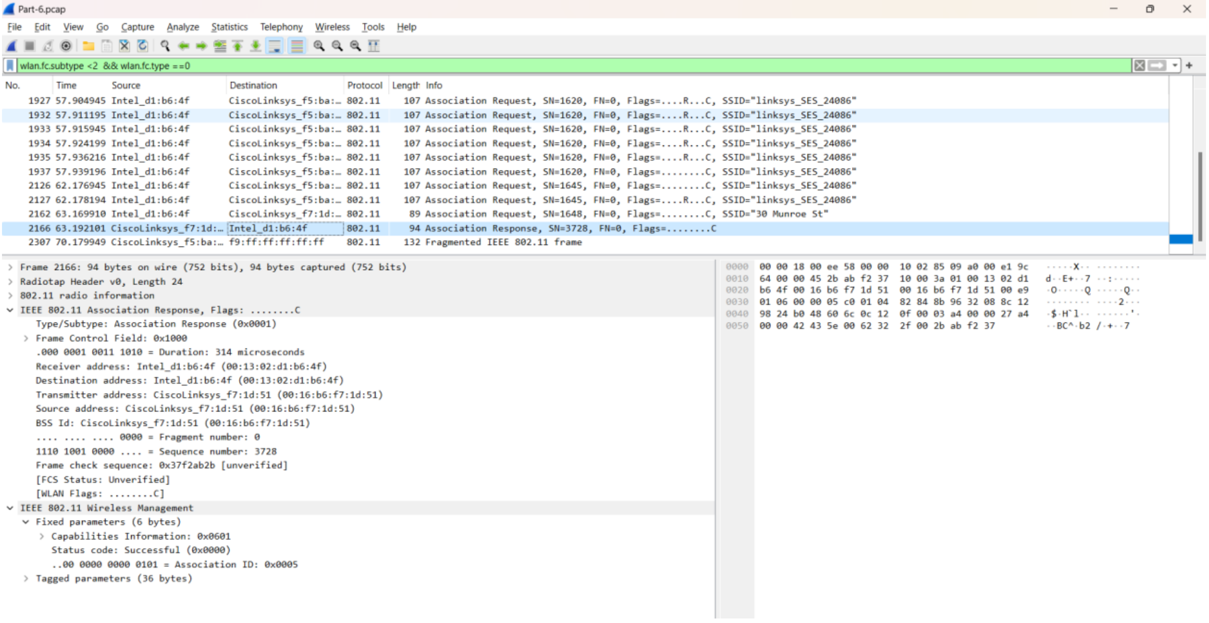


```
No.   Time      Source                 Destination            Protocol Length Info
 1927 57.904945 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1932 57.911195 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1933 57.915945 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1934 57.924199 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1935 57.936216 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1937 57.939196 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
 2126 62.176945 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24086"
 2127 62.178194 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 2162 63.169910 Intel_d1:b6:4f         CiscoLinksys_f7:1d:… 802.11    89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
 2166 63.192101 CiscoLinksys_f7:1d:… Intel_d1:b6:4f         802.11    94 Association Response, SN=3728, FN=0, Flags=........C
 2307 70.179949 CiscoLinksys_f5:ba:… f9:ff:ff:ff:ff:ff      802.11   132 Fragmented IEEE 802.11 frame
```

```
> Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  > Frame Control Field: 0x0000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_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]
    [WLAN Flags: ........C]
v IEEE 802.11 Wireless Management
  v Fixed parameters (4 bytes)
    > Capabilities Information: 0xce01
      Listen Interval: 0x000a
  > Tagged parameters (33 bytes)
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e3 9c   ·····X·· ·l······
0010  64 00 00 47 c6 ad 3b fe  00 00 2c 00 00 16 b6 f7   d··G··;· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f7 1d 51 00 67   ·Q·····O ·····Q·g
0030  01 ce 0a 00 00 0c 33 30  20 4d 75 6e 72 6f 65 20   ······30  Munroe
0040  53 74 01 08 82 84 8b 96  8c 12 98 24 2e 01 00 32   St······ ···$.··2
0050  04 b0 48 60 6c c6 ad 3b  fe                        ··H`l··; ·
```

Rates given in response:


Part-6.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

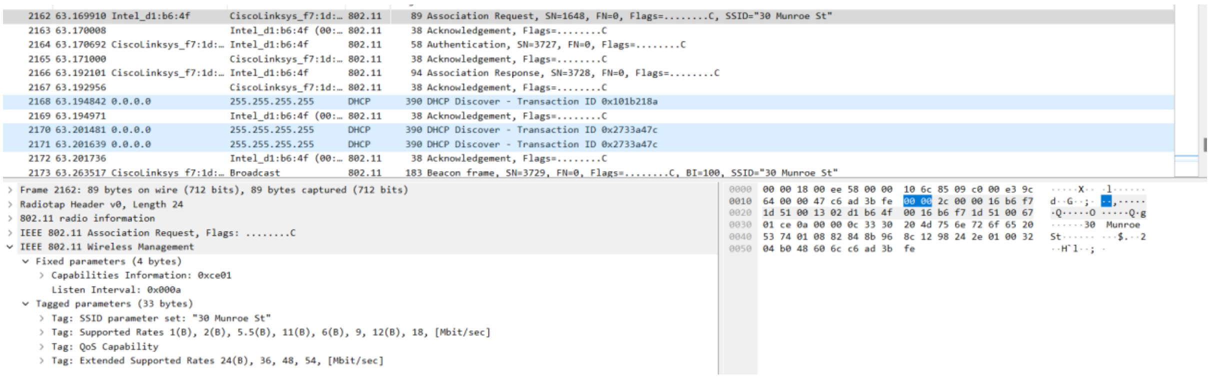
```
wlan.fc.subtype <2  && wlan.fc.type ==0
```

```
No.   Time      Source                 Destination            Protocol Length Info
 1927 57.904945 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1932 57.911195 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1933 57.915945 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1934 57.924199 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1935 57.936216 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 1937 57.939196 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
 2126 62.176945 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24086"
 2127 62.178194 Intel_d1:b6:4f         CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
 2162 63.169910 Intel_d1:b6:4f         CiscoLinksys_f7:1d:… 802.11    89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
 2166 63.192101 CiscoLinksys_f7:1d:… Intel_d1:b6:4f         802.11    94 Association Response, SN=3728, FN=0, Flags=........C
 2307 70.179949 CiscoLinksys_f5:ba:… f9:ff:ff:ff:ff:ff      802.11   132 Fragmented IEEE 802.11 frame
```

```
> Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Association Response, Flags: ........C
    Type/Subtype: Association Response (0x0001)
  > Frame Control Field: 0x1000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: CiscoLinksys_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]
    [WLAN Flags: ........C]
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
    > Capabilities Information: 0x0601
      Status code: Successful (0x0000)
      ..00 0000 0000 0101 = Association ID: 0x0005
  > Tagged parameters (36 bytes)
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e1 9c   ·····X·· ········
0010  64 00 00 45 2b ab f2 37  10 00 3a 01 00 13 02 d1   d··E+··7 ··:·····
0020  b6 4f 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 00 e9   ·O·····Q ·····Q··
0030  01 06 00 00 05 c0 01 04  82 84 8b 96 32 08 8c 12   ········ ····2···
0040  98 24 b0 48 60 6c 0c 12  0f 00 03 a4 00 00 27 a4   ·$·H`l·· ······'·
0050  00 00 42 43 5e 00 62 32  2f 00 2b ab f2 37         ··BC^·b2 /·+··7
```

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 A]
A] Supported transmission rates and extended transmission rates can be seen here.



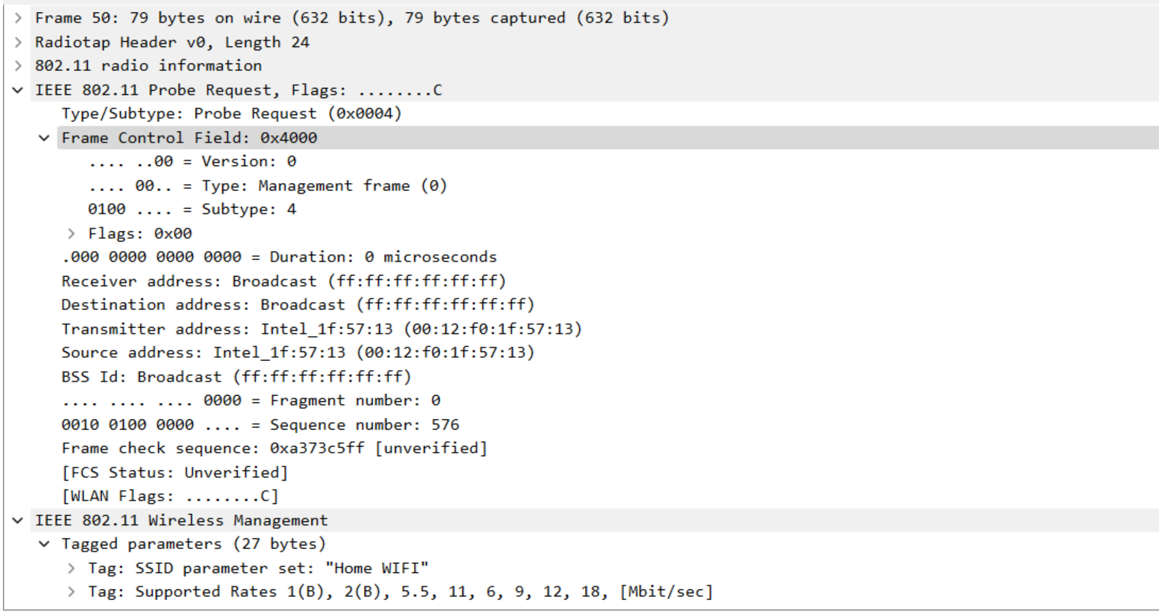
```
 2162 63.169910 Intel_d1:b6:4f         CiscoLinksys_f7:1d:… 802.11    89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
 2163 63.170008                        Intel_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=........C
 2164 63.170692 CiscoLinksys_f7:1d:… Intel_d1:b6:4f         802.11    58 Authentication, SN=3727, FN=0, Flags=........C
 2165 63.171000                        CiscoLinksys_f7:1d:… 802.11    38 Acknowledgement, Flags=........C
 2166 63.192101 CiscoLinksys_f7:1d:… Intel_d1:b6:4f         802.11    94 Association Response, SN=3728, FN=0, Flags=........C
 2167 63.192956                        CiscoLinksys_f7:1d:… 802.11    38 Acknowledgement, Flags=........C
 2168 63.194842 0.0.0.0                255.255.255.255        DHCP     390 DHCP Discover - Transaction ID 0x101b218a
 2169 63.194971                        Intel_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=........C
 2170 63.201481 0.0.0.0                255.255.255.255        DHCP     390 DHCP Discover - Transaction ID 0x2733a47c
 2171 63.201639 0.0.0.0                255.255.255.255        DHCP     390 DHCP Discover - Transaction ID 0x2733a47c
 2172 63.201736                        Intel_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=........C
 2173 63.263517 CiscoLinksys_f7:1d:… Broadcast              802.11   183 Beacon frame, SN=3729, FN=0, Flags=........C, BI=100, 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
v IEEE 802.11 Wireless Management
  v Fixed parameters (4 bytes)
    > Capabilities Information: 0xce01
      Listen Interval: 0x000a
  v Tagged parameters (33 bytes)
    > Tag: SSID parameter set: "30 Munroe St"
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    > Tag: QoS Capability
    > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e3 9c   ·····X·· ·l······
0010  64 00 00 47 c6 ad 3b fe  00 00 2c 00 00 16 b6 f7   d··G··;· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f7 1d 51 00 67   ·Q·····O ·····Q·g
0030  01 ce 0a 00 00 0c 33 30  20 4d 75 6e 72 6f 65 20   ······30  Munroe
0040  53 74 01 08 82 84 8b 96  8c 12 98 24 2e 01 00 32   St······ ···$.··2
0050  04 b0 48 60 6c c6 ad 3b  fe                        ··H`l··; ·
```

Part-4: Other Frame types

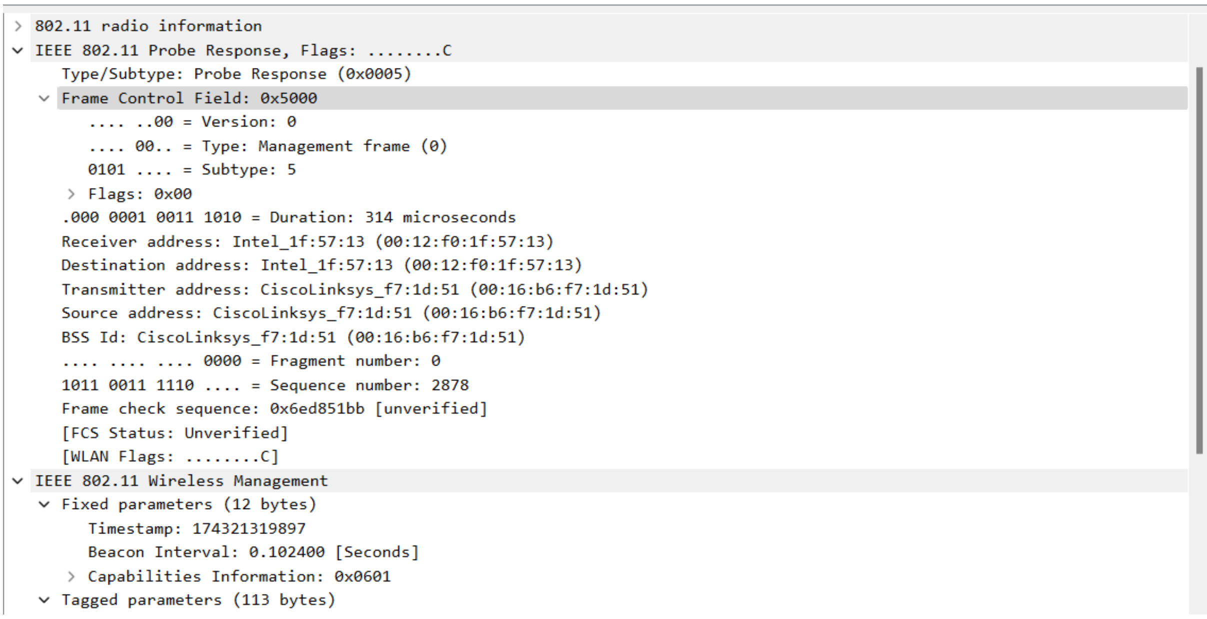
1. Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames. 1. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?
   A] Probe request:
   • Sender MAC address: 00:12:f0:1f:57:13 , which is the source address.
   • Receiver MAC address: ff:ff:ff:ff:ff:ff , which is the Ethernet broadcast address.
   • BSS ID MAC address: ff:ff:ff:ff:ff:ff , which is the Ethernet broadcast address



```
> Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  v Frame Control Field: 0x4000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0100 .... = Subtype: 4
    > Flags: 0x00
    .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: Intel_1f:57:13 (00:12:f0:1f:57:13)
    Source address: Intel_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]
    [WLAN Flags: ........C]
v IEEE 802.11 Wireless Management
  v Tagged parameters (27 bytes)
    > Tag: SSID parameter set: "Home WIFI"
    > Tag: Supported Rates 1(B), 2(B), 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
```

Probe Response:

- Sender MAC address: 00:16:b6:f7:1d:51 , which is the source address.
- Receiver MAC address: 00:12:f0:1f:57:13 , which is as seen in the Receiver Address field.
- BSS ID MAC address: 00:16:b6:f7:1d:51 , which is the as seen in the BSS ID field.



```
›  802.11 radio information
⌄  IEEE 802.11 Probe Response, Flags: ........C
      Type/Subtype: Probe Response (0x0005)
   ⌄  Frame Control Field: 0x5000
         .... ..00 = Version: 0
         .... 00.. = Type: Management frame (0)
         0101 .... = Subtype: 5
      ›  Flags: 0x00
      .000 0001 0011 1010 = Duration: 314 microseconds
      Receiver address: Intel_1f:57:13 (00:12:f0:1f:57:13)
      Destination address: Intel_1f:57:13 (00:12:f0:1f:57:13)
      Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
      Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
      BSS Id: CiscoLinksys_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]
      [WLAN Flags: ........C]
⌄  IEEE 802.11 Wireless Management
   ⌄  Fixed parameters (12 bytes)
         Timestamp: 174321319897
         Beacon Interval: 0.102400 [Seconds]
      ›  Capabilities Information: 0x0601
   ⌄  Tagged parameters (113 bytes)
```