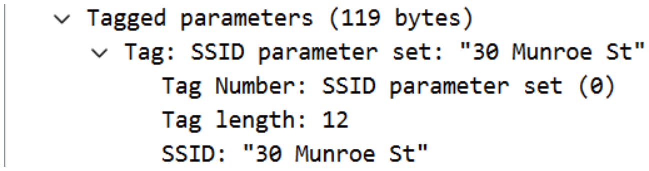
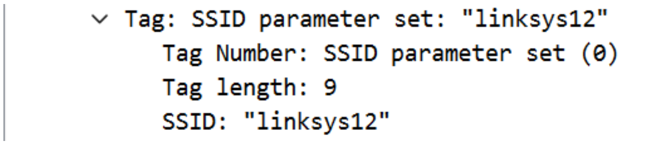
Assignment 12

Part-1

1. The SSIDs of the two access points that are issuing most of the beacon frames in this trace are **30 Munroe St** and **linksys12**.

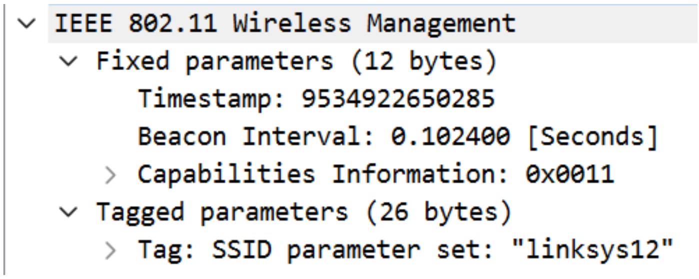


```
  ∨ Tagged parameters (119 bytes)
    ∨ Tag: SSID parameter set: "30 Munroe St"
        Tag Number: SSID parameter set (0)
        Tag length: 12
        SSID: "30 Munroe St"
```



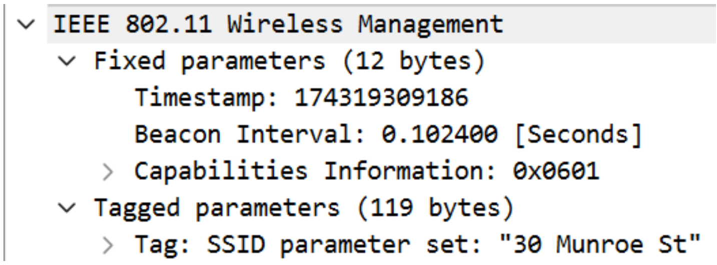
```
    ∨ Tag: SSID parameter set: "linksys12"
        Tag Number: SSID parameter set (0)
        Tag length: 9
        SSID: "linksys12"
```

2. The interval of time between the transmissions of the beacon frames and the linksys_ses_24086 access point is: **0.102400 seconds**



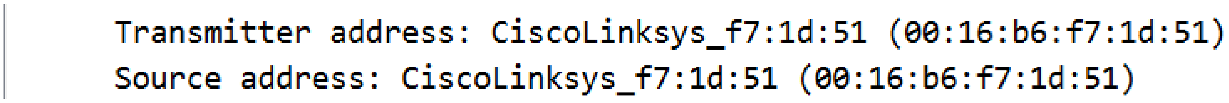
```
∨ IEEE 802.11 Wireless Management
  ∨ Fixed parameters (12 bytes)
      Timestamp: 9534922650285
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0011
  ∨ Tagged parameters (26 bytes)
    > Tag: SSID parameter set: "linksys12"
```

From the 30 Munroe St. access point: **0.102400 seconds**



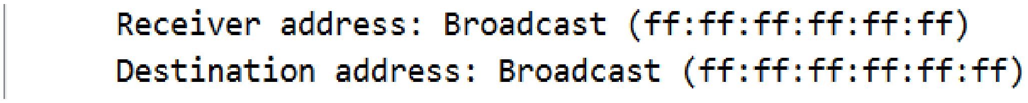
```
∨ IEEE 802.11 Wireless Management
  ∨ Fixed parameters (12 bytes)
      Timestamp: 174319309186
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  ∨ Tagged parameters (119 bytes)
    > Tag: SSID parameter set: "30 Munroe St"
```

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



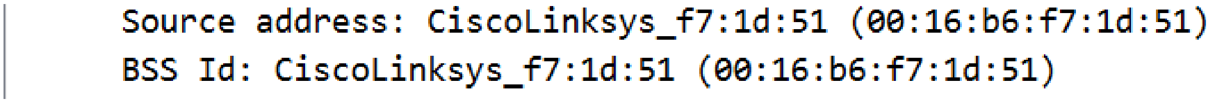
```
    Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

4. The destination MAC address in hexadecimal notation on the beacon frame from 30 Munroe St is: **ff:ff:ff:ff:ff:ff**



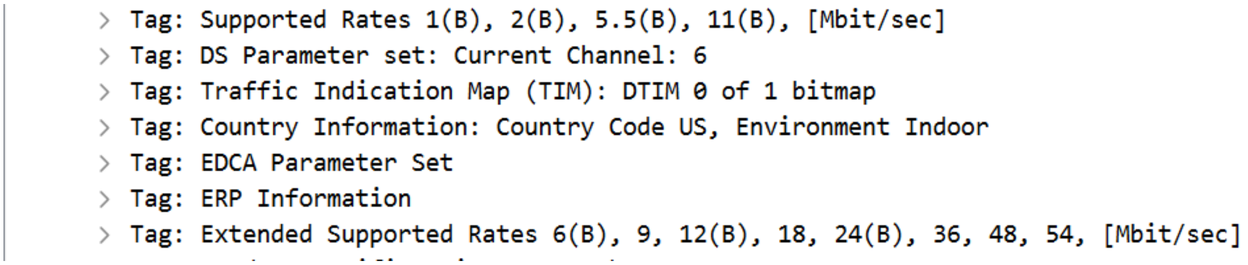
```
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
```

5. The MAC BSS ID in hexadecimal notation on the beacon frame from 30 Munroe St is: **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)
```

6. Supported rates: **1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]**
Extended supported rates: **6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]**

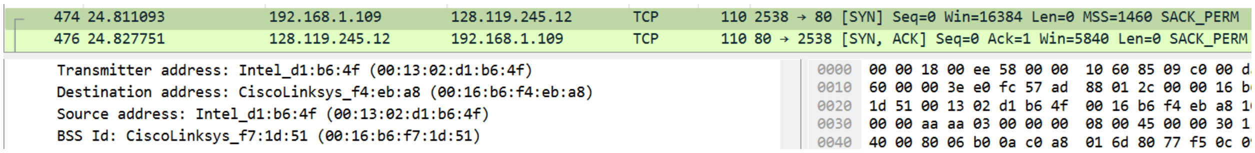


```
> Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
> Tag: DS Parameter set: Current Channel: 6
> Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
> Tag: Country Information: Country Code US, Environment Indoor
> Tag: EDCA Parameter Set
> Tag: ERP Information
> Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
```

Part-2

1. The 3 MAC addresses fields in the 802.11 frame are:

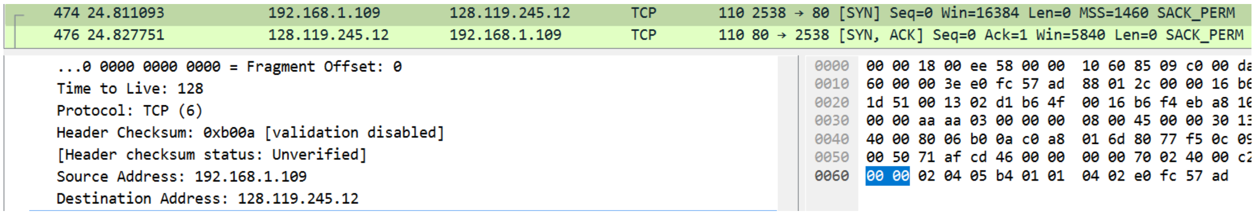
- Source Address: **00:13:02:d1:b6:4f**
  The Source address corresponds to the host device.
- Destination Address: **00:16:b6:f4:eb:a8**
  The Destination address corresponds to the first-hop device.
- BSS ID: **00:16:b6:f7:1d:51**
  The BSS ID corresponds to the access point.



```
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

    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)          0000  00 00 18 00 ee 58 00 00  10 60 85 09 c0 00 d
    Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)   0010  60 00 00 3e e0 fc 57 ad  88 01 2c 00 00 16 b
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)               0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 1
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)                0030  00 00 aa aa 03 00 00 00  08 00 45 00 00 30 1
                                                                     0040  40 00 80 06 b0 0a c0 a8  01 6d 80 77 f5 0c 0
```

- Source IP address: **192.168.1.109**
  Source IP address corresponds to the host address.
- Destination IP address: **128.119.245.12**
  Destination address corresponds to the server.

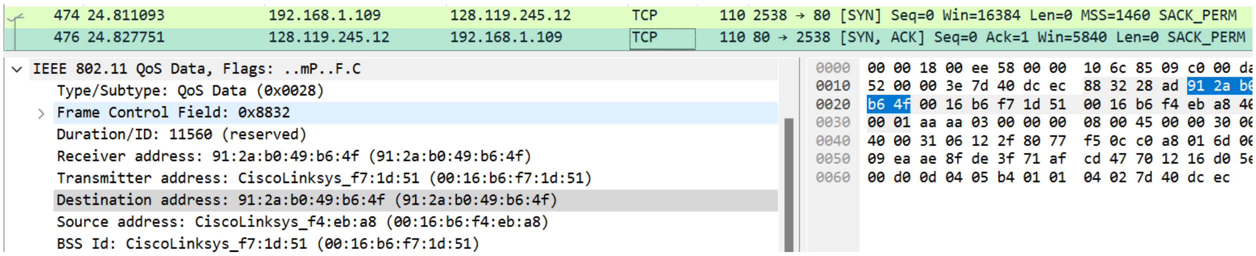


```
474 24.811093   192.168.1.109   128.119.245.12   TCP   110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
476 24.827751   128.119.245.12  192.168.1.109    TCP   110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM

    ...0 0000 0000 0000 = Fragment Offset: 0                0000  00 00 18 00 ee 58 00 00  10 60 85 09 c0 00 da
    Time to Live: 128                                        0010  60 00 00 3e e0 fc 57 ad  88 01 2c 00 00 16 b6
    Protocol: TCP (6)                                        0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 16
    Header Checksum: 0xb00a [validation disabled]            0030  00 00 aa aa 03 00 00 00  08 00 45 00 00 30 13
    [Header checksum status: Unverified]                     0040  40 00 80 06 b0 0a c0 a8  01 6d 80 77 f5 0c 09
    Source Address: 192.168.1.109                            0050  00 50 71 af cd 46 00 00  00 00 70 02 40 00 c2
    Destination Address: 128.119.245.12                      0060  00 00 02 04 05 b4 01 01  04 02 e0 fc 57 ad
```

2. The 3 MAC addresses fields in this 802.11 frames are:

- Source Address: **00:16:b6:f4:eb:a8**
  The source address corresponds to the first-hop device.
- Destination Address: **91:2a:b0:49:b6:4f**
  The destination address corresponds to the host device.
- BSS ID: **00:16:b6:f7:1d:51**
  The BSS ID corresponds to the access point.



```
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
```

```
∨ 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)
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 da
0010  52 00 00 3e 7d 40 dc ec  88 32 28 ad 91 2a b6
0020  b6 4f 00 16 b6 f7 1d 51  00 16 b6 f4 eb a8 40
0030  00 01 aa aa 03 00 00 00  08 00 45 00 00 30 06
0040  40 00 31 06 12 2f 80 77  f5 0c c0 a8 01 6d 06
0050  09 ea ae 8f de 3f 71 af  cd 47 70 12 16 d0 5e
0060  00 d0 0d 04 05 b4 01 01  04 02 7d 40 dc ec
```

Source IP address: **128.199.245.12**

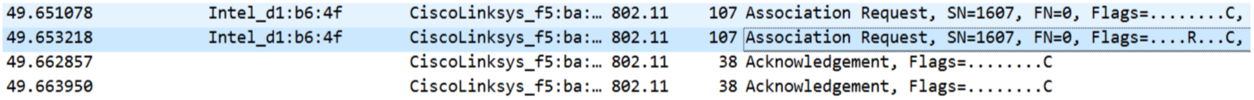
Destination IP address: **192.168.1.109**

Part-3

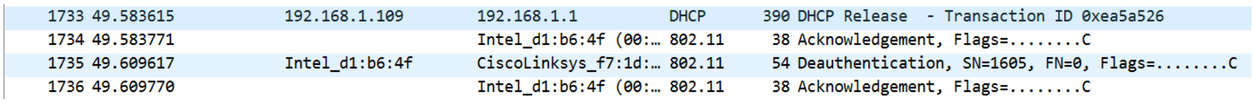
1. At t = 49.583615 a **DHCP** release is sent by the host to the DHCP server in the network that the host is leaving.

At t = 49.609617, the host sends a **Deauthentication** frame

One might have expected to see a **Disassociation** request to have been sent.



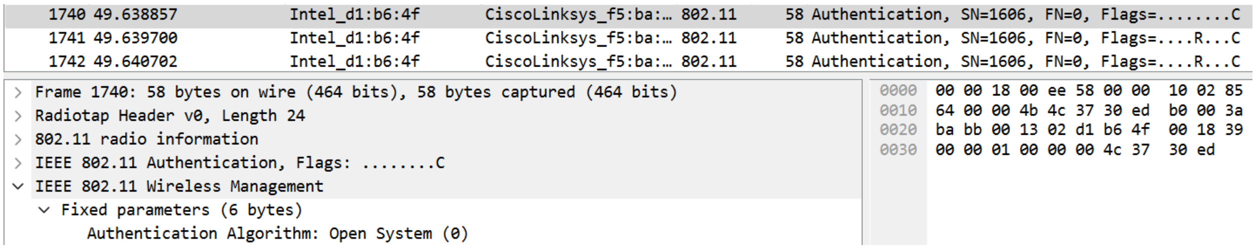
```
49.651078   Intel_d1:b6:4f   CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1607, FN=0, Flags=........C,
49.653218   Intel_d1:b6:4f   CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1607, FN=0, Flags=....R...C,
49.662857                    CiscoLinksys_f5:ba:… 802.11    38 Acknowledgement, Flags=........C
49.663950                    CiscoLinksys_f5:ba:… 802.11    38 Acknowledgement, Flags=........C
```



```
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
```

2. Total **17 Authentication** messages were sent from the wireless host to the linksys_ses_24086 AP.

3. The host is requesting that the association be **open** (by specifying Authentication Algorithm: Open System (0)).



```
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
```

```
> Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: ........C
∨ IEEE 802.11 Wireless Management
  ∨ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
```

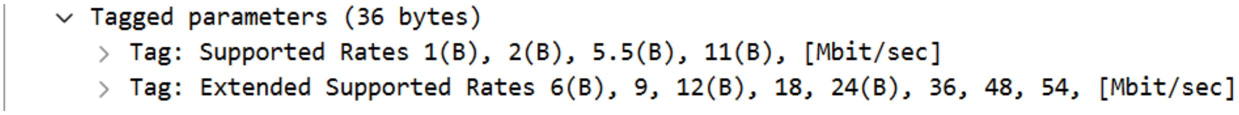
```
0000  00 00 18 00 ee 58 00 00  10 02 85
0010  64 00 00 4b 4c 37 30 ed  b0 00 3a
0020  ba bb 00 13 02 d1 b6 4f  00 18 39
0030  00 00 01 00 00 00 4c 37  30 ed
```

4. No, there is no reply from the AP. The AP is probably ignoring requests for open access (i.e. not responding to them) because it is set up to require a key when connecting to that AP.

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

6. The wireless host at **00:13:02:d1:b6:4f** sends an **Association Request** frame **to 00:16:b7:f7:1d:51** at time **t = 63.169910** (the BSS). On the reverse route, from the BSS to the wireless host, an **Association Response** is sent at time **t = 63.192101**.

7. The supported rates are listed as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps in the Association Request frame. The Association Response also lists the same rates.



```
∨ 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]
```

Part-4

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 **BSS ID: ff:ff:ff:ff:ff:ff**.
At **t=2.300697** there is a Probe response sent with **source: 00:16:b6:f7:1d:51**, **destination: 00:16:b6:f7:1d:51** and a **BSS ID: 00:16:b6:f7:1d:51**.
During active scanning, a host locates an Access Point by sending a Probe request as broadcast. The access point responds to the host making the request, by issuing a Probe response.