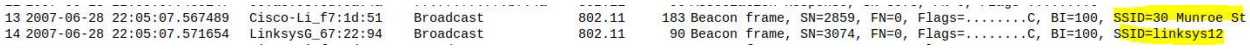
Kevin Huang
Lab 4: 802.11
CSS 537
03/11/2022

Introduction

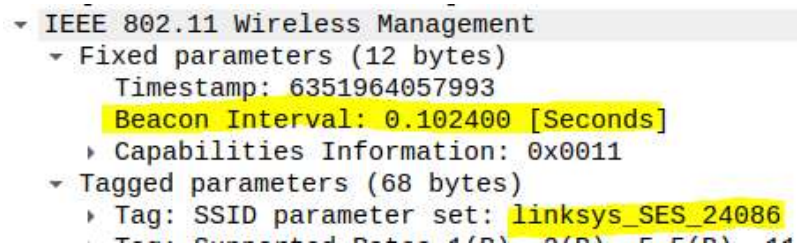
In this lab, I used Wireshark to analyze an 802.11 trace file. I looked at beacon frames, how data transfers over 802.11, association/dissociation, and probe requests/responses.

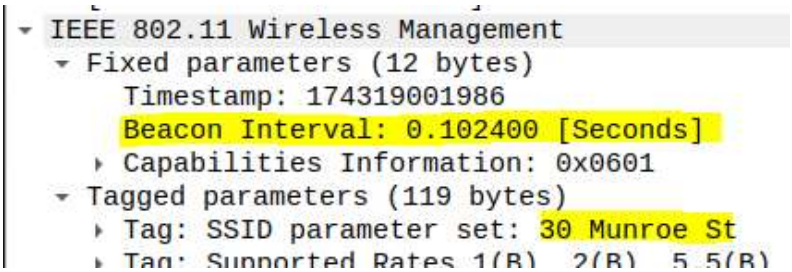
2. Beacon Frames

1. Using 'wlan[0] == 0x80', I was able to filter for all the beacon frames. The two access points that are issuing most of the beacon frames in this trace is "30 Munroe St" and "linksys12'

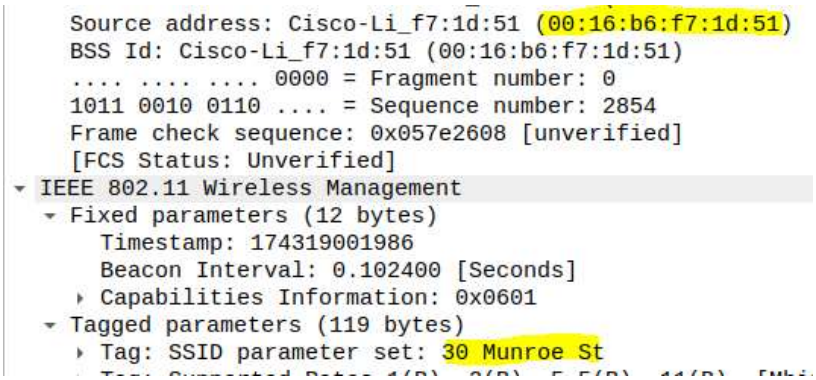


2. The interval between the transmissions of beacon frames for linksys_ses_24086 and 30 Munroe St is both 0.102400 seconds.

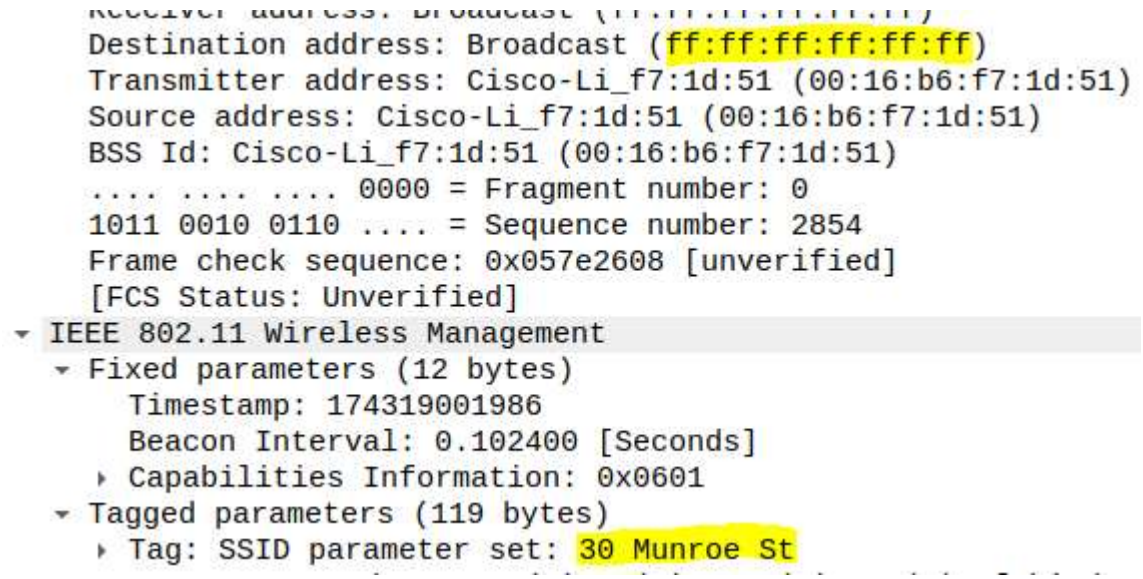




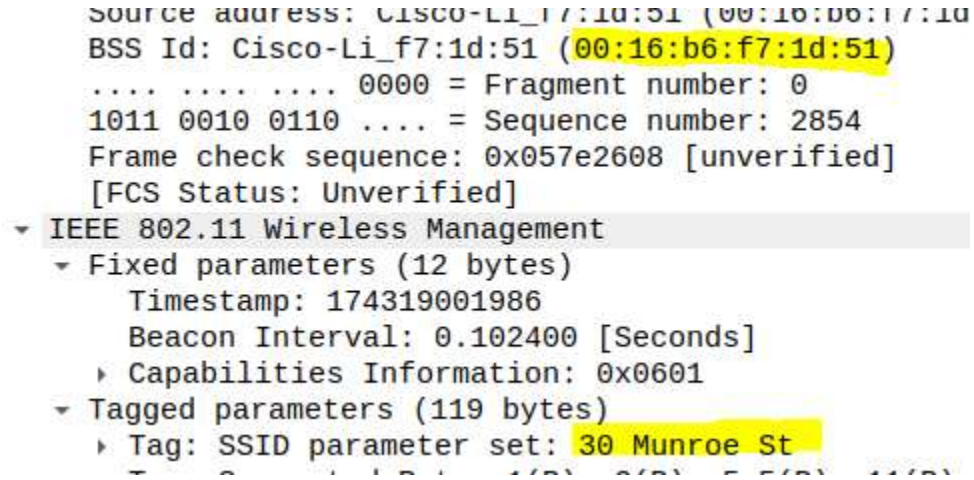
3. The source MAC address on the beacon frame from 30 Munroe St is 00:16:b6:f7:1d:51



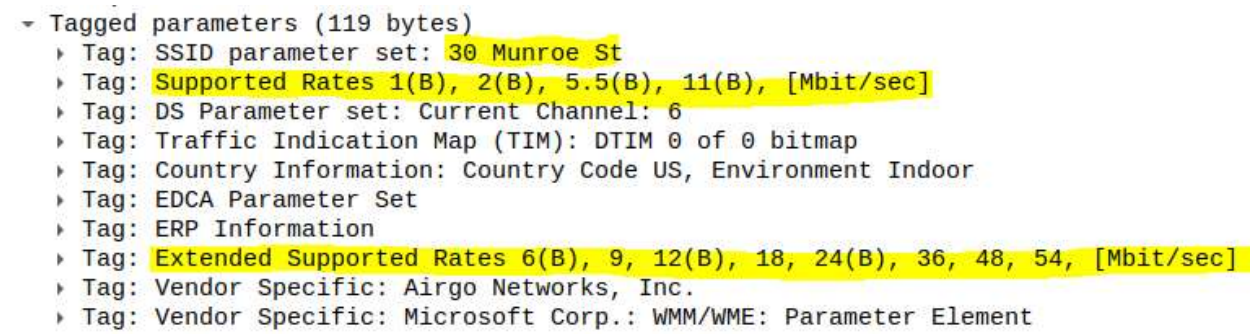
4. The destination MAC address on the beacon frame from 30 Munroe St is ff:ff:ff:ff:ff:ff



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

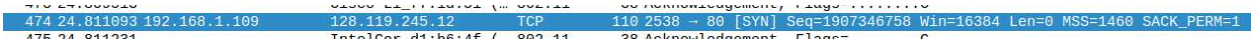


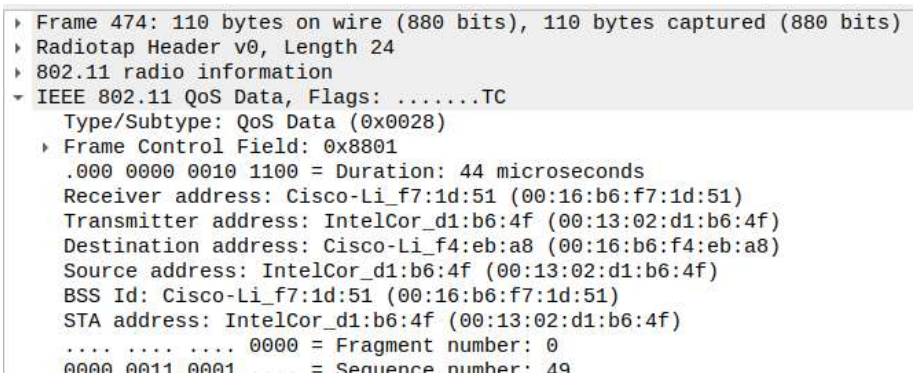
6. The four supported data rates for 30 Munroe St are 1(B), 2(B), 5.5(B), and 11(B), [Mbit/sec]. The eight extended supported rates are 6(B), 9, 12(B), 18, 24(B), 36, 48, and 54, [Mbit/sec]



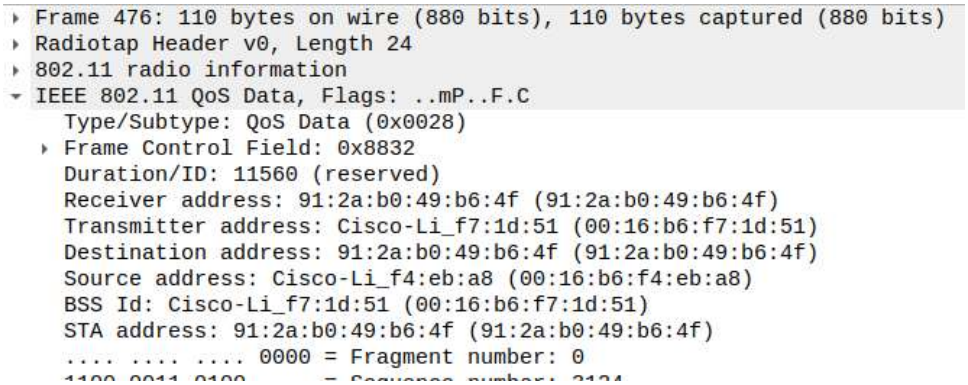
3. Data Transfer

7. The three MAC address fields in the 802.11 frame containing the SYN TCP segment are source = 00:13:02:d1:b6:4f, destination = 00:16:b6:f4:eb:a8, BSS = 00:16:b6:f7:1d:51
The MAC address for the wireless host is 00:13:02:d1:b6:4f
The MAC address of access point is 00:16:b6:f4:eb:a8
The MAC address of first-hop router is 00:16:b6:f4:eb:a8
The IP address of wireless host sending the TCP segment is 192.168.1.109
The destination IP address is 128.119.245.12
The destination IP address is the address for gaia.cs.umass.edu which is some other network-attached device. When the TCP segment gets to the first-hop router, it will identify that the IP address is outside the local network and send the segment out of its interface that can go to gaia.cs.umass.edu.





8. The three MAC address fields in the 802.11 frame containing the SYNACK TCP segment are source = 00:16:b6:f4:eb:a8, destination = 91:2a:b0:49:b6:4f, BSS = 00:16:b6:f7:1d:51
The MAC address for the wireless host is 91:2a:b0:49:b6:4f
The MAC address of access point is 00:16:b6:f4:eb:a8
The MAC address of first-hop router is 00:16:b6:f4:eb:a8
No, the sender MAC address in the frame does not correspond to the IP of the device that sent the TCP segment. This is because when the TCP segment goes through the router, it switches interfaces. Each interface has its own IP address. To get to the wireless host, the segment will need to go through the interface that is facing the wireless host.



3. Association/Disassociation

9. A DHCP release frame and a deauthentication frame were sent by the host to end the association with the 30 Munroe St AP. It looks like there might be a disassociation notification that we do not see here.

```
1733 49.583615 192.168.1.109    192.168.1.1          DHCP      390 DHCP Release  - Transaction ID 0xea5a526
1734 49.583771                  IntelCor_d1:b6:4f (… 802.11     38 Acknowledgement, Flags=........C
1735 49.609617 IntelCor_d1:b6:4f Cisco-Li_f7:1d:51    802.11     54 Deauthentication, SN=1605, FN=0, Flags=........C
```

```
▸ 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 1011 1000 .... = Sequence number: 184
  Frame check sequence: 0x90381791 [unverified]
  [FCS Status: Unverified]
▸ Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 192.168
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Release)
```

```
▾ IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  ▸ Frame Control Field: 0xc000
    .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)
```

The disassociation service may be invoked by either party to an association (non-AP STA or AP). Disassociation is a notification, not a request. Disassociation cannot be refused by either party to the association.

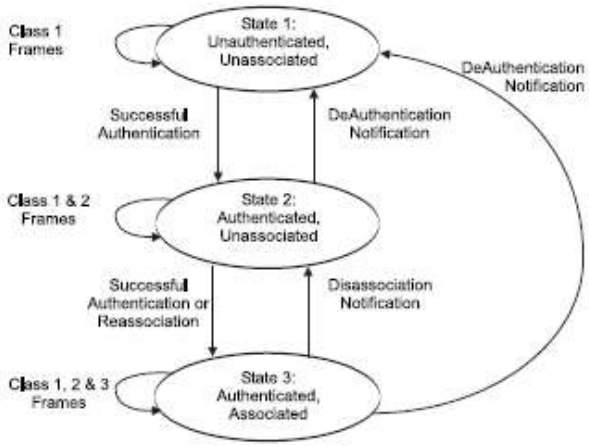


Figure 8—Relationship between state variables and services

10. Looks like there was 15 authentication messages from the wireless host to Cisco_Li_f5:ba:bb

wlan.fc.type_subtype == 11

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, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=........C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=........C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=........C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=........C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=........C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=........C

11. The host wants the authentication to be open

```
    Type/Subtype: Authentication (0x000b)
  ▸ Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
    Destination address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
    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_f5:ba:bb (00:18:39:f5:ba:bb)
    .... .... .... 0000 = Fragment number: 0
    0110 0100 0110 .... = Sequence number: 1606
    Frame check sequence: 0xed30374c [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)
```

12. I was not able to find a reply authentication from linksys_ses_24086 AP.

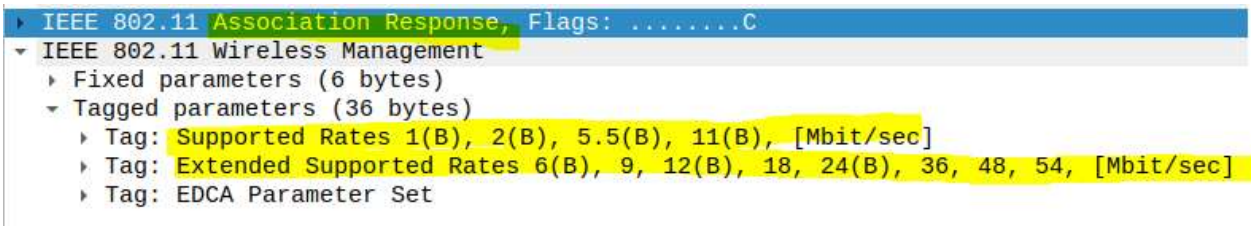
13. The host sends authentication frames to 30 Munroe St AP at 63.168087 and 63.169707. There are replies at 63.169071 and 63.170692

```
2156 63.168087 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11      58 Authentication, SN=1647, FN=0, Flags=........C
2158 63.169071 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11      58 Authentication, SN=3726, FN=0, Flags=........C
2160 63.169707 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11      58 Authentication, SN=1647, FN=0, Flags=....R...C
2164 63.170692 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11      58 Authentication, SN=3727, FN=0, Flags=........C
```

14. The host sends an associate request at time 63.169910. There is an associate reply at 63.192101.

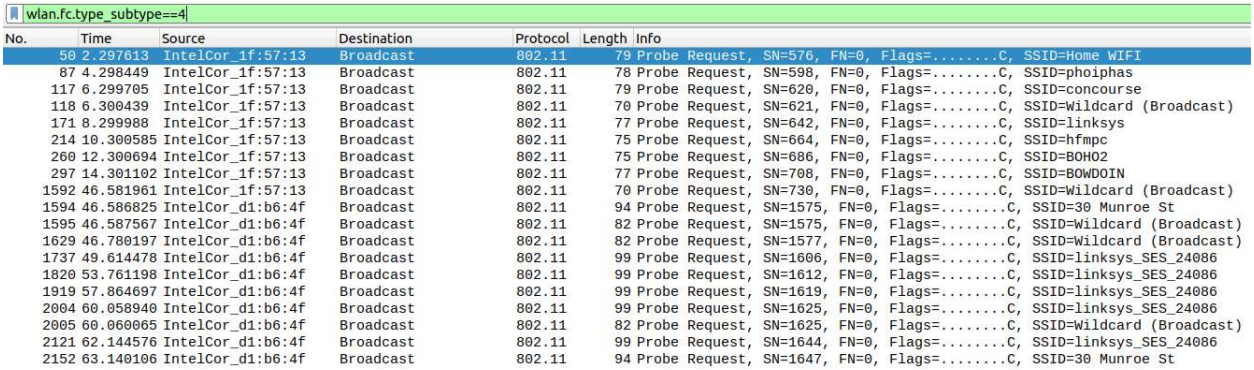
```
2162 63.169910 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11      89 Association Request, SN=1648, FN=0, Flags=........C, SSID=30 Munroe St
2166 63.192101 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11      94 Association Response, SN=3728, FN=0, Flags=........C
```

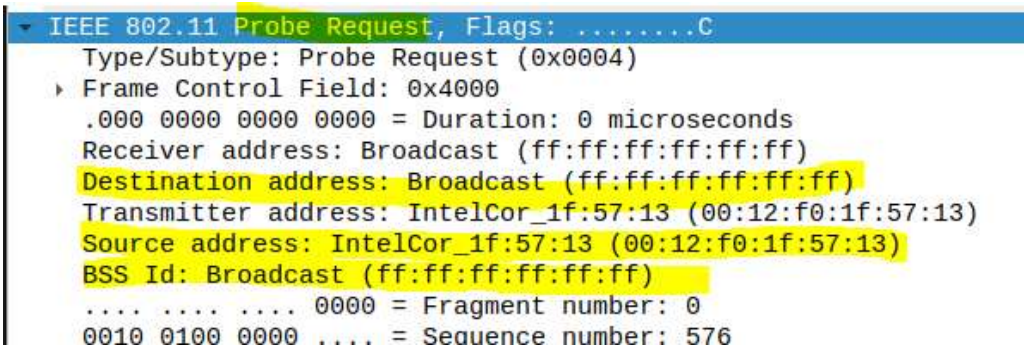
15. Both the host and AP support 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec] and also support the extended rates 24(b), 35, 48, 54, [Mbit/sec]

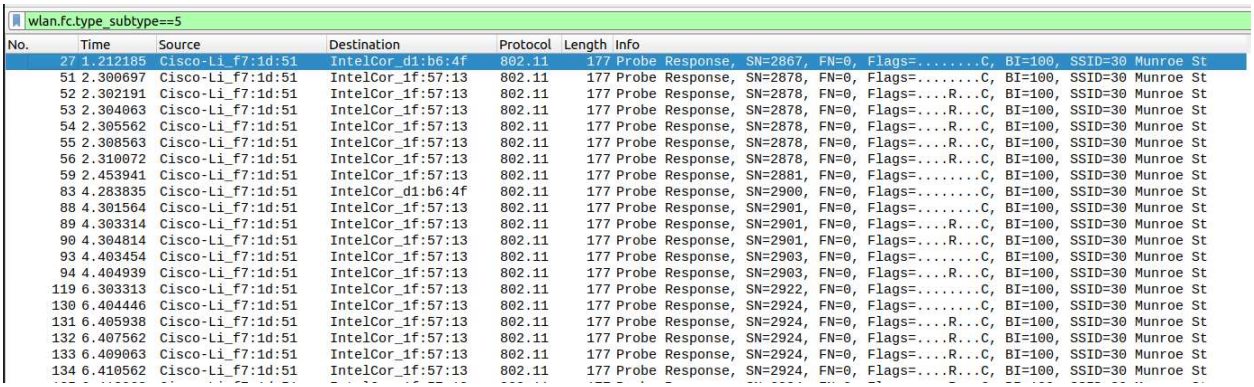


4. Other Frame types

16. For the probe request, the sender is 00:12:f0:1f:57:13, receiver is ff:ff:ff:ff:ff:ff, BSS ID is ff:ff:ff:ff:ff:ff. The receiver is broadcast. For the probe response, the sender/BSS ID belongs to the AP that is responding. The probe response sender is 00:16:b6:f7:1d:51, receiver is 00:13:02:d1:b6:4f, BSS ID is 00:16:b6:f7:1d:51. The probe request is used to scan all the AP's. The probe responses are replies from the AP's giving the host their info.

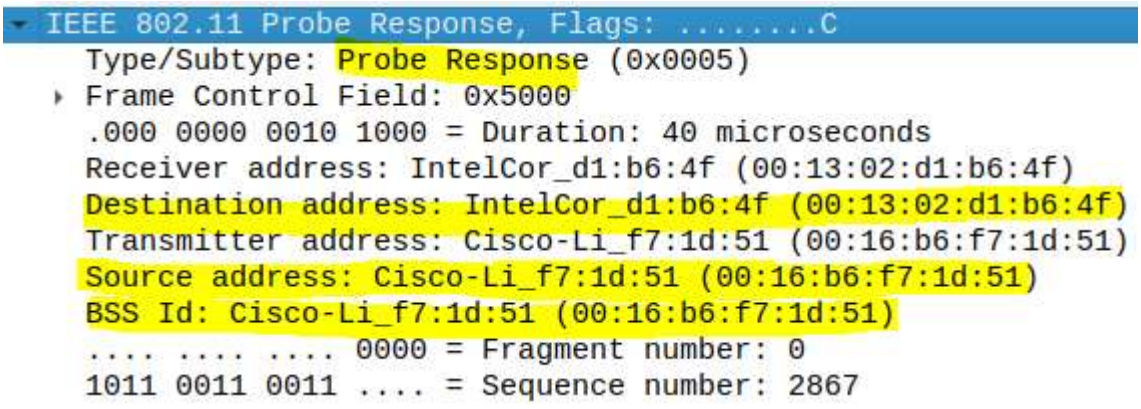






wlan.fc.type_subtype==5

No.	Time	Source	Destination	Protocol	Length	Info
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
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
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
53	2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
54	2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
55	2.308563	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
56	2.310072	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
59	2.453941	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2881, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
83	4.283835	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2900, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
88	4.301564	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2901, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
89	4.303314	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2901, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
90	4.304814	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2901, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
93	4.403454	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2903, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
94	4.404939	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2903, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
119	6.303313	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2922, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
130	6.404446	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
131	6.405938	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
132	6.407562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
133	6.409063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
134	6.410562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St



```
▾ IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
  ▸ Frame Control Field: 0x5000
    .000 0000 0010 1000 = Duration: 40 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    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 0011 .... = Sequence number: 2867
```