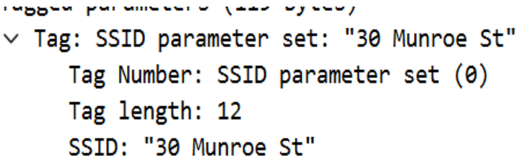
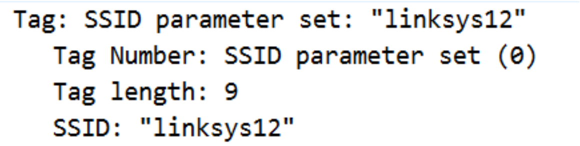
CS-315 COMPUTER NETWORKS LAB-12 (WIFI)

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.

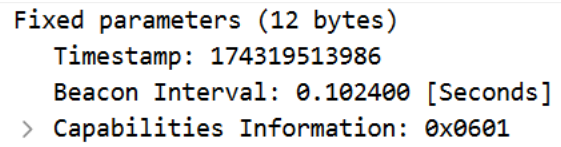


```
∨ Tag: SSID parameter set: "30 Munroe St"
      Tag Number: SSID parameter set (0)
      Tag length: 12
      SSID: "30 Munroe St"
```

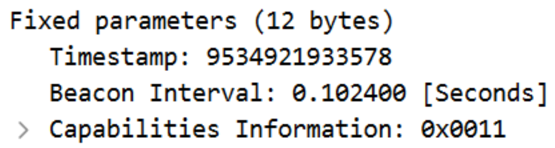


```
Tag: SSID parameter set: "linksys12"
   Tag Number: SSID parameter set (0)
   Tag length: 9
   SSID: "linksys12"
```

2. The beacon interval in the linksys_ses_24086 access point is 0.102400 seconds. The beacon interval in the 30 Munroe St. access point also is 0.102400 seconds.

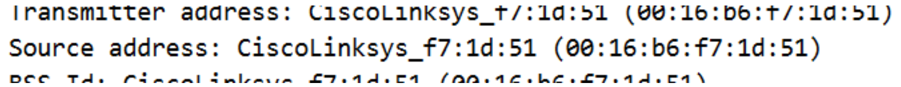


```
Fixed parameters (12 bytes)
   Timestamp: 174319513986
   Beacon Interval: 0.102400 [Seconds]
 › Capabilities Information: 0x0601
```



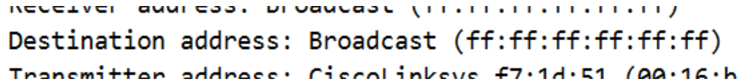
```
Fixed parameters (12 bytes)
   Timestamp: 9534921933578
   Beacon Interval: 0.102400 [Seconds]
 › Capabilities Information: 0x0011
```

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



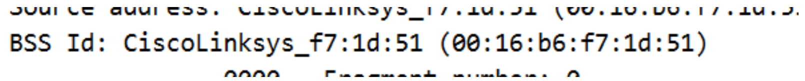
```
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

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



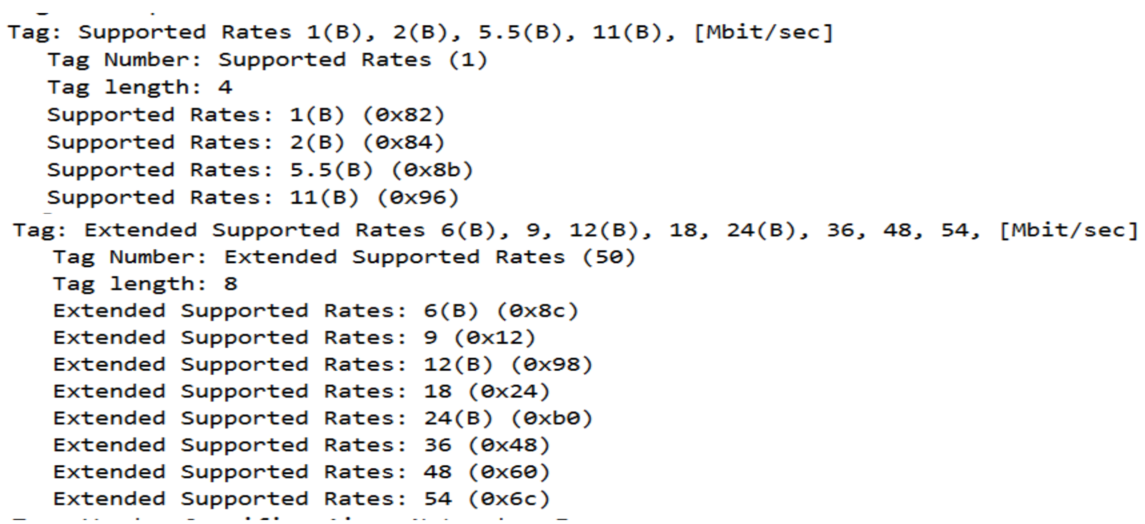
```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6
```

5. The MAC BSS ID 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:5
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

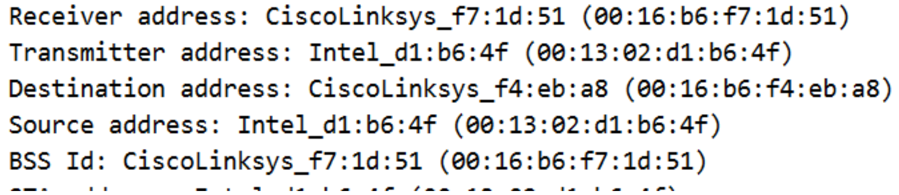
6. Supported Rates: 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec] Extended Supported Rates: 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]. These rates represent the data rates at which the access point can communicate with wireless devices. The "B" designation indicates that these rates are as per the 802.11b standard.



```
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)
```

Part-2:

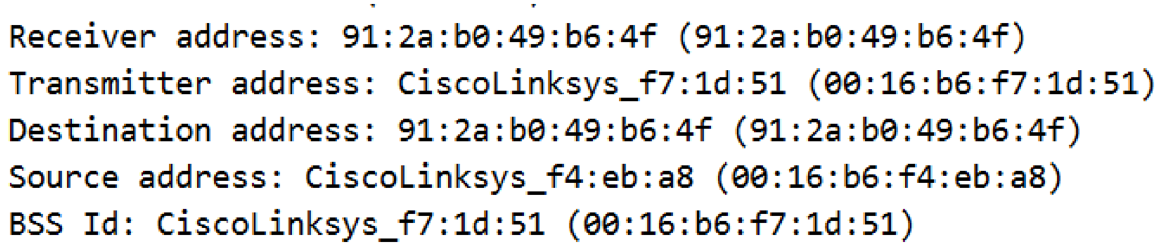
1. The 3 MAC address fields in the 802.11 frame are:
   Source address: 00:13:02:d1:b6:4f
   Destination address: 00:16:b6:f4:eb:a8
   BSS Id: 00:16:b6:f7:1d:51

   ```
   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)
   ```

   The source address (00:13:02:d1:b6:4f) corresponds to the wireless host. The BSS Id (00:16:b6:f7:1d:51) corresponds to the access point. The Destination Address (00:16:b6:f4:eb:a8) corresponds to the first-hop router. The IP address of the wireless host = 192.168.1.109 and the Destination IP address = 128.119.245.12.

2. The 3 MAC address fields in the 802.11 frame are:
   Source address: 00:16:b6:f4:eb:a8
   Destination address: 91:2a:b0:49:b6:4f
   BSS Id: 00:16:b6:f7:1d:51

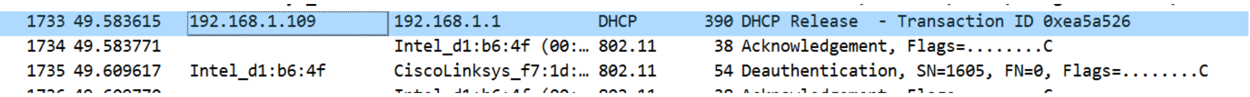


```
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

The source address (00:16:b6:f4:eb:a8) corresponds to the first-hop router. The BSS Id (00:16:b6:f7:1d:51) corresponds to the access point. The Destination Address (91:2a:b0:49:b6:4f) corresponds to the wireless host. The IP address of the server sending the TCP SYNACK is 128.119.245.12.

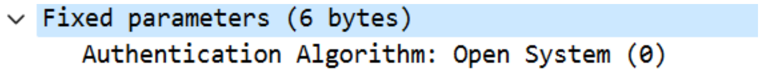
Part-3:

1. At t=49.583615, in packet no. 1733, the host sends a DHCP release message to the DHCP server in the network signaling that the host is leaving and wants to end the association with the AP. At t=49.609617, in packet no. 1735, the host sends a Deauthentication message. We expected to see a Disassociation request frame to have been sent, but it can’t be seen here.



```
 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
```

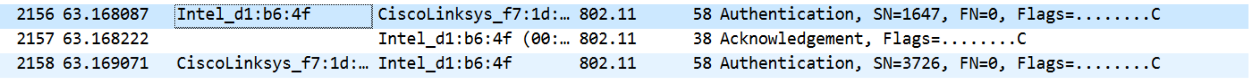
2. A total of 15 Authentication messages are sent from the wireless host to the linksys_ses_24086 AP starting at around t=49. The packet numbers are 1740, 1741, 1742, 1744, 1746, 1749, 1821, 1822, 1921, 1922, 1923, 1924, 2122, 2123 and 2124.
3. The host wants the authentication to be open as we can see below the Authentication algorithm is set to Open System (0).



```
⌄ Fixed parameters (6 bytes)
     Authentication Algorithm: Open System (0)
```

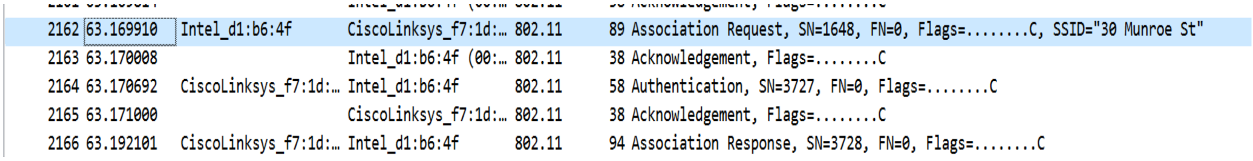
4. No, as the AP is probably ignoring requests from open access as it may have been configured to require a key for connecting.
5. At t = 63.168087, an Authentication frame is sent from the wireless host (00:13:02:d1:b6:4f) to 30 Munroe St. AP(MAC address =

00:16:b6:f7:1d:51). At t = 63.169071, an Authentication reply is sent from that AP to the host reply.



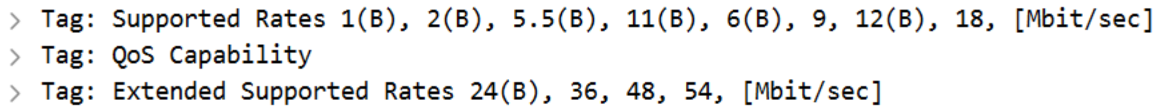
```
2156 63.168087   Intel_d1:b6:4f       CiscoLinksys_f7:1d:… 802.11       58 Authentication, SN=1647, FN=0, Flags=........C
2157 63.168222                        Intel_d1:b6:4f (00:… 802.11       38 Acknowledgement, Flags=........C
2158 63.169071   CiscoLinksys_f7:1d:… Intel_d1:b6:4f       802.11       58 Authentication, SN=3726, FN=0, Flags=........C
```

6. At t = 63.169910, an ASSOCIATE REQUEST is sent from the host (00:13:02:d1:b6:4f) to 30 Munroe St AP. The corresponding ASSOCIATE RESPONSE is sent at t = 63.192101.

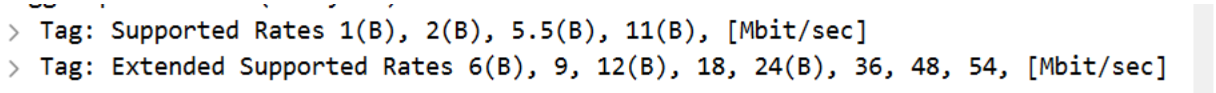


```
2162 63.169910  Intel_d1:b6:4f       CiscoLinksys_f7:1d:… 802.11   89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
2163 63.170008                       Intel_d1:b6:4f (00:… 802.11   38 Acknowledgement, Flags=........C
2164 63.170692  CiscoLinksys_f7:1d:… Intel_d1:b6:4f       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
```

7. Both the host and the AP are willing to use the following transmission rates: 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec].



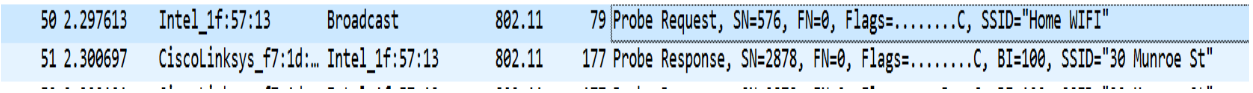
```
> Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
> Tag: QoS Capability
> Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```



```
> 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]
```

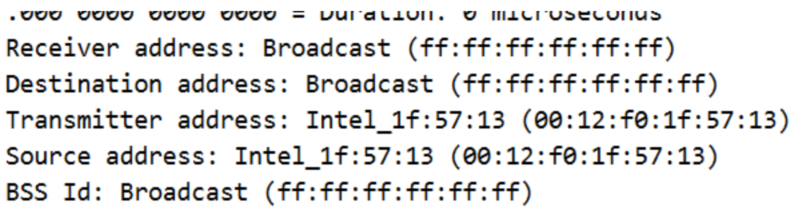
Part-4:

1. For the PROBE REQUEST sent at t = 2.297613, the MAC address of the sender(source) is 00:12:f0:1f:57:13, destination(receiver) is ff:ff:ff:ff:ff:ff and BSS ID is ff:ff:ff:ff:ff:ff. For the PROBE RESPONSE received at t = 2.300697, the MAC address of the sender(source) is 00:16:b6:f7:1d:51, destination(receiver) is 00:12:f0:1f:57:13 and BSS ID is 00:16:b6:f7:1d:51. Probe Request frames are sent by client devices to search for available networks, while Probe Response frames are sent by access points to provide information about their network in response to Probe Requests. These frames facilitate the process of discovering and connecting to wireless networks. In short, A probe request is used by a host in active scanning to find an access point and a probe response is sent by the access point back to the host.



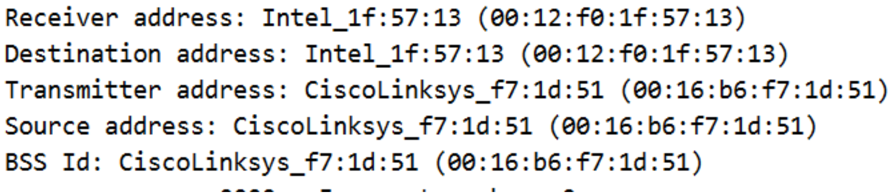
```
50 2.297613   Intel_1f:57:13      Broadcast        802.11    79 Probe Request, SN=576, FN=0, Flags=........C, SSID="Home WIFI"
51 2.300697   CiscoLinksys_f7:1d:… Intel_1f:57:13  802.11   177 Probe Response, SN=2878, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
```

Request:



```
.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)
```

Response:



```
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)
```