Computer Networks 1

Lab 7

Wireshark Lab: 802.11 WiFi v8.0

Student Name: **Nguyễn Quý Hải**

Student No.: **2052974**

I. Objectives

- Investigate the 802.11 wireless network protocol

II. Content

1. Beacon Frames

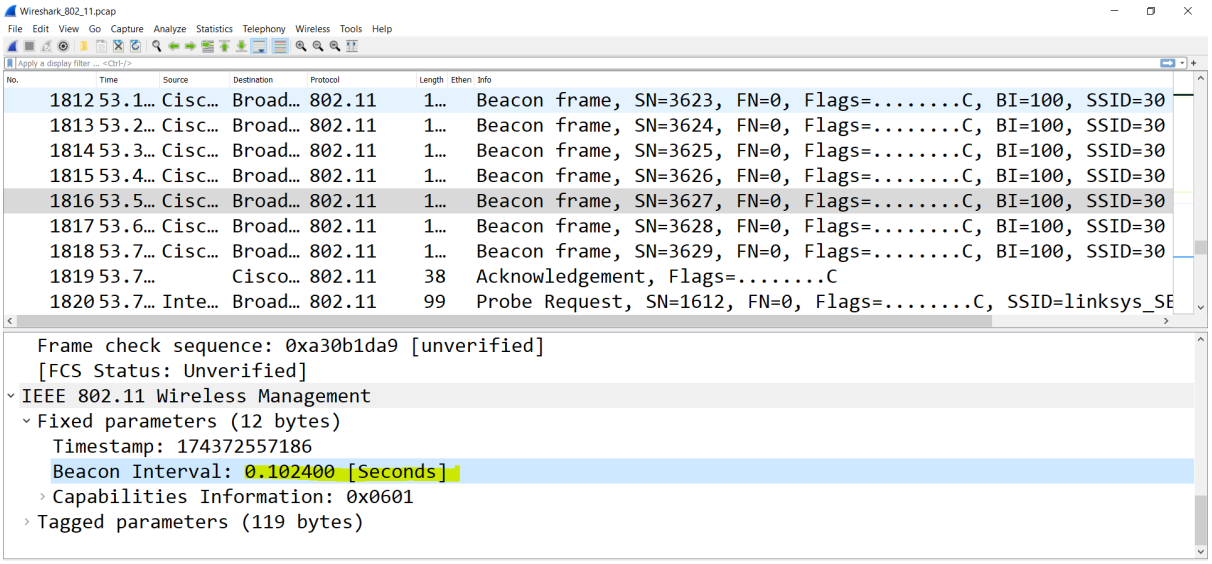
- Q1: What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

  Answer: The two access points that are issuing most of the beacon frames have an SSID of **"30 Munroe St"** and **"linsys_SES_24086"**.

	Destination	Protocol	Length	Ethen	Info
:…	Broad…	802.11	1…		Beacon frame, SN=3623, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
:…	Broad…	802.11	1…		Beacon frame, SN=3624, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
:…	Broad…	802.11	1…		Beacon frame, SN=3625, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
:…	Broad…	802.11	1…		Beacon frame, SN=3626, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
:…	Broad…	802.11	1…		Beacon frame, SN=3627, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
:…	Broad…	802.11	1…		Beacon frame, SN=3628, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
:…	Broad…	802.11	1…		Beacon frame, SN=3629, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
	Cisco…	802.11	38		Acknowledgement, Flags=.....C
:…	Broad…	802.11	99		Probe Request, SN=1612, FN=0, Flags=.....C, SSID=linksys_SES_24086
:…	Cisco…	802.11	58		Authentication, SN=1612, FN=0, Flags=.....C
:…	Cisco…	802.11	58		Authentication, SN=1612, FN=0, Flags=....R...C
	Cisco…	802.11	38		Acknowledgement, Flags=.....C
:…	Cisco…	802.11	1…		Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
:…	Cisco…	802.11	1…		Association Request, SN=1613, FN=0, Flags=....R...C, SSID=linksys_SES_24086
	Cisco…	802.11	38		Acknowledgement, Flags=.....C
:…	Cisco…	802.11	1…		Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086

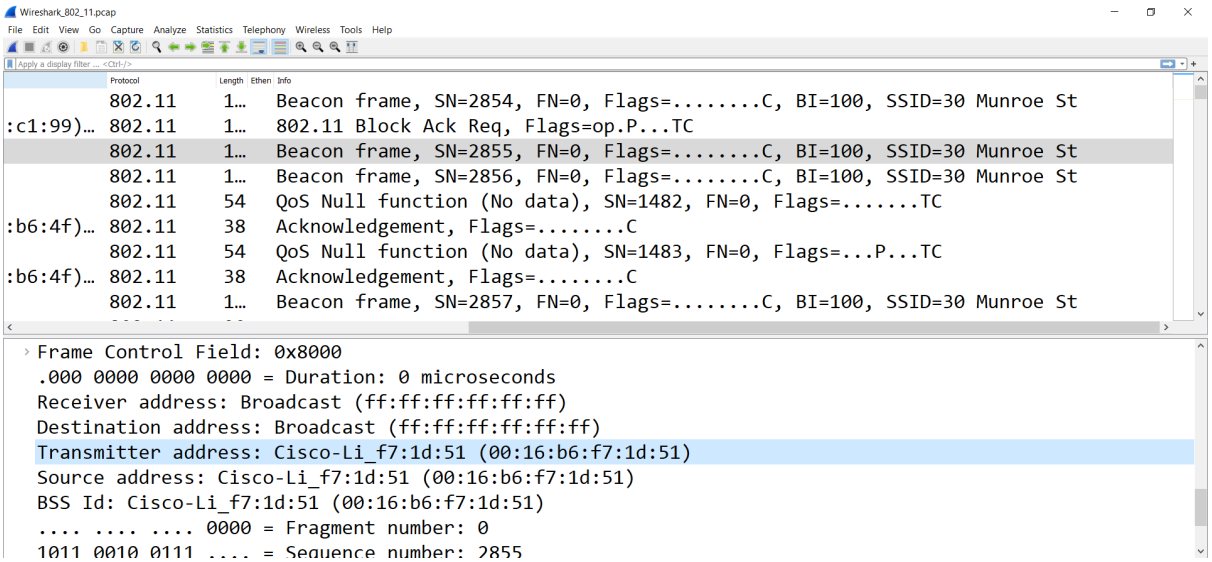
- Q2. What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).

  Answer: 0.1024s



- Q3. 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).

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



- Q4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??

  Answer: he destination MAC address on the beacon frame from 30 Munroe St is: ff:ff:ff:ff:ff:ff (Broadcast)

- Q5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?

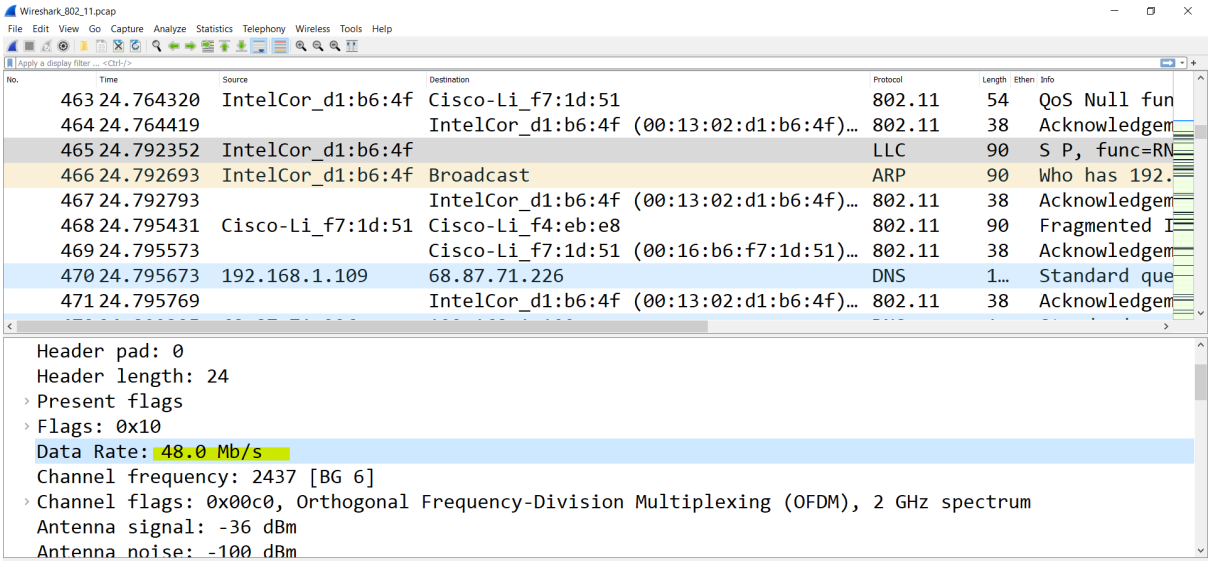
Answer: The MAC BSS ID address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51 (as you can see in the figure above)

- Q6. 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?

Answer:

Four data rates: 1.0, 2.0, 5.5, 11.0 Mbps.

Eight additional "extended supported rates" are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0 Mbps



2. Data Transfer

- Q7: 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? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

Answer:

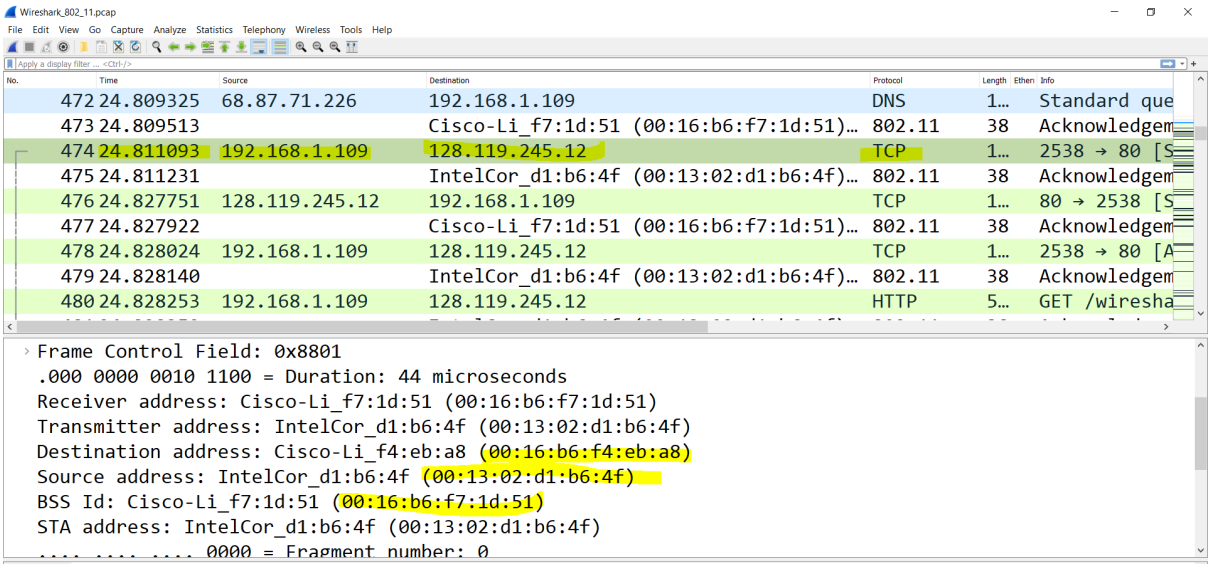
The MAC address for the host sending the TCP SYN is 00:13:02:d1:b6:4f.

The 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.

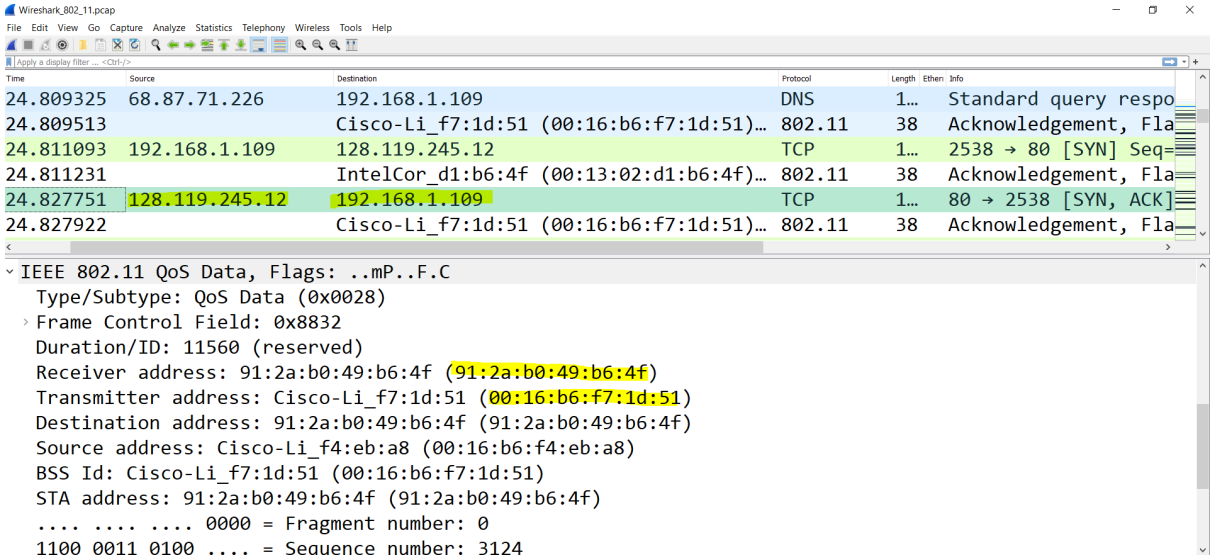
The destination address is 128.199.245.12. This corresponds to the server gaia.cs.umass.edu.



- Q8: 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 MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).

  Answer:

  - Three MAC address fields in the 802.11 frame are BSS id: 00:16:b6:f7:1d:51, Destination: 00:13:02:d1:b6:4f and source address: 00:16:b6:f4:eb:a8
  - The MAC corresponds to the host is 00:13:02:d1:b6:4f (destination)
  - The MAC corresponds to the first hop is 00:16:b6:f4:eb:a8 (Source)
  - The sender MAC address in the frame does not correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram, because the TCP SYNACK's IP address is 128:199:245:12 but the destination IP address is 192.168.1.109.

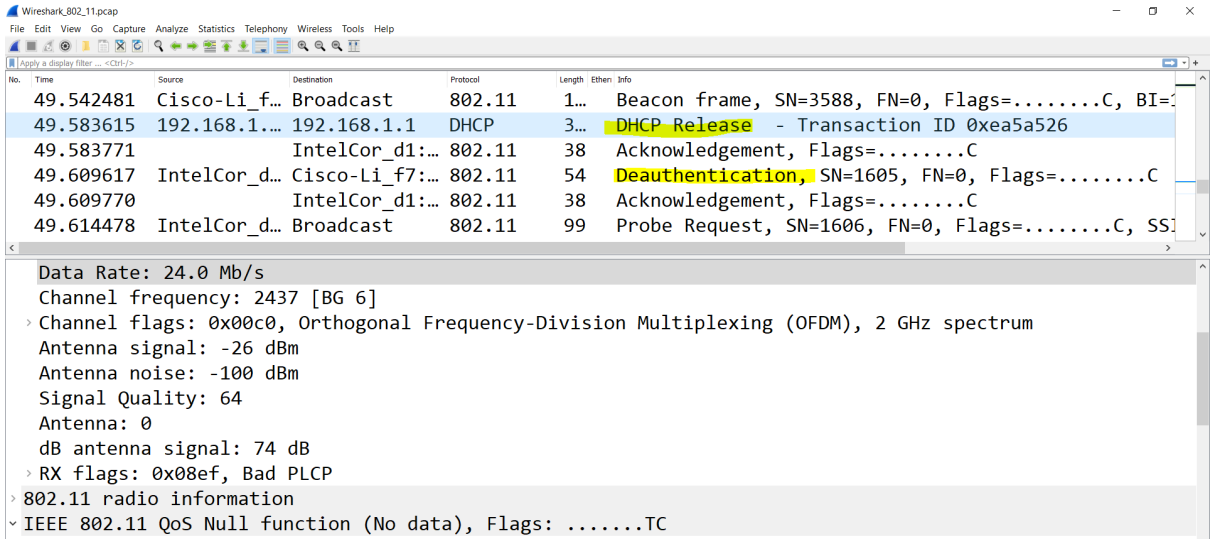


3. Association/Disassociation

- Q9: 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?

  <u>Answer</u>:

  - At t = 49.583615 a DHCP release is sent by the host to the DHCP server
  - At t = 49.609617, the host sends a DEAUTHENTICATION frame



- Q10. 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? .

Answer: There are 17 AUTHENTICATION messages from the wireless host to the linksys_ses_24086 AP.

- Q11. Does the host want the authentication to require a key or be open?

  Answer: The host is requesting that the association be open

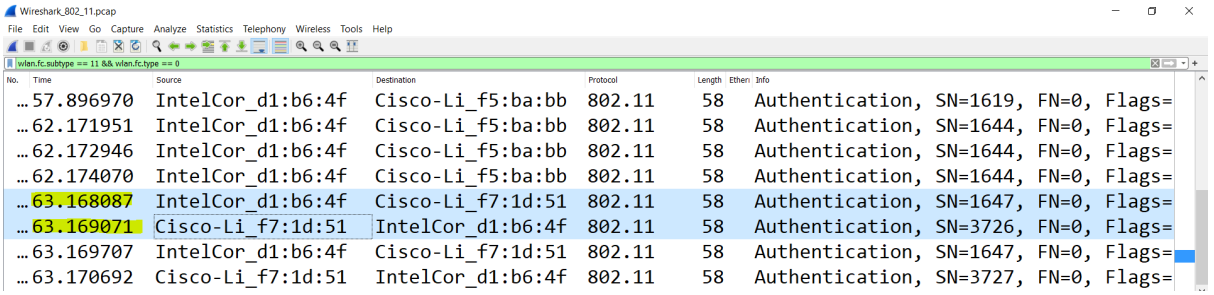
- Q12. Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?

  Answer: I can not see.

- Q13. 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 and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

  Answer:

  - At t = 63.168087 there is a AUTHENTICATION frame sent from 00:13:02:d1:b6:4f
  - At t = 63.169071 there is an AUTHENTICATION from sent in the reverse direction from the BSS to the wireless host



- Q14: An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

  Answer:

- At t = 63.169910 there is an 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

- Q15. 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.

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

```
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)
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 36 (0x48)
    Extended Supported Rates: 48 (0x60)
    Extended Supported Rates: 54 (0x6c)
```

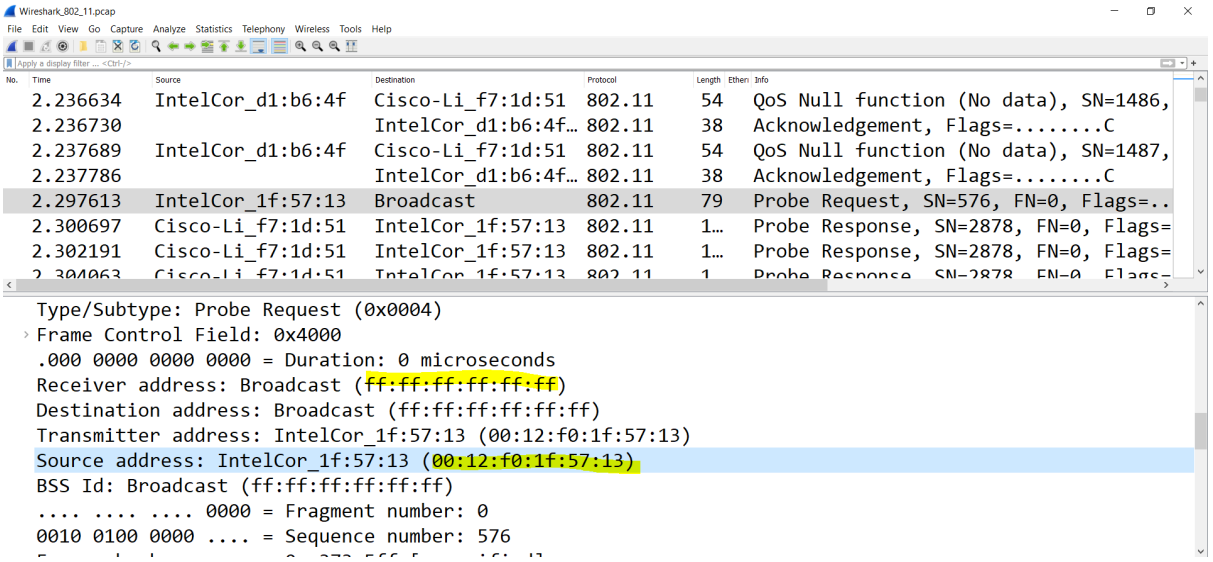
4. Other Frame types

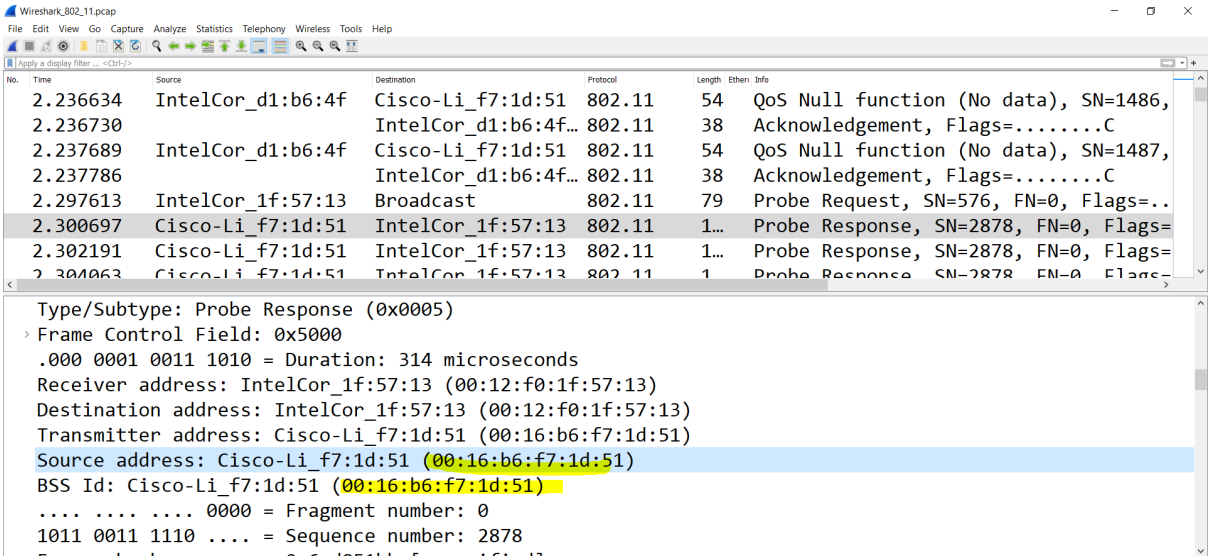
- Q16: What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).

  Answer:

  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 there is a PROBE RESPONSE 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 (broadcast) to find an Access Point. A PROBE RESPONSE is sent by the access point to the host sending the request