**Assignment 12: Wireshark Lab: 802.11 WiFi**

**210010020**

Part1:

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

A] .The two access points that are issuing most of the beacon frame have an SSID of “linksys12” and “30 Munroe St”.

1. What are the beacon intervals in the *linksys\_ses\_24086* access point and the *30 Munroe St*. access point?

A] Beacon Interval of the 802.11 wireless LAN Management frame as.**102400 seconds** for both the mentioned access points.

1. 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).

A] Source Address: 00:16:b6:f7:1d:51

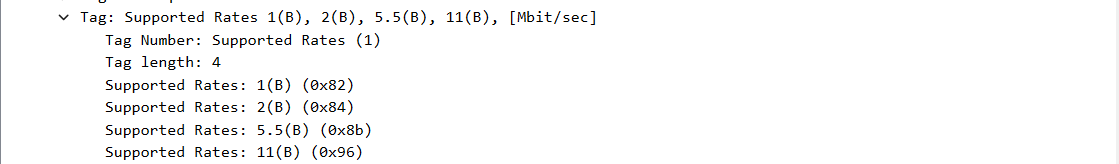
1. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*??

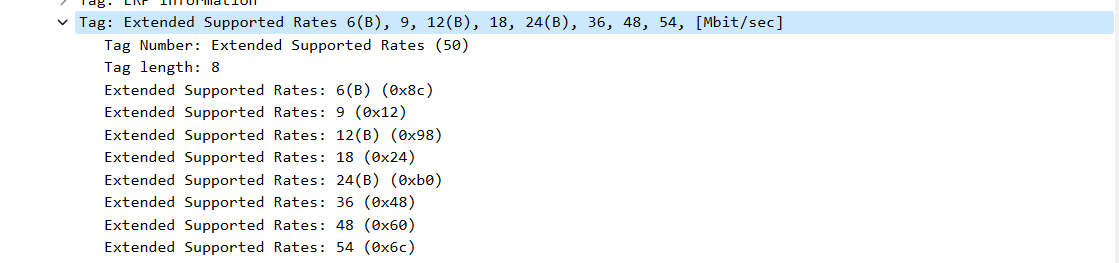
A] ff:ff:ff:ff:ff:ff this is the broadcast MAC Address of the beacon frame.

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

A] BSS Id: CiscoLinksys\_f7:1d:51 (00:16:b6:f7:1d:51) same as the source address.

1. 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?  
   A]   
   Data rates:

  
Extended supported rates:

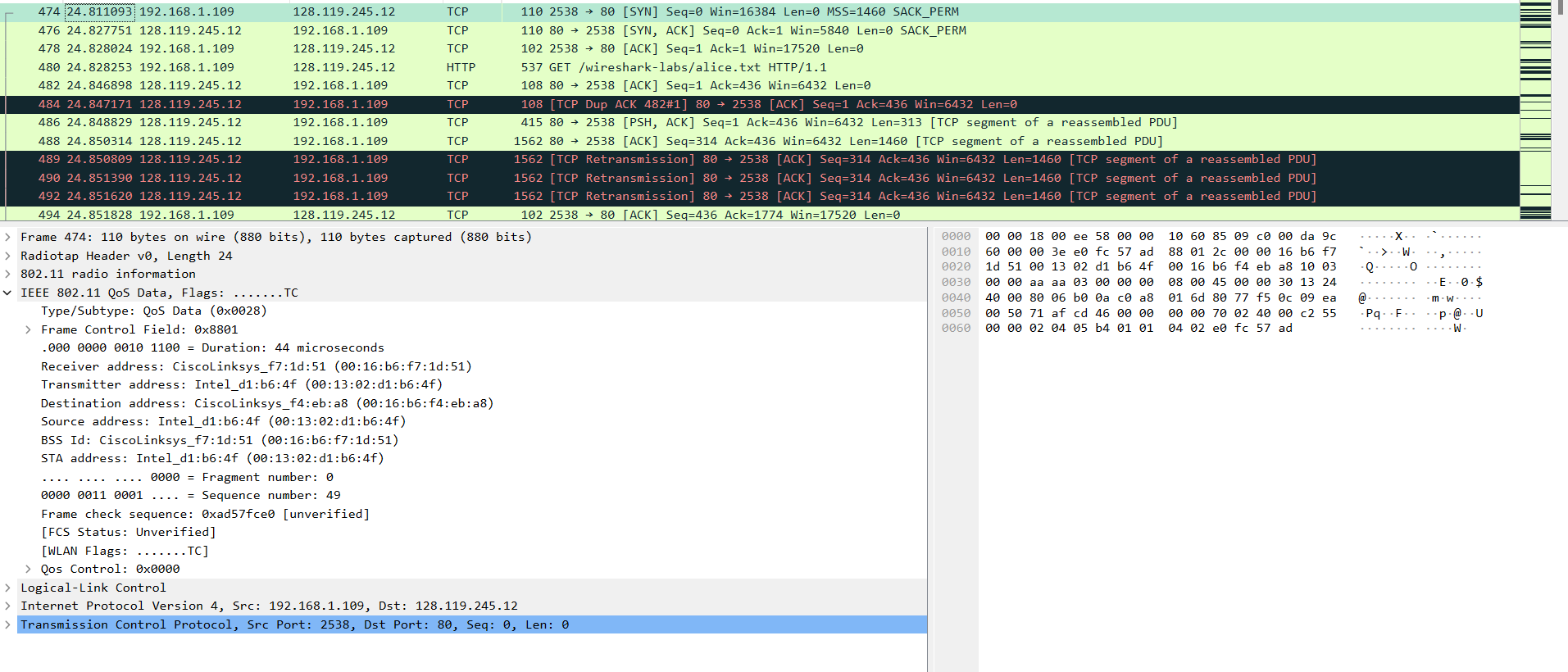


Part 2

1. 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?

A] The TCP SYN is sent at 24.81s. There are three addresses in the 802.11 frame: The

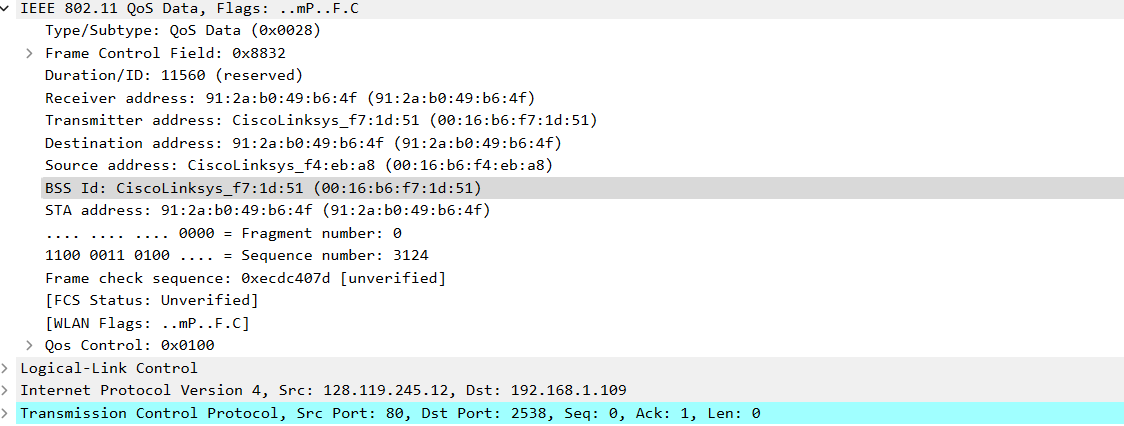
* Transmitter address = **00:13:02:d1:b6:4f** this is the source address.
* Receiver address **= 00:16:b6:f7:1d:51**
* MAC address for the destination, which the first hop router to which the host is connected, is **00:16:b6:f4:eb:a8.**
* The MAC address for the BSS is 00:16:b6:f7:1d:51. The IP address of the host sending the TCP SYN is 192.168.1.109.
* The IP address of wireless host sending TCP segment is 192.168.1.109 and that f destination is 128.119.245.12.



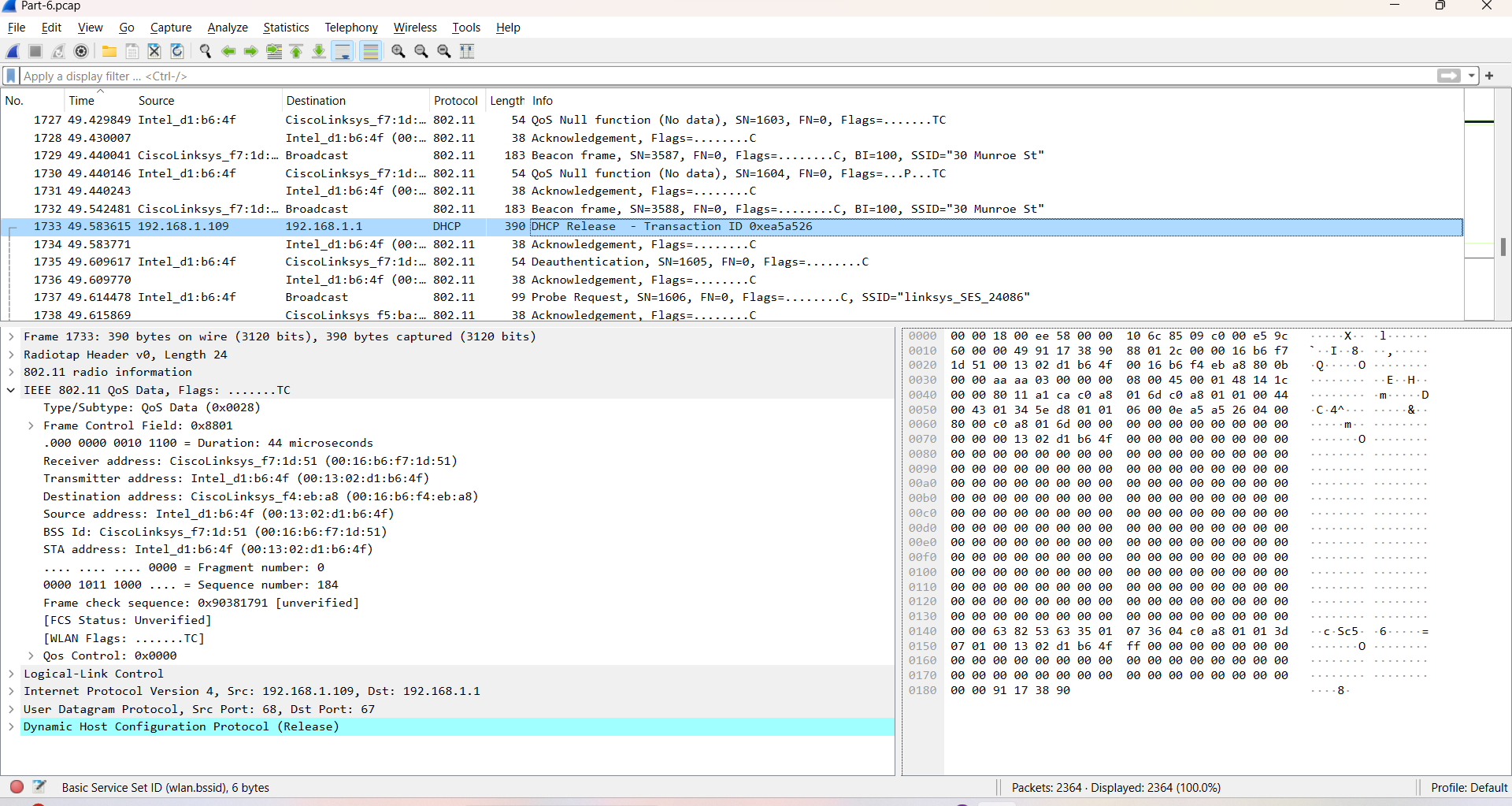
1. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which of these are the MAC addresses corresponding to the host sending SYNACK, destination and BSS? What is the IP address of the server sending the TCP SYNACK?

A]

* Sending address / source address : 00:16:b6:f4:eb:a8. Mac address of first hop router.
* destination address / receiver address : 91:2a:b0:49:b6:4f.
* BSS Id & Transmitter address: 00:16:b6:f7:1d:51  
  IP address of server sending TCP SYN ACK: 128.119.245.12



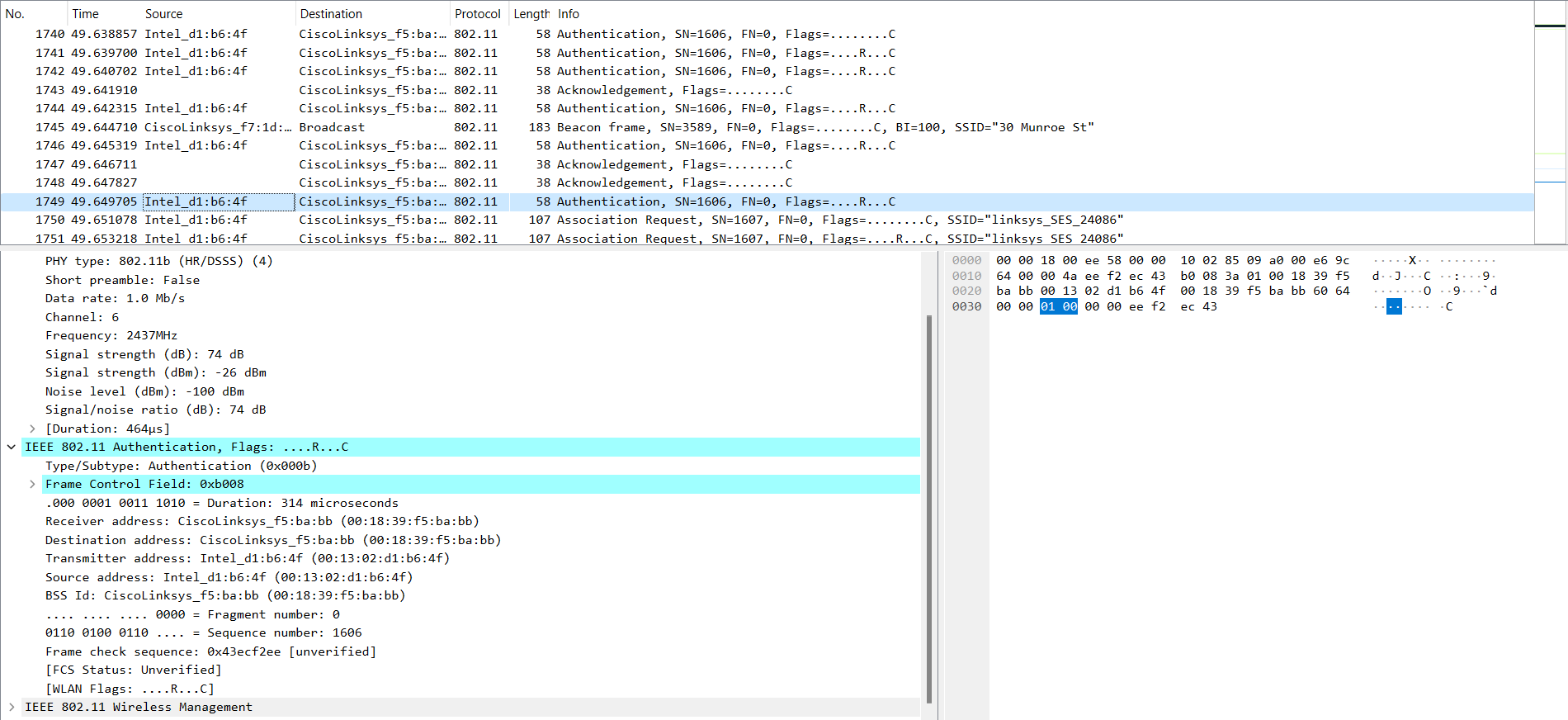
Part3:

1. 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?  
   A]   
   

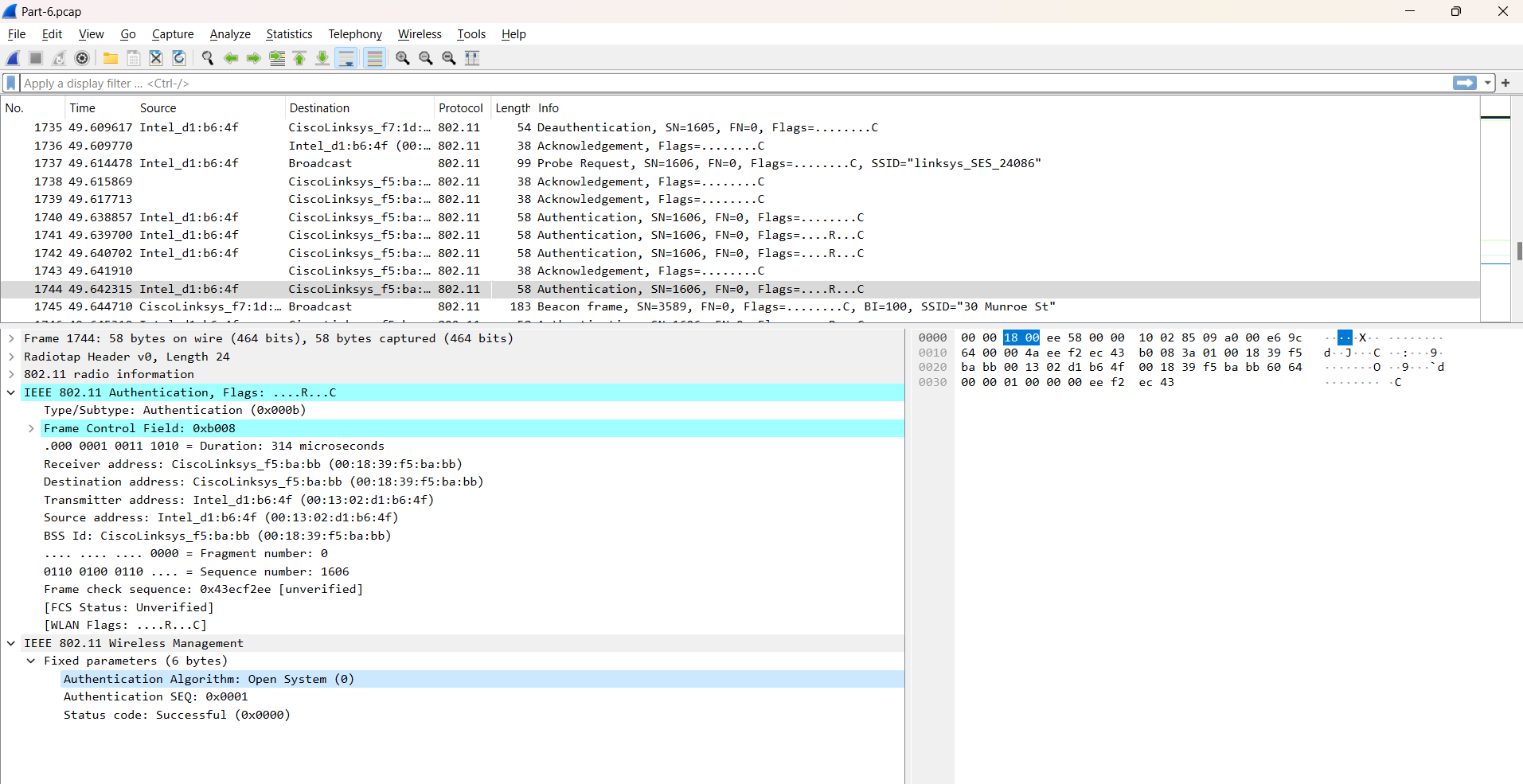
* At t=49.58 a DHCP release message is sent with an option as end to the server with   
  IP address as can be seen in the UDP Dst: 192.168.1.1. The host is releasing its IP address back to the DHCP server, and is exiting the network.
* At t=49.609617, Deauthentication is done, to terminate a Wi-Fi Connection.
* Expected to observe a DISASSOCIATION request, but that is not observed here

1. 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?*

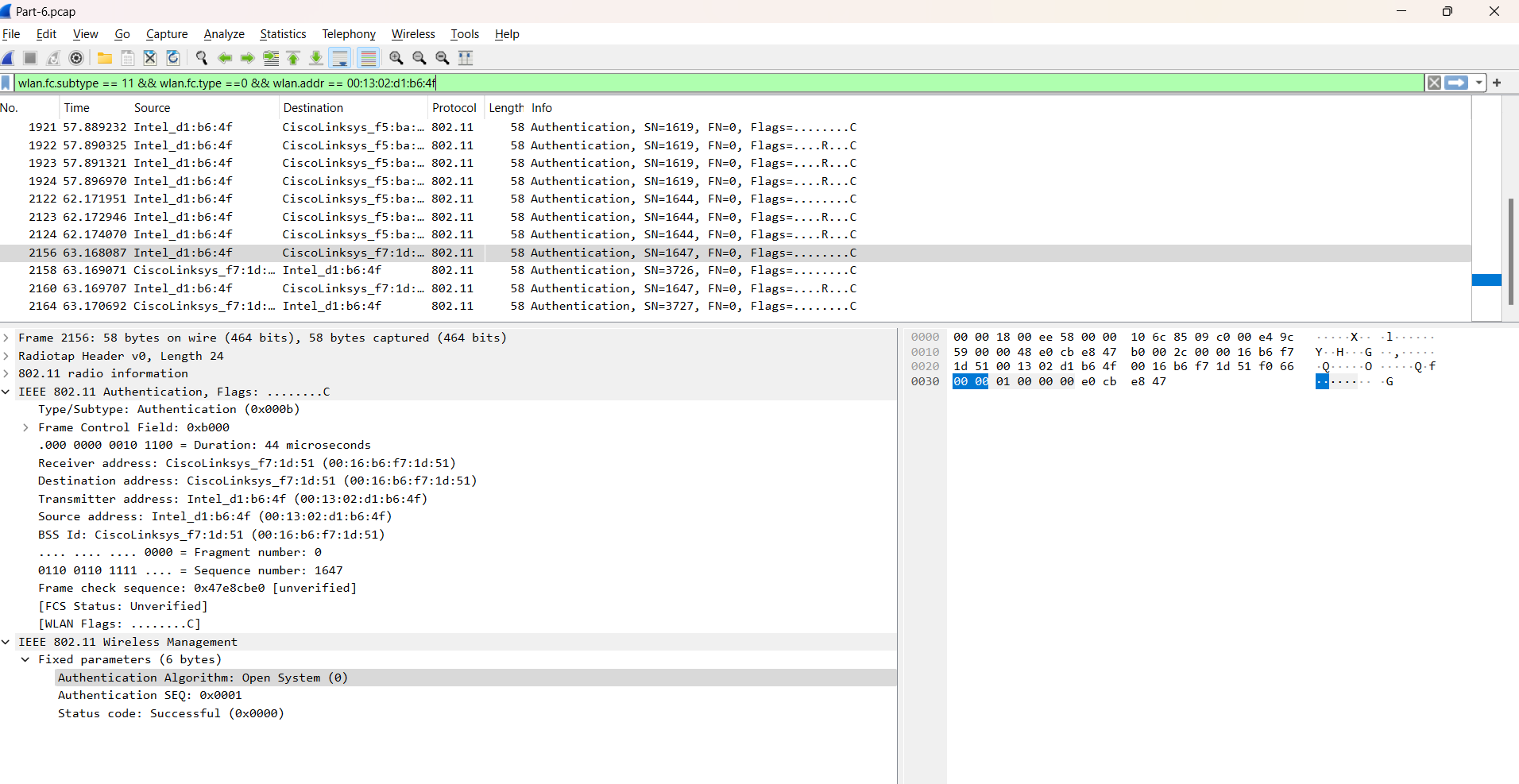
A] There are 6 AUTHENTICATION messages are sent from the wireless host to the linksys ses\_24086. Note that the first AUTHENTICATION frame sent out successfully was observed to be at time t = 49.639705



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

A] The host does not require any authentication key as it is open.

1. Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?  
   A] No there is no reply that can be seen.
2. 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 an AP and vice versa. At what times is there an AUTHENTICATION frame from the host to 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host reply? (Note that you can use the filter expression “wlan.fc.subtype == 11 && wlan.fc.type == 0 && wlan.addr == IntelCor\_d1:b6:4f” to display only the AUTHENTICATION frames in this trace for this wireless host.)

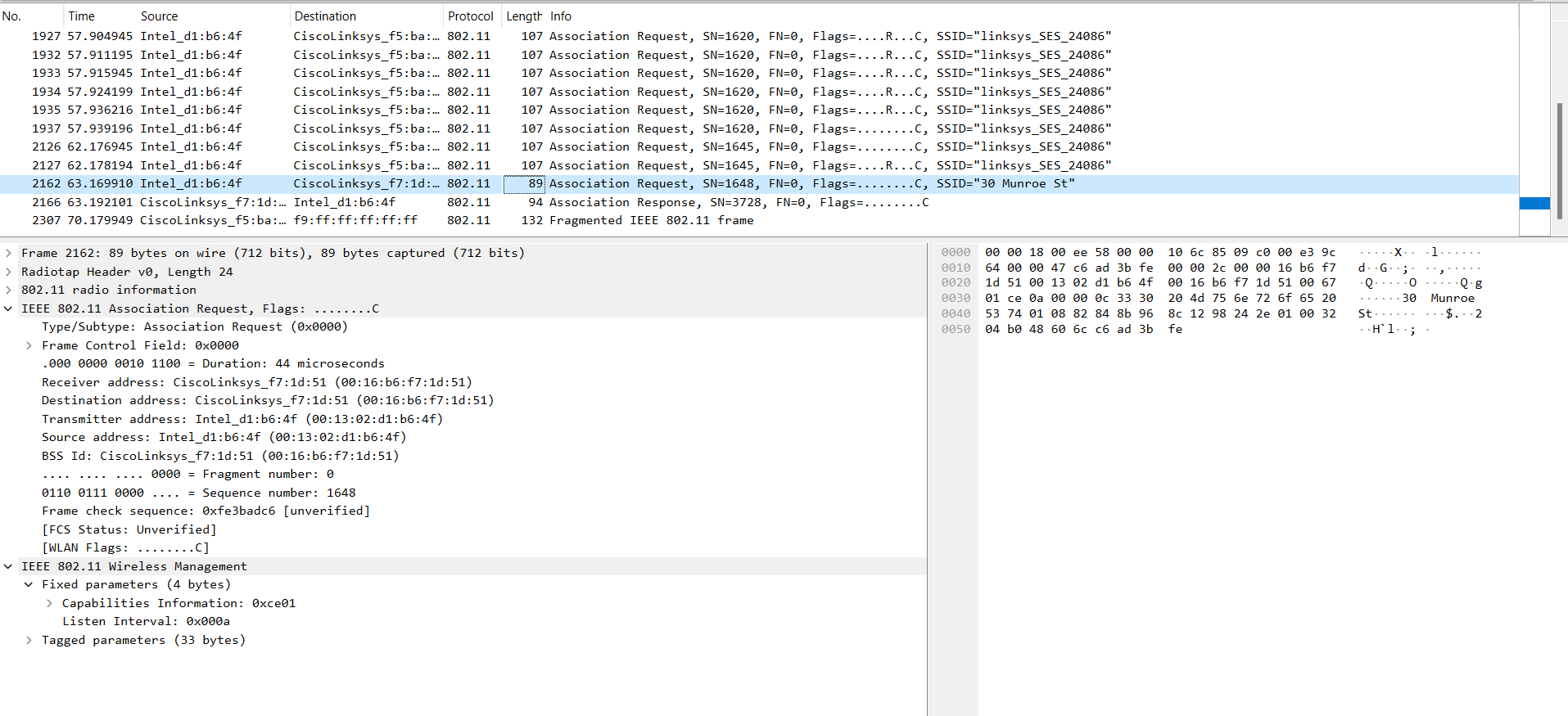
A]   


By using wlan.fc.subtype == 11 && wlan.fc.type ==0 && wlan.addr == 00:13:02:d1:b6:4f we can find that

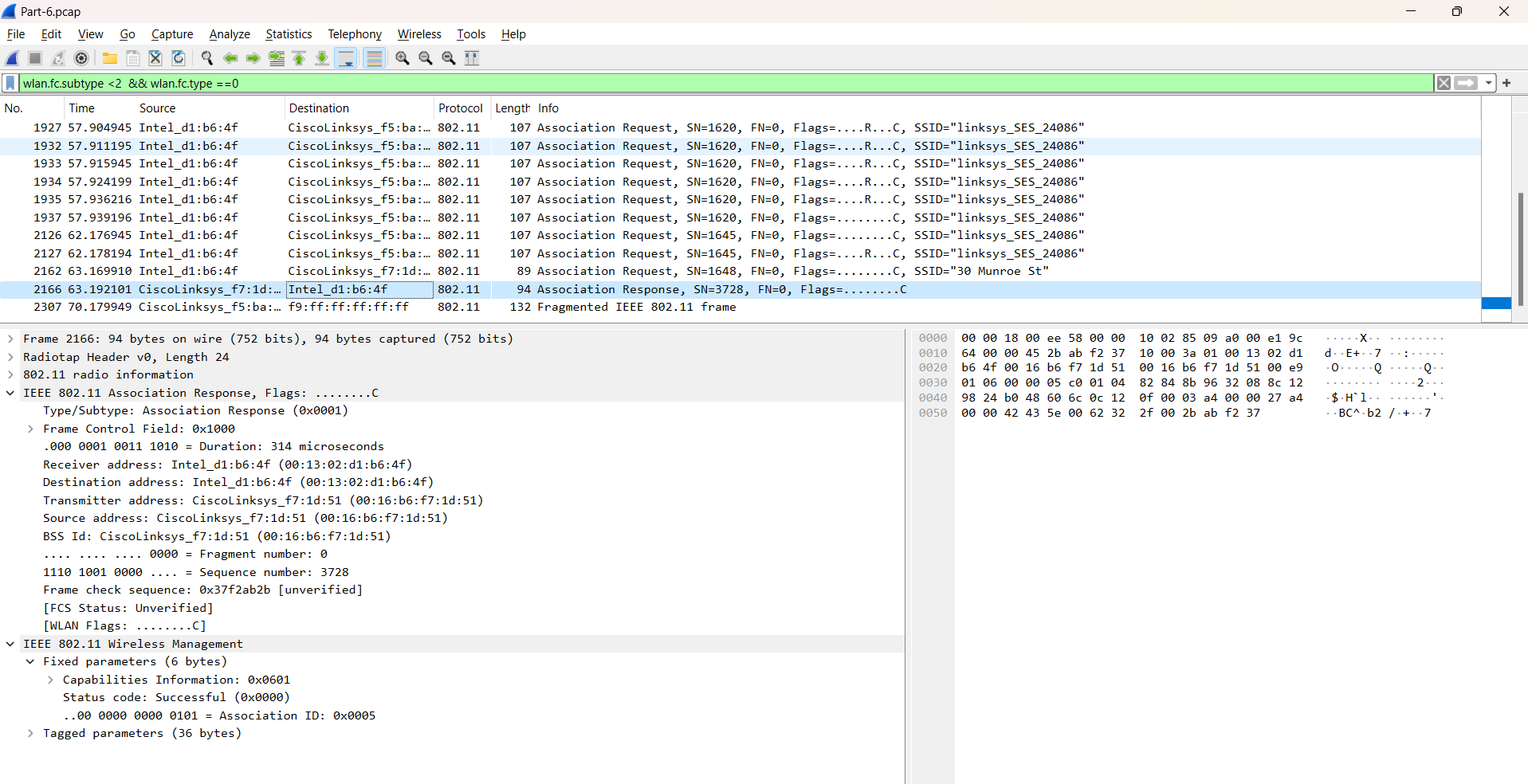
* T = 63.169071s Authentication is sent from Host to 30 Munroe ST
* T = 63.1697007s Authentication comes from 30 Munroe St to Host

1. An ASSOCIATE REQUEST from the host to AP and a corresponding ASSOCIATE RESPONSE frame from AP to the host is used for the host to be associated with an AP. At what time is there an ASSOCIATE REQUEST from the host to 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression “wlan.fc.subtype < 2 && wlan.fc.type == 0 && wlan.addr == IntelCor\_d1:b6:4f” to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

A] At t = 63.169910 there is a 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.

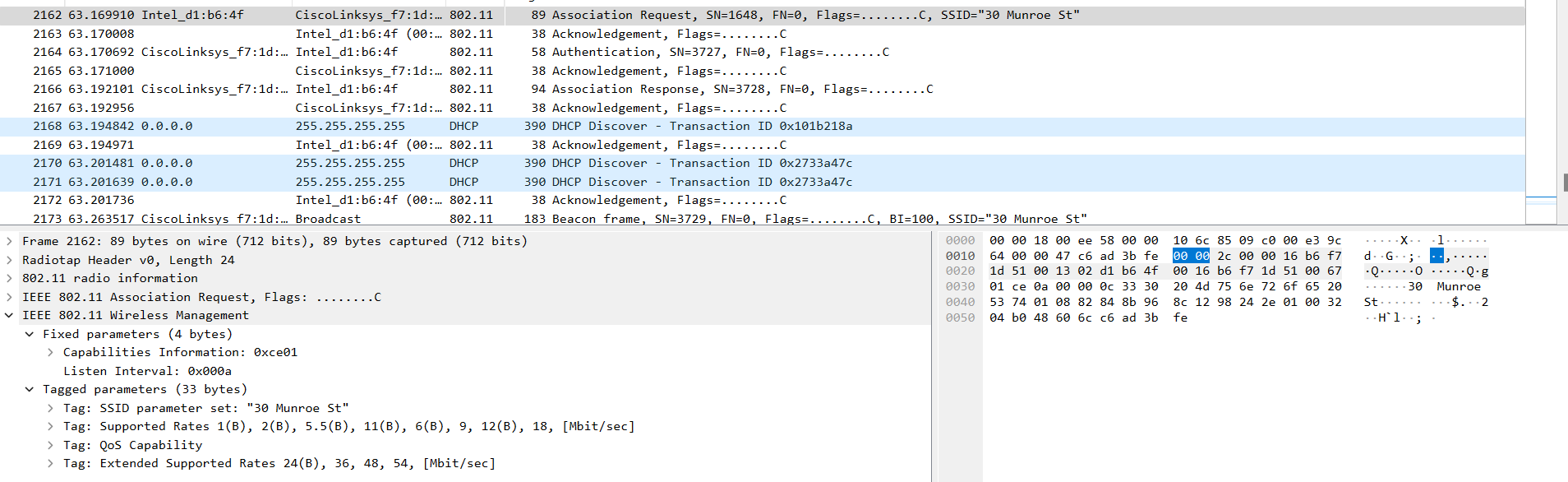


Rates given in response:



1. 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 A]

A] Supported transmission rates and extended transmission rates can be seen here.



Part-4: Other Frame types

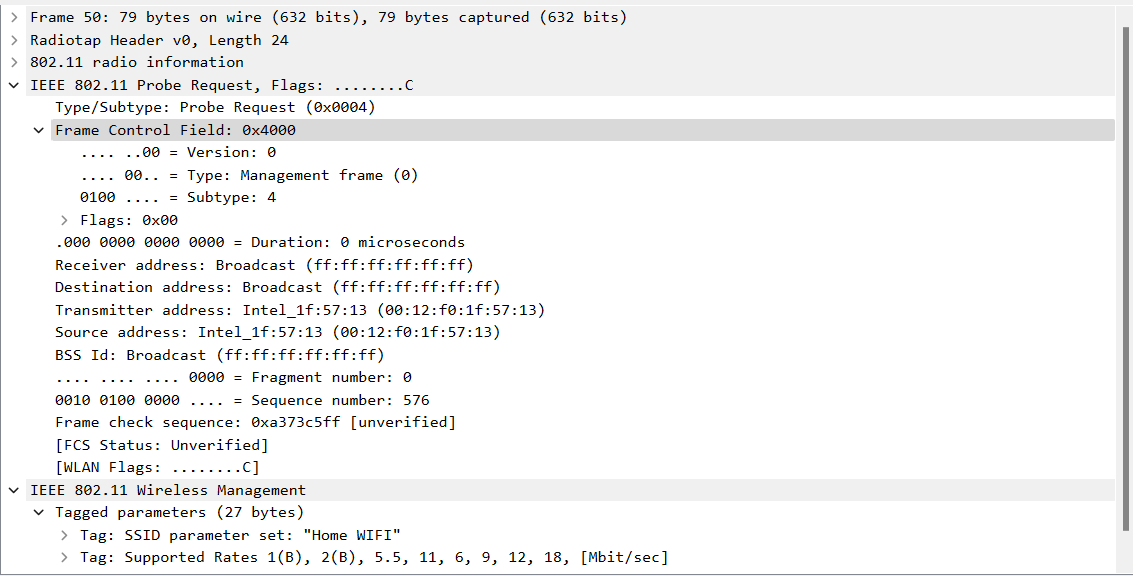
* 1. Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames. 1. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?

A] Probe request:

• Sender MAC address: 00:12:f0:1f:57:13 , which is the source address.

• Receiver MAC address: ff:ff:ff:ff:ff:ff , which is the Ethernet broadcast address.

• BSS ID MAC address: ff:ff:ff:ff:ff:ff , which is the Ethernet broadcast address



Probe Response:

* Sender MAC address: 00:16:b6:f7:1d:51 , which is the source address.
* Receiver MAC address: 00:12:f0:1f:57:13 , which is as seen in the Receiver Address field.
* BSS ID MAC address: 00:16:b6:f7:1d:51 , which is the as seen in the BSS ID field.

