Họ tên : Lê Bảo Khánh

MSSV : 1911363

Lớp : L01

**LAB 7**

(using the file Wireshark\_802\_11.pcap)

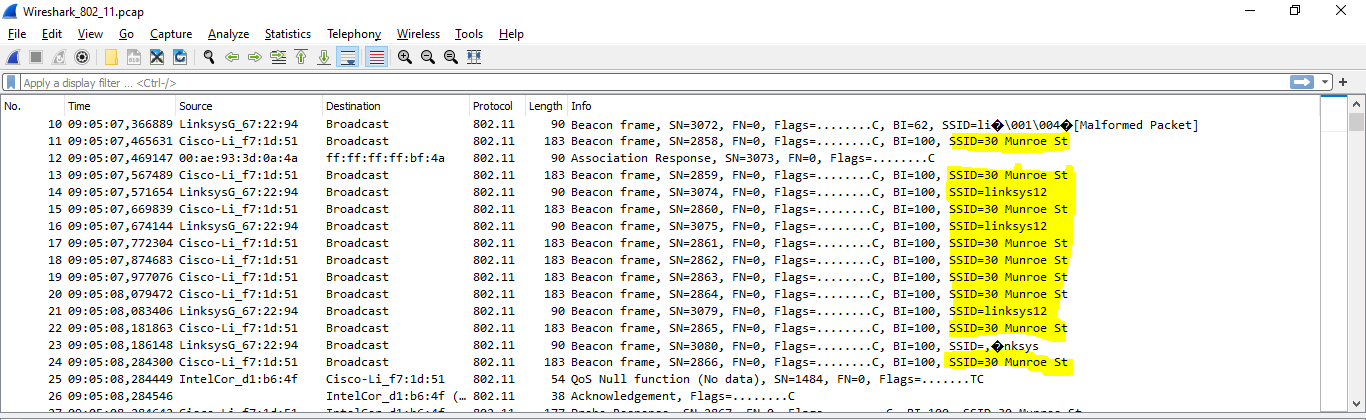
**2. Beacon Frames**

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

**ANSWER:**

30 Munroe St

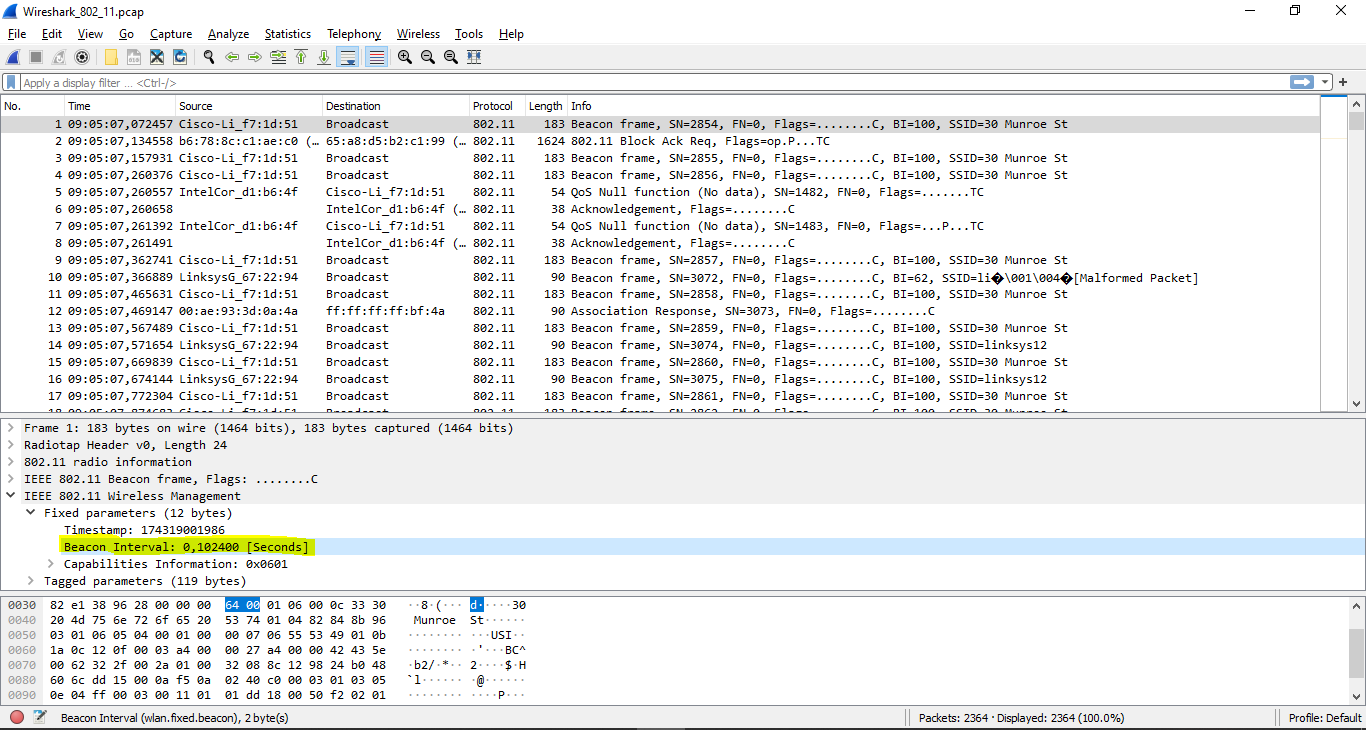
linsys\_SES\_24086



**Question 2:** 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:**

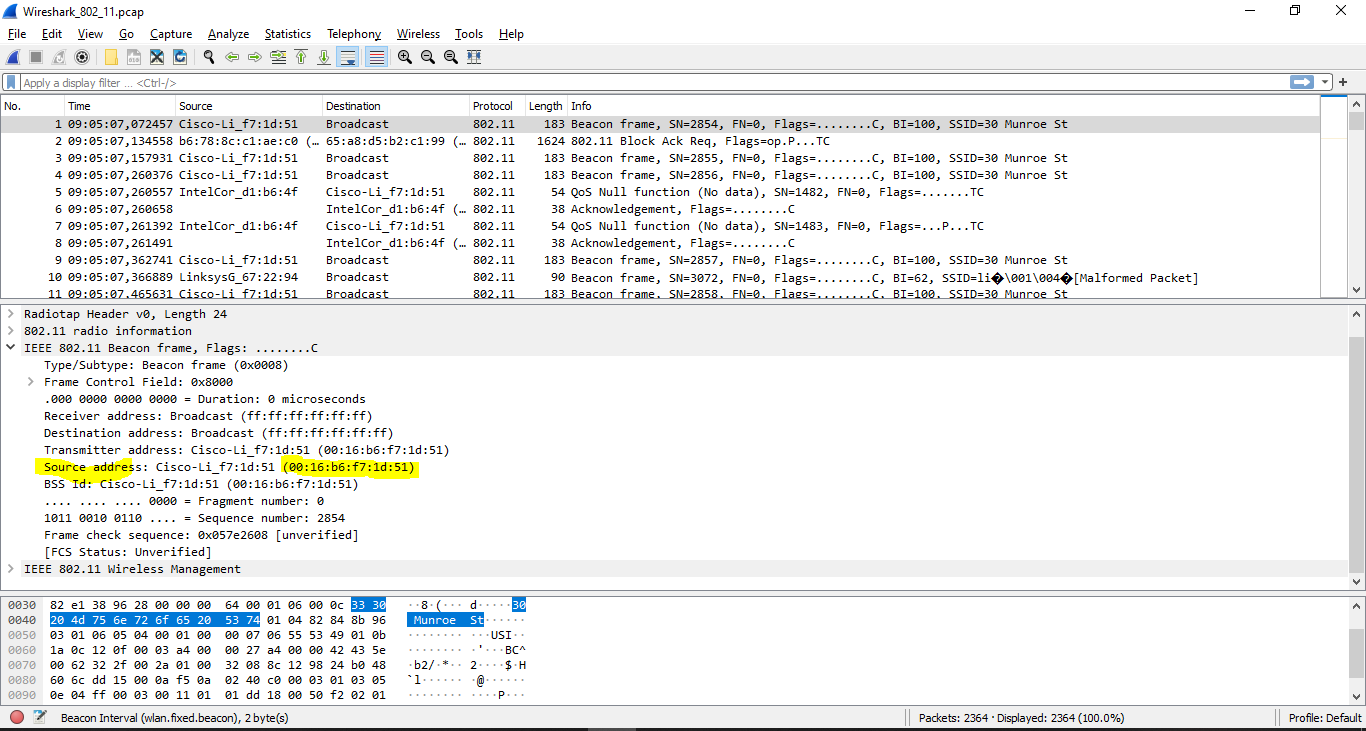
0.1024 s



**Question 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).

**ANSWER:**

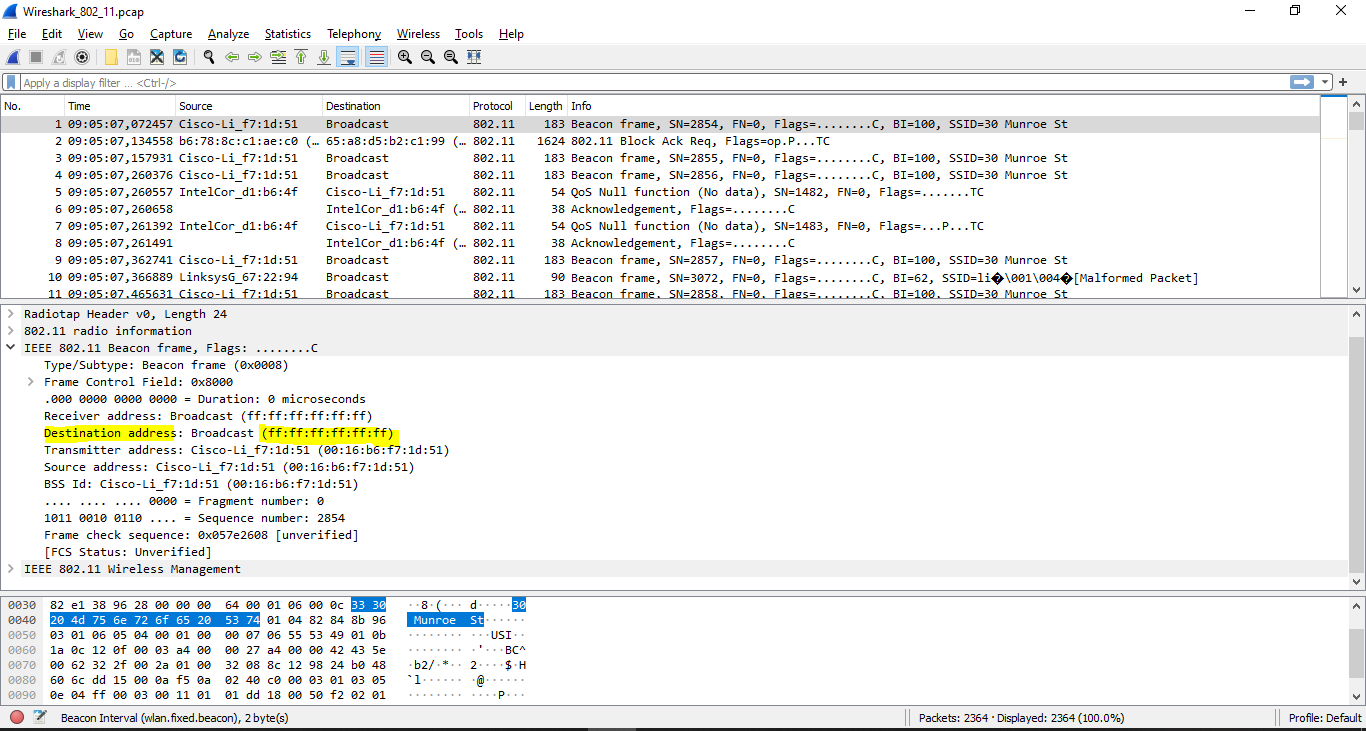
00:16:b6:f7:1d:51



**Question 4:** What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??

**ANSWER:**

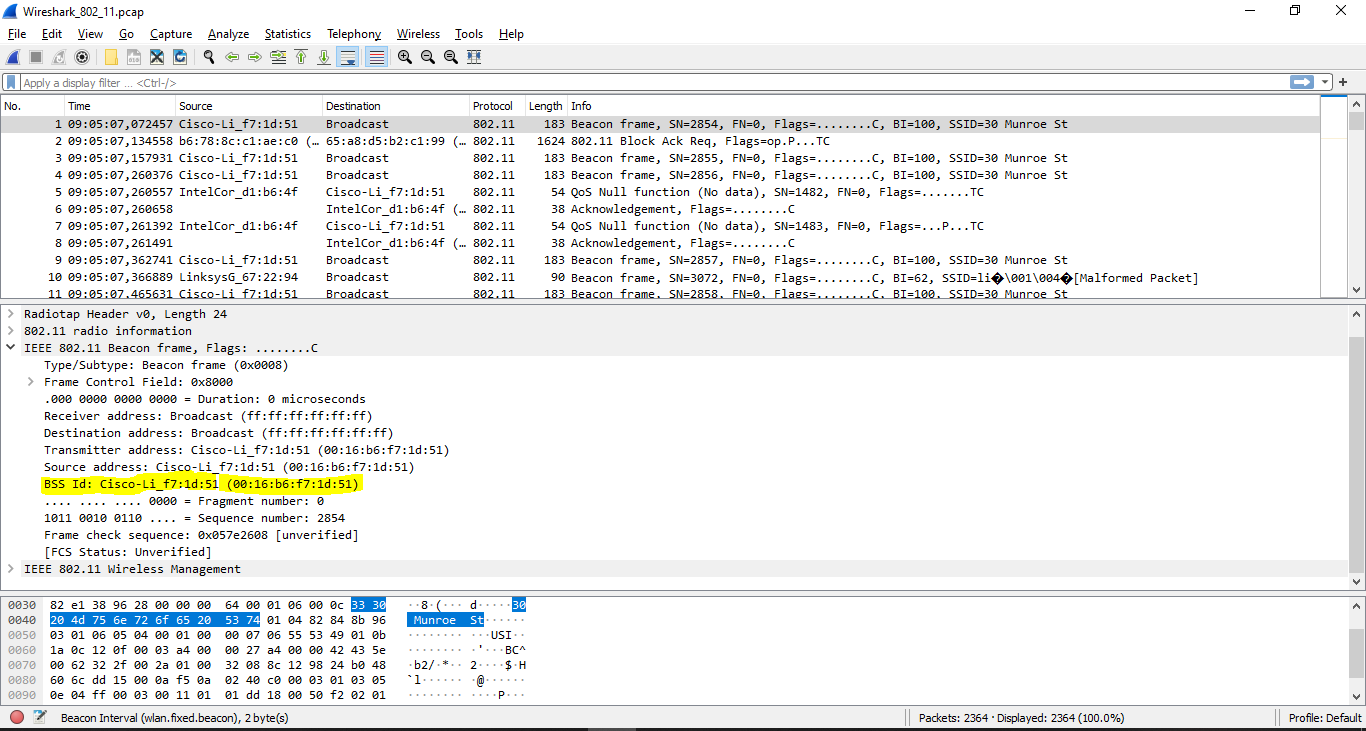
ff:ff:ff:ff:ff:ff



**Question 5:** What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30Munroe St?

**ANSWER:**

00:16:b6:f7:1d:51

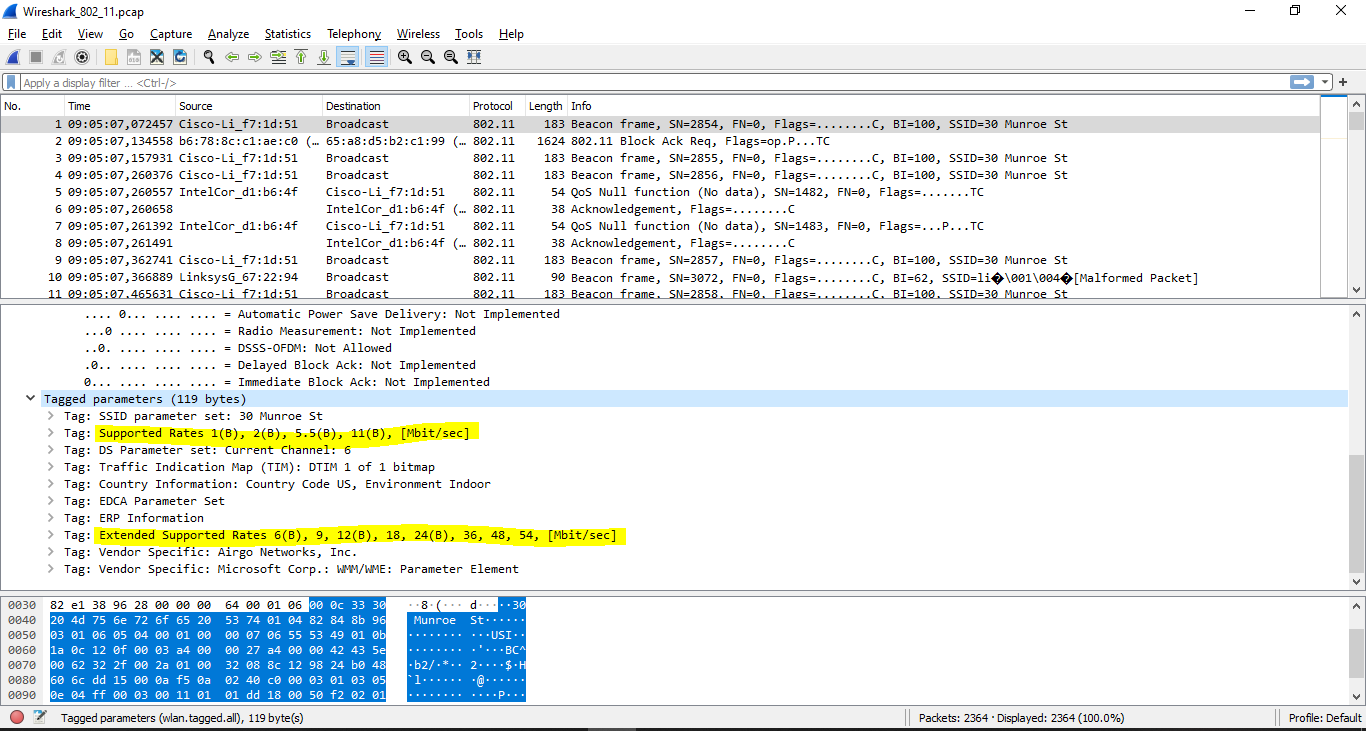


**Question 6:** The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?

**ANSWER:**

4 data rates: 1.0, 2.0, 5.5, 11 Mbps

8 additional “extended supported rates” : 6, 9, 12, 18, 24, 36, 48, 54 Mbps



**3. Data Transfer**

**Question 7:** 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:**

Those MAC addresses are BSSid, source address, destination.

The MAC address corresponds to:

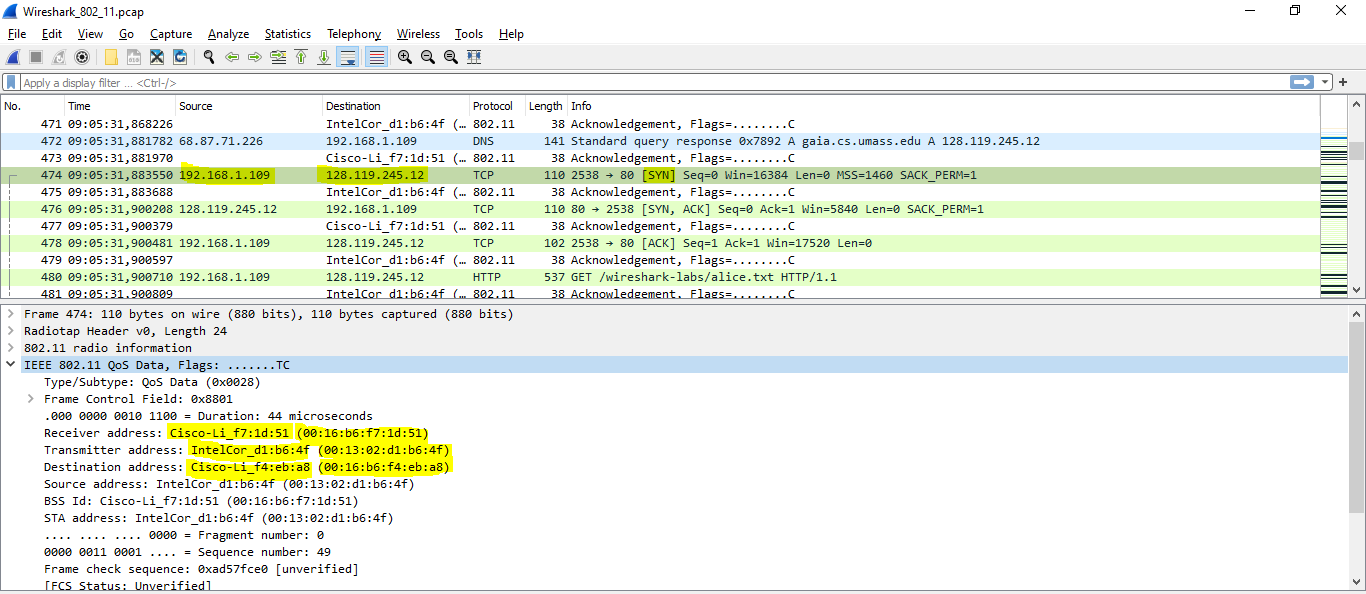
+ The wireless host: **00:13:02:d1:b6:4f**.

+ The 1st hop router: **00:16:b6:f4:eb:a8**.

+ The wireless host sending this TCP segment: **00:16:b6:f7:1d:51**.

The corresponding IP of the wireless host: **192.168.1.109**.

Destination IP: **128.199.245.12** (corresponds to the host)



**Question 8:** 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:

+ BSS id: **00:16:b6:f7:1d:51**

+ Destination: **00:13:02:d1:b6:4f**

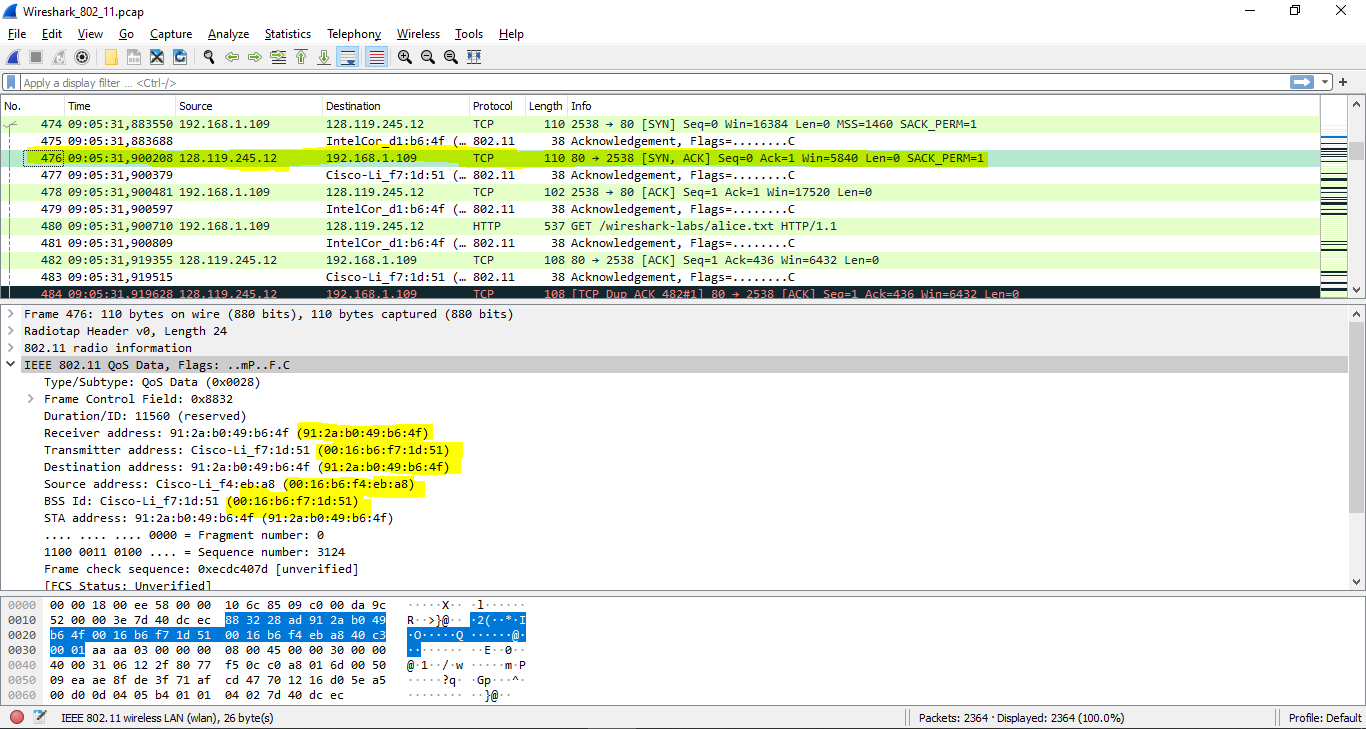
+ Source address: **00:16:b6:f4:eb:a8**

The MAC corresponds to

+ The host: 00:13:02:d1:b6:4f (destination)

+ 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**)

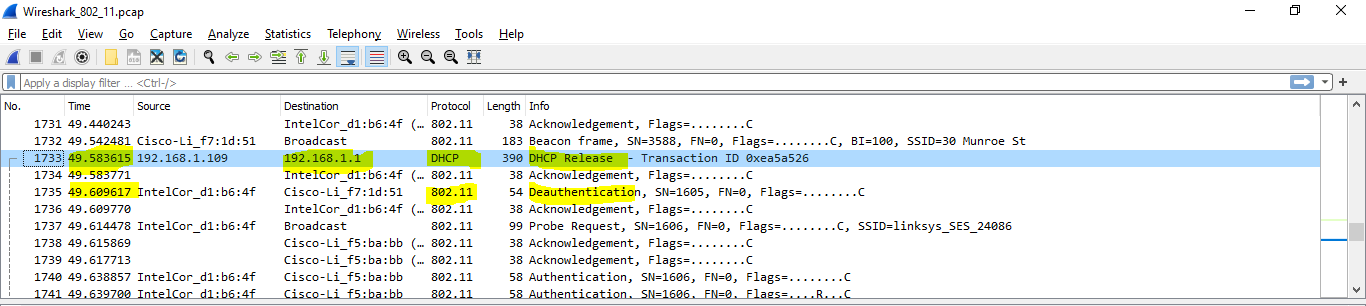


**3. Association/Disassociation**

**Question 9:** 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?

**ANSWER:**

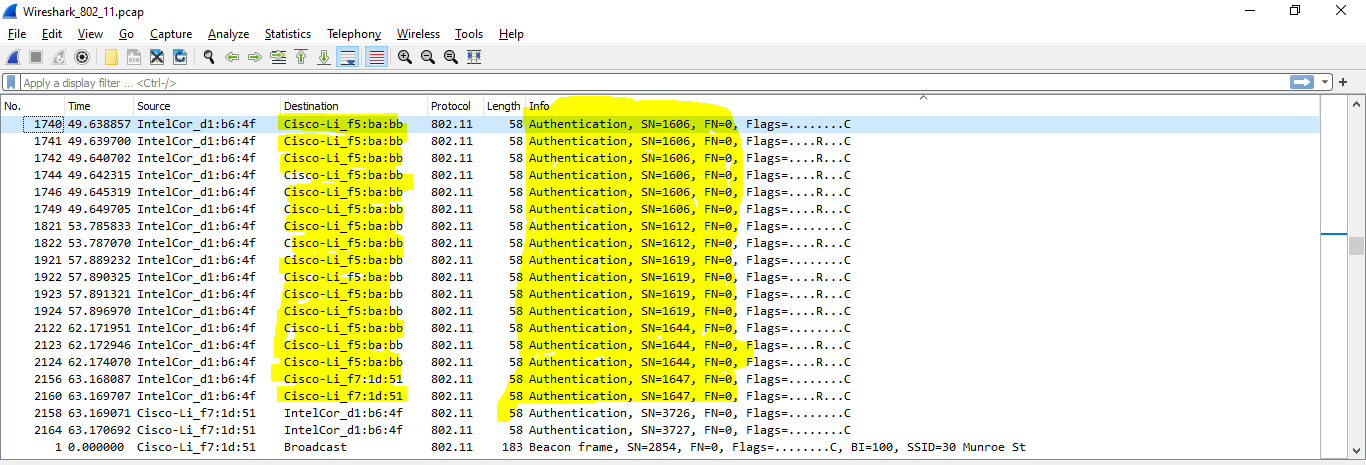
1. A DHCP is sent to 192.168.1.1
2. The host sends a DEAUTHENTICATION frame after 0.02



**Question 10:** Examine the trace file and look for AUTHENICATION 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:**

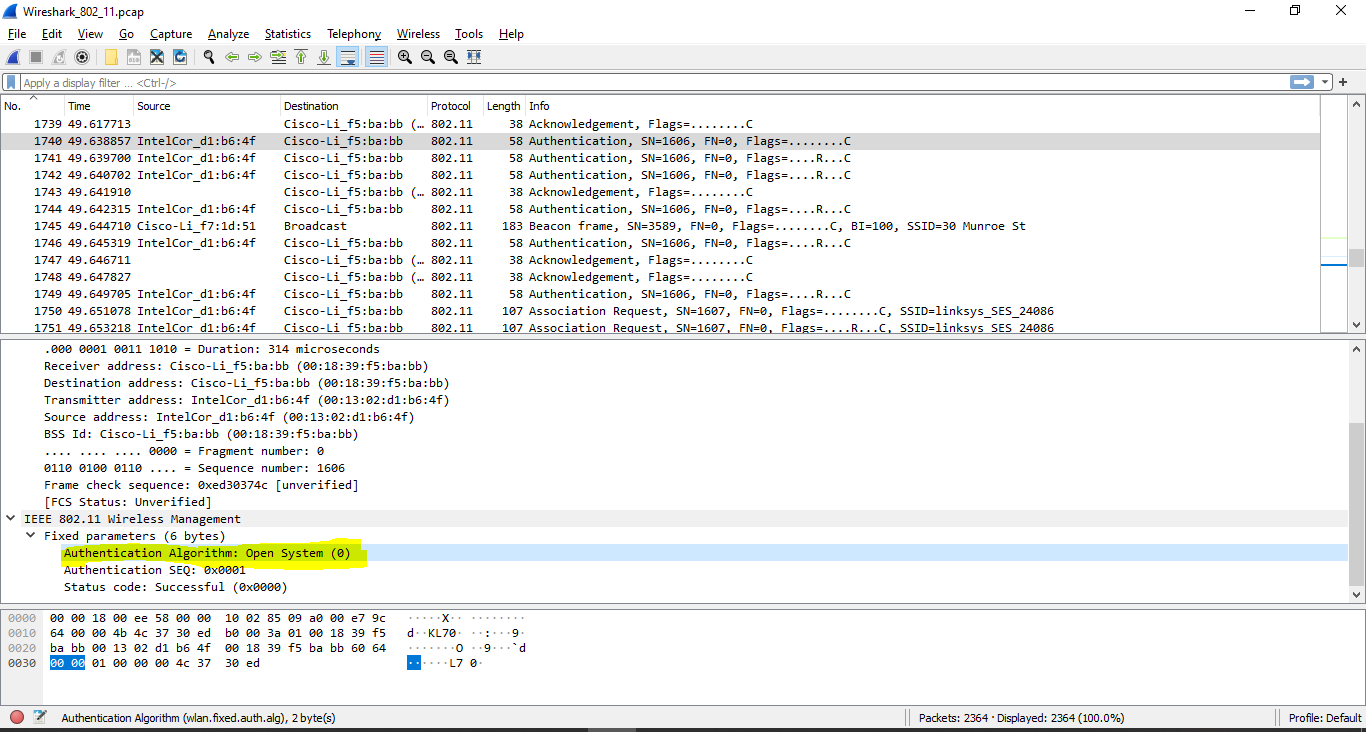
There are **17** AUTHENTICATION messages from the wireless host to the linksys\_ses\_24086 AP



**Question 11:** Does the host want the authentication to require a key or be open?

**ANSWER:**

It’s open



**Question 12:** Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?

**ANSWER:**

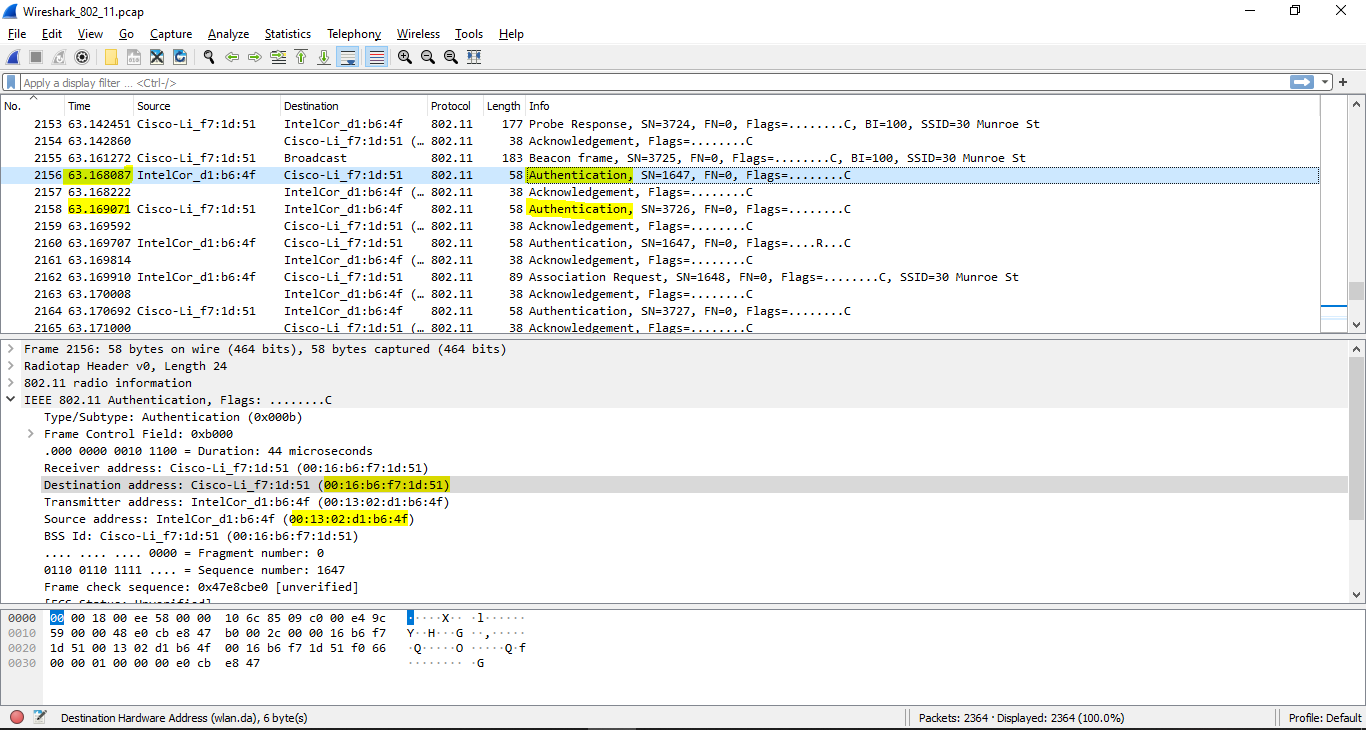
No

**Question 13:** 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 AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30Munroe 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:**

There is an AUTHENTICATION frame from 00:13:02:d1:b6:4f to 00:16:b7:f7:1d:51 when **t = 63.168087.**

The AUTHENTICATION sent back at **t = 63.169071**

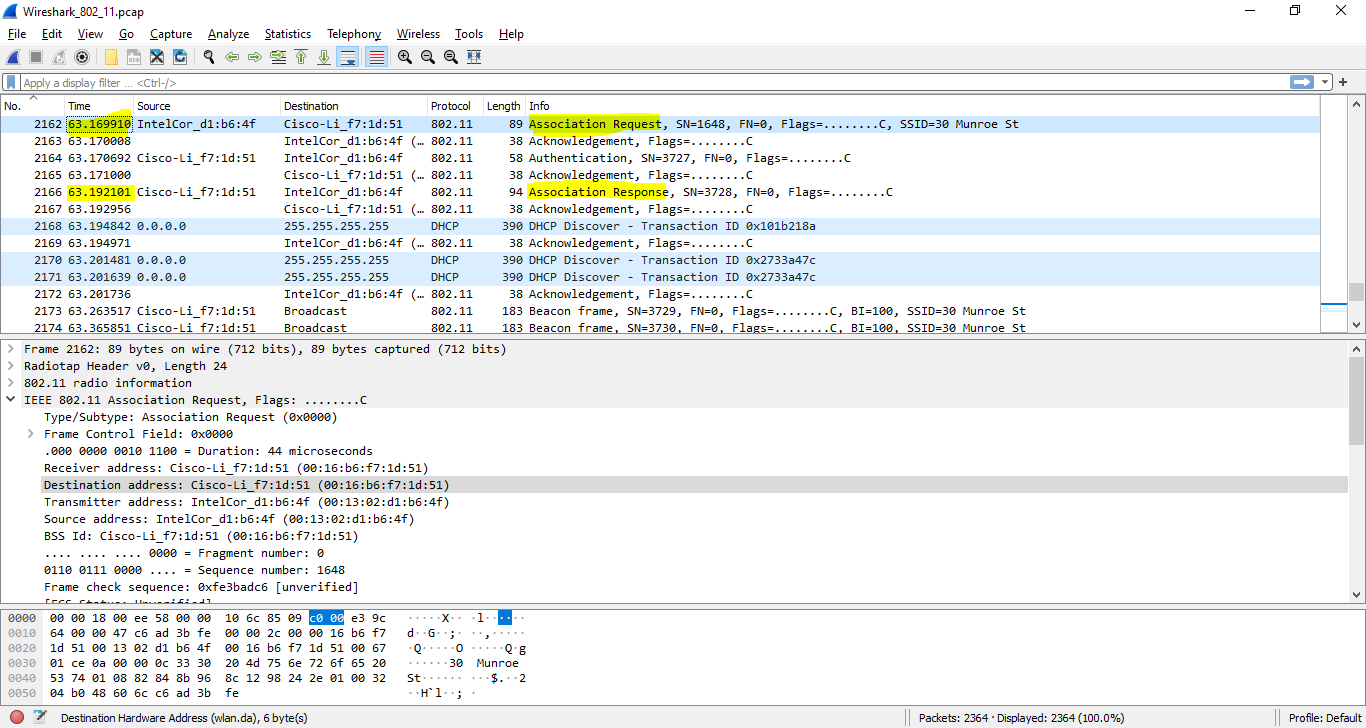


**Question 14:** An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe StAP? When is the corresponding ASSOCIATE REPLY sent? (Note that you 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:**

ASSOCIATE REQUEST from host to the 30 Munroe St AP at **t = 63.169910**

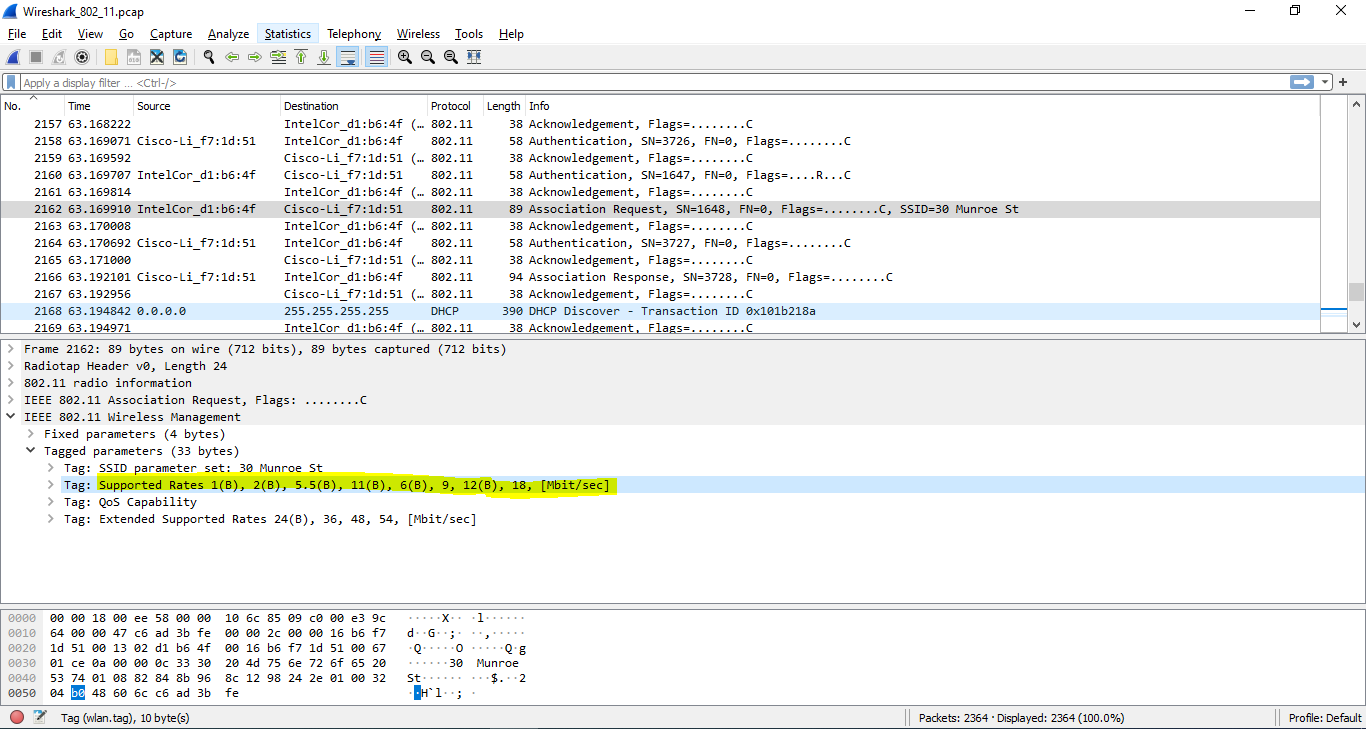
Corresponding reply sent at **t = 63.192101**



**Question 15:** 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:**

The possible rates are 1, 2, 5.5, 11, 6, 9, 12, 18 Mbps



**4. Other Frame types**

**Question 16:** 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).

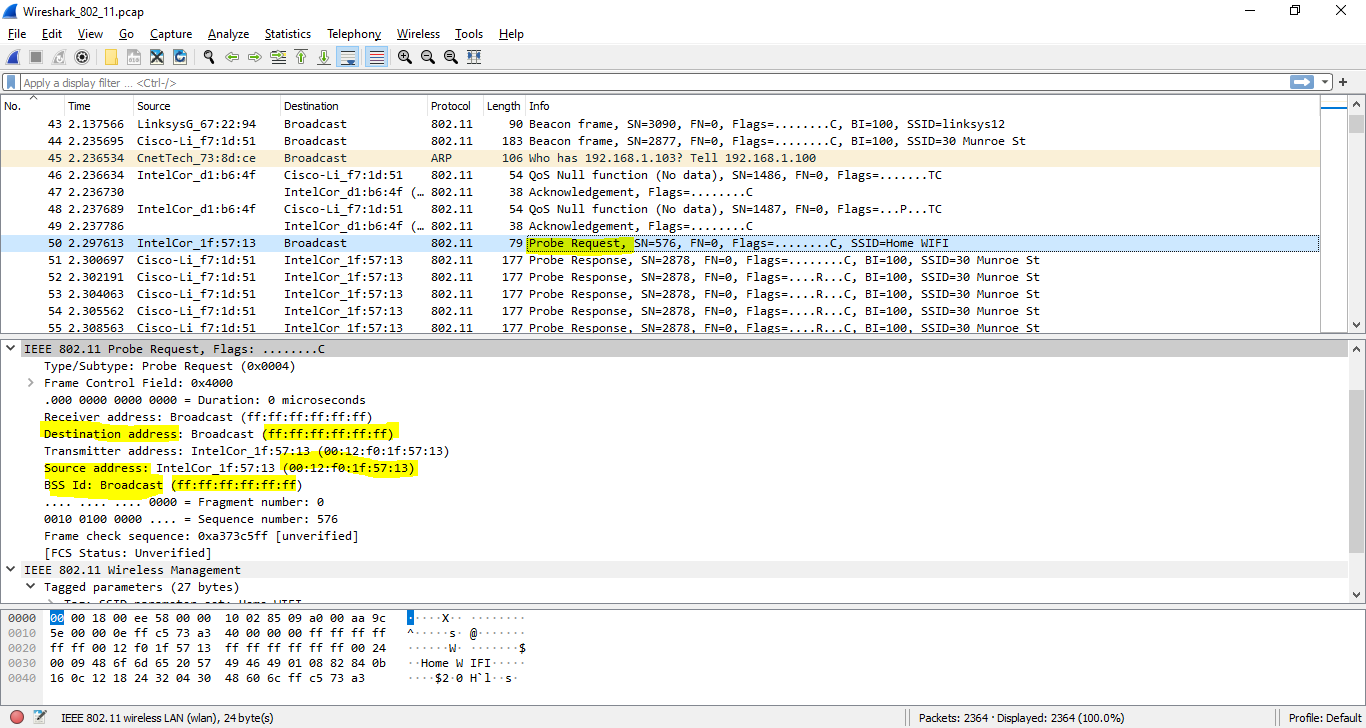
**ANSWER:**

Probe request:

+ Source: 00:12:f0:1f:57:13

+ Destination: ff:ff:ff:ff:ff:ff

+ BSSID: ff:ff:ff:ff:ff:ff

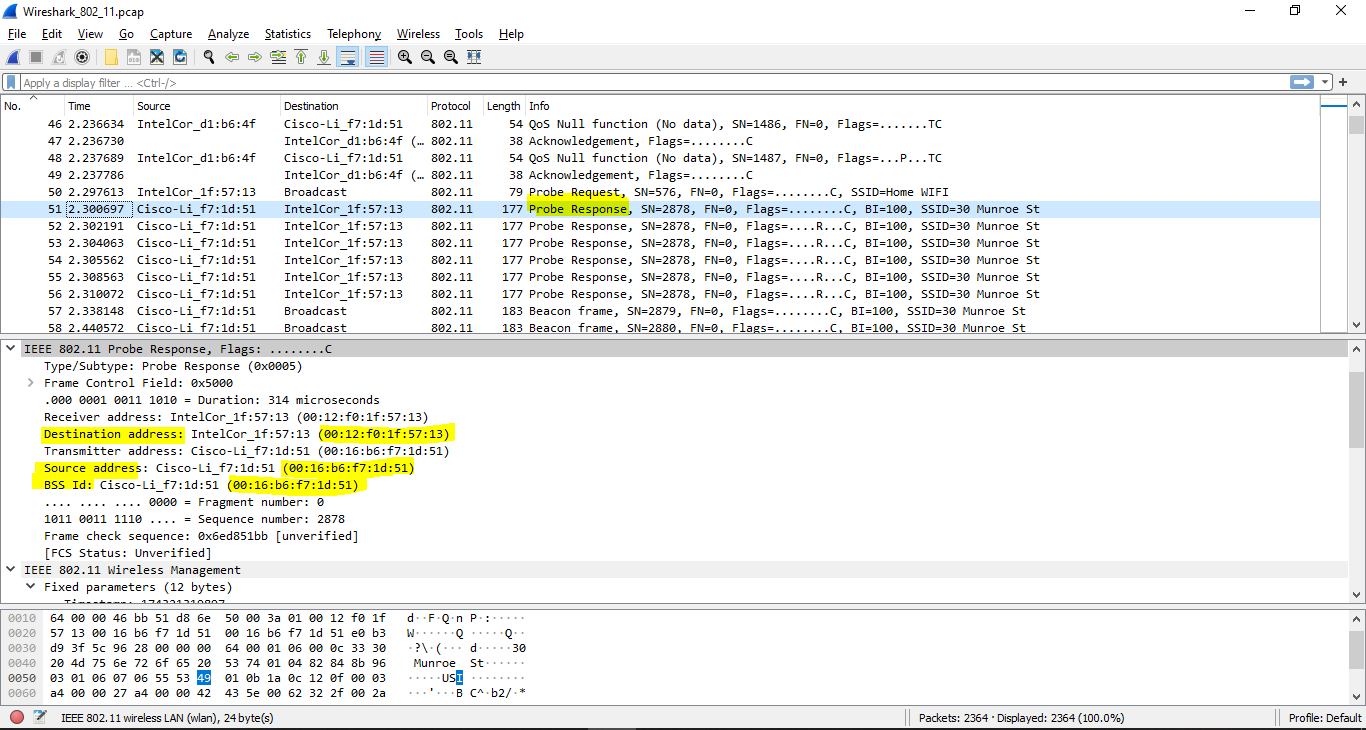


Probe response:

+ Source: 00:16:b6:f7:1d:51

+ Destination: 00:12:f0:1f:57:13

+ BSSID: 00:16:b6:f7:1d:51



The probe request is a broadcast to scan for an access point from the host. The probe response is used to response the host from the access point