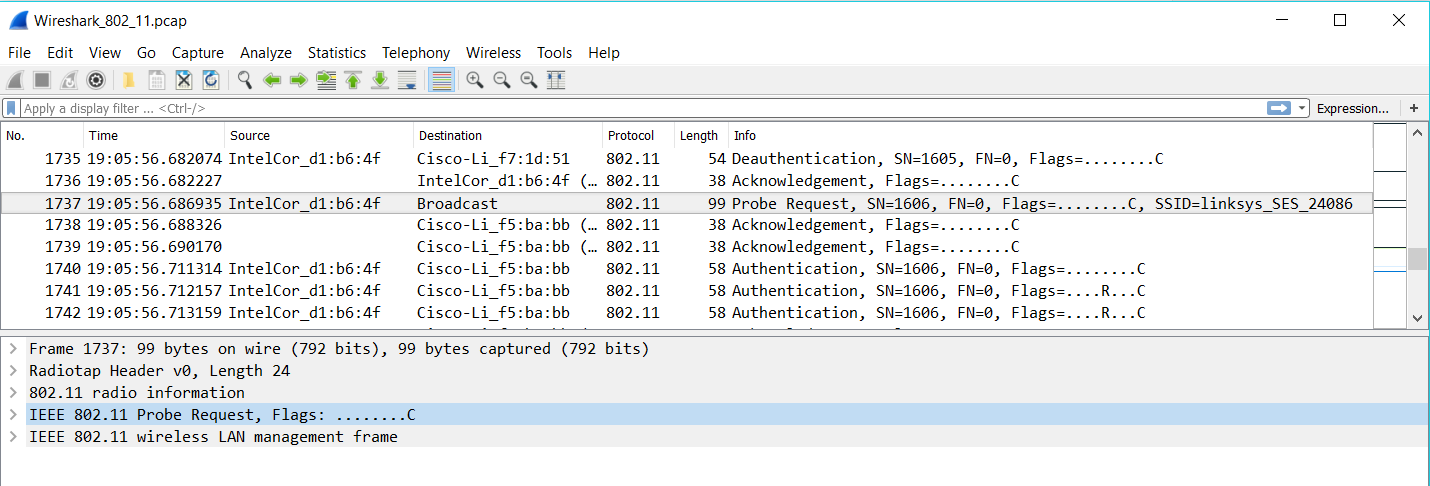
Broc Nickodemus

Lab6

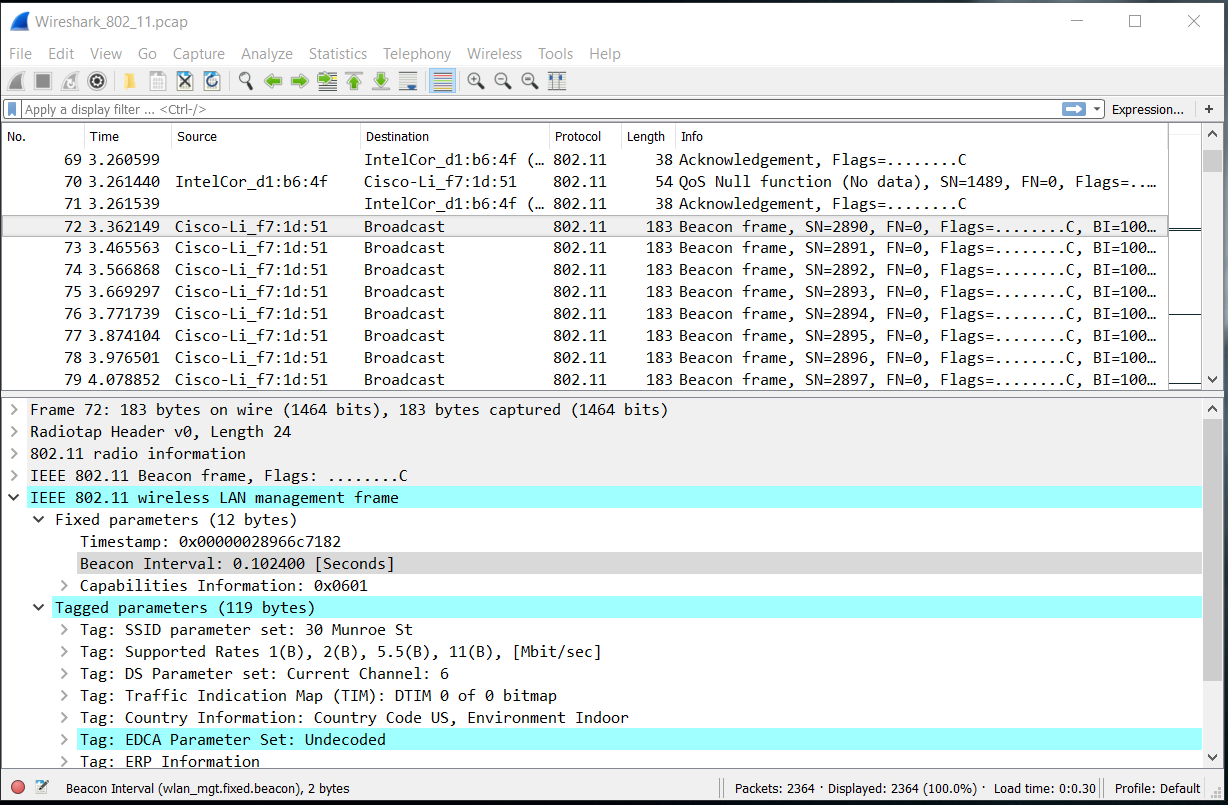
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

30 Munroe St and linsys\_SES\_24086



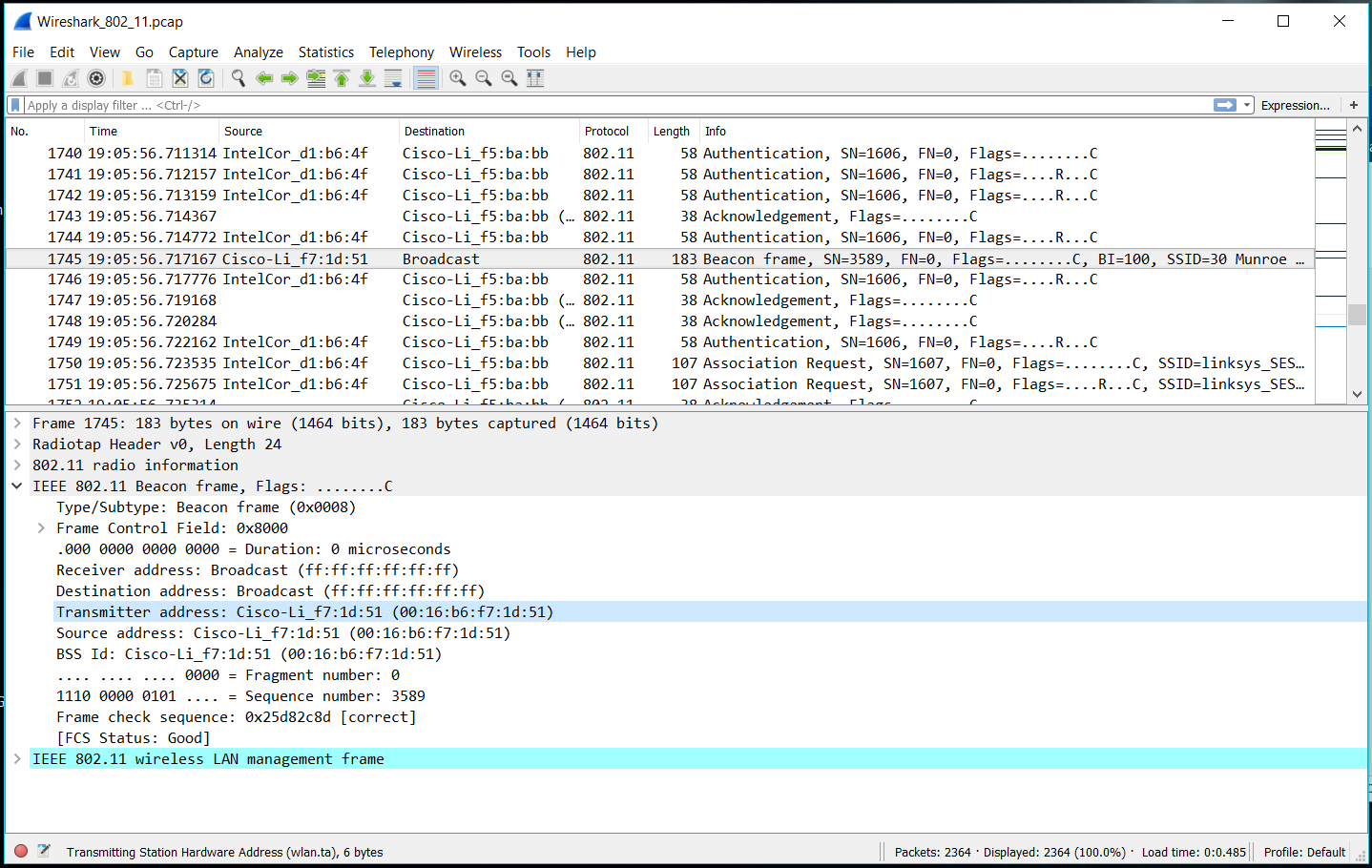
2. What are the intervals of time between the transmissions of the beacon frames the *linksys\_ses\_24086* access point? From the *30 Munroe St*. access point? (Hint: this interval of time is contained in the beacon frame itself).

They are both 0.1024 seconds



3. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 6.13 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).

The mac address is 00:16:b6:f7:1d:51



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

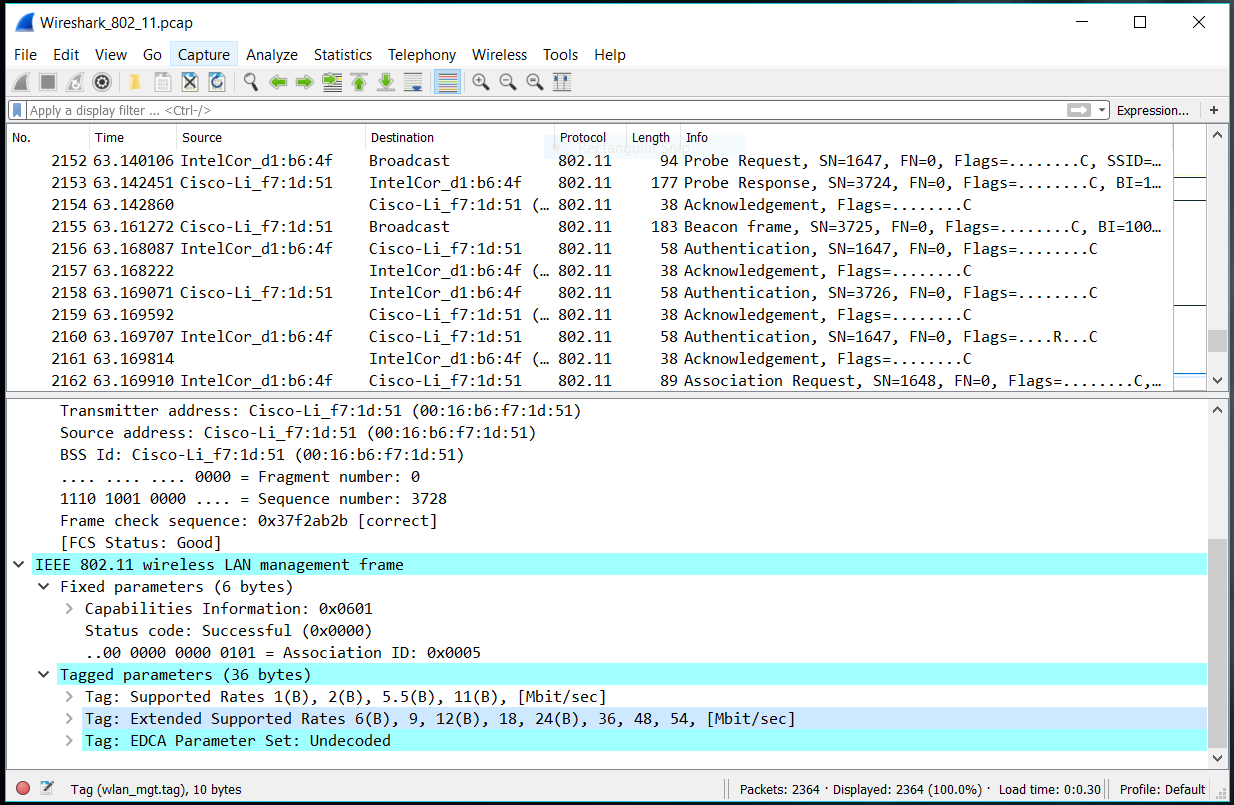
The destination mac address is ff:ff:ff:ff:ff:ff

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

The mac bss id is 00:16:b6:f7:1d:51

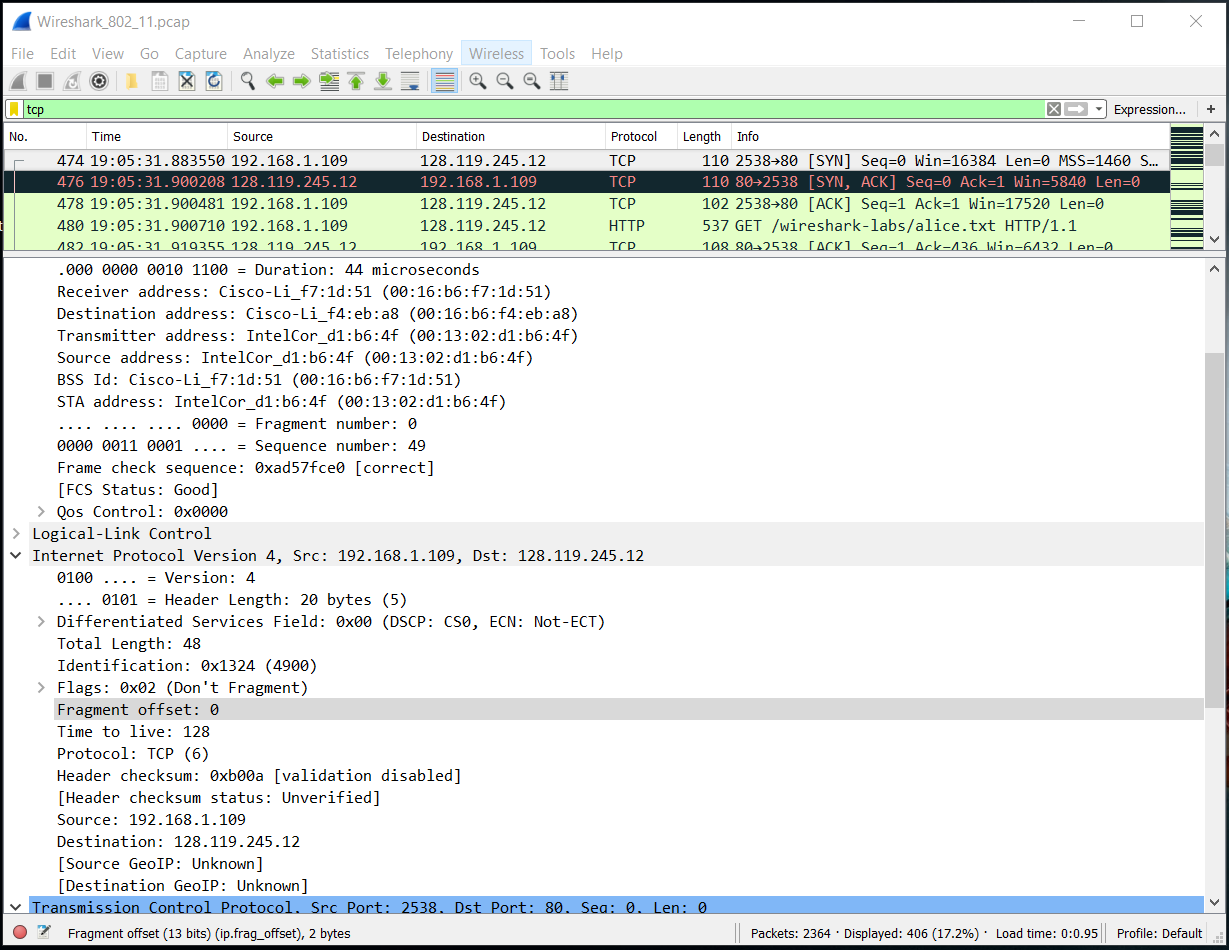
6. The beacon frames from the *30 Munroe St* access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?

The extended rates are 6, 9, 12, 18, 24, 36, 48, 54 mbps



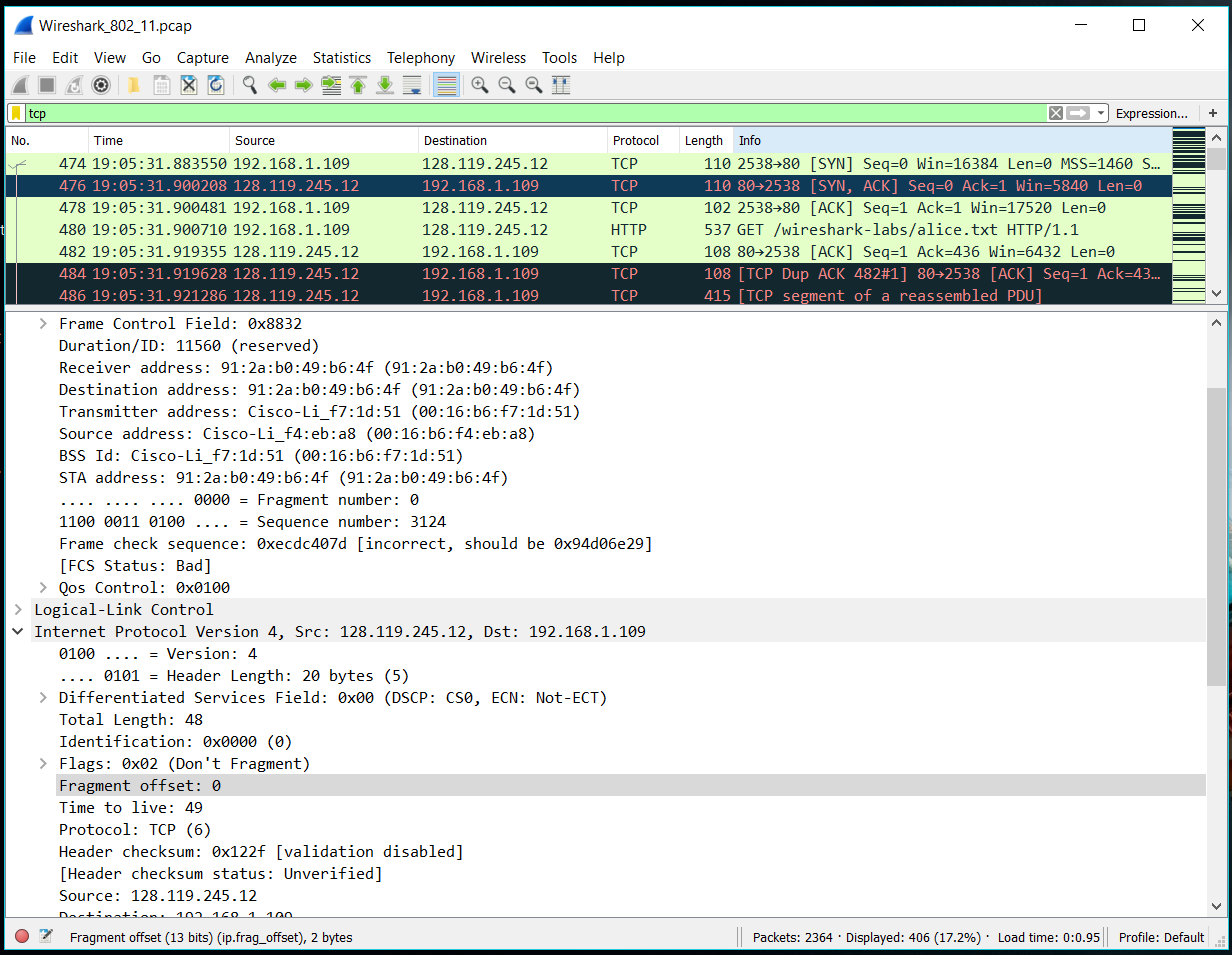
7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? 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.

The mac address of the host is 00:13:02:d11:b6:4f, the router host is 00:16:b6:f4:eb:a8, and the sender is 00:16:b6:f7:1d:71. The ip address of the sender is 192.168.1.109 and the receiver is 128.119.245.12. The destination ip corresponds to the server.



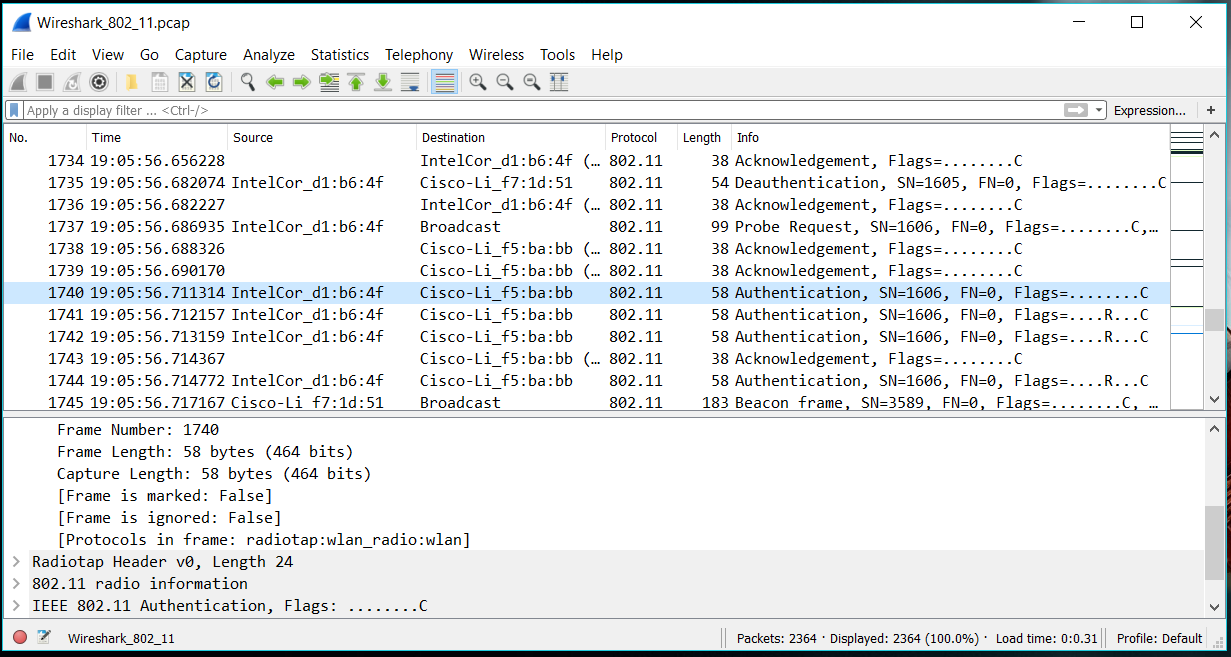
8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 5.19 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).

The bss mac is 00:16:b6:f7:1d:51, destination mac is 00:13:02:d1:b6:4f, the source mac is 00:16:b6:f4:eb:a8. The destination corresponds to the host (00:13:02:d1:b6:4f). the source mac address corresponds to the first hop (00:16:b6:f4:eb:a8), and the sender mac does not correspond to the ip of the device.



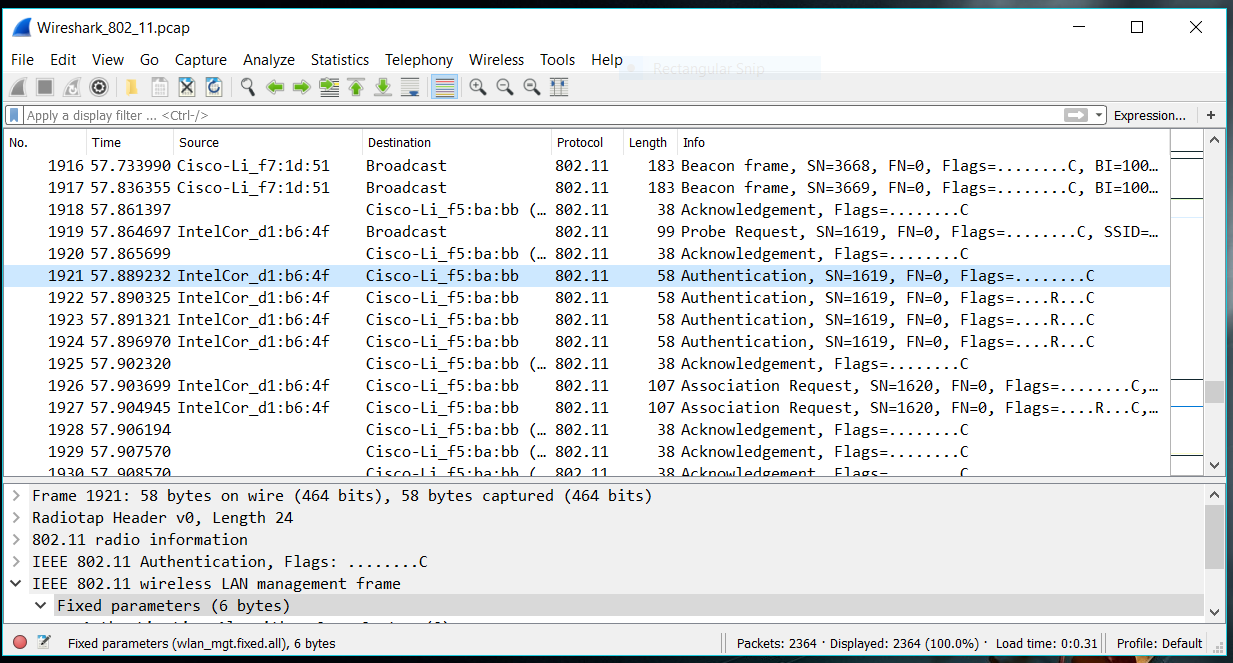
9. What two actions are taken (i.e., frames are sent) by the host in the trace just after *t=49*, to end the association with the *30 Munroe St* AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don’t see here?

A DHCP is sent and the host sends a deauthentication



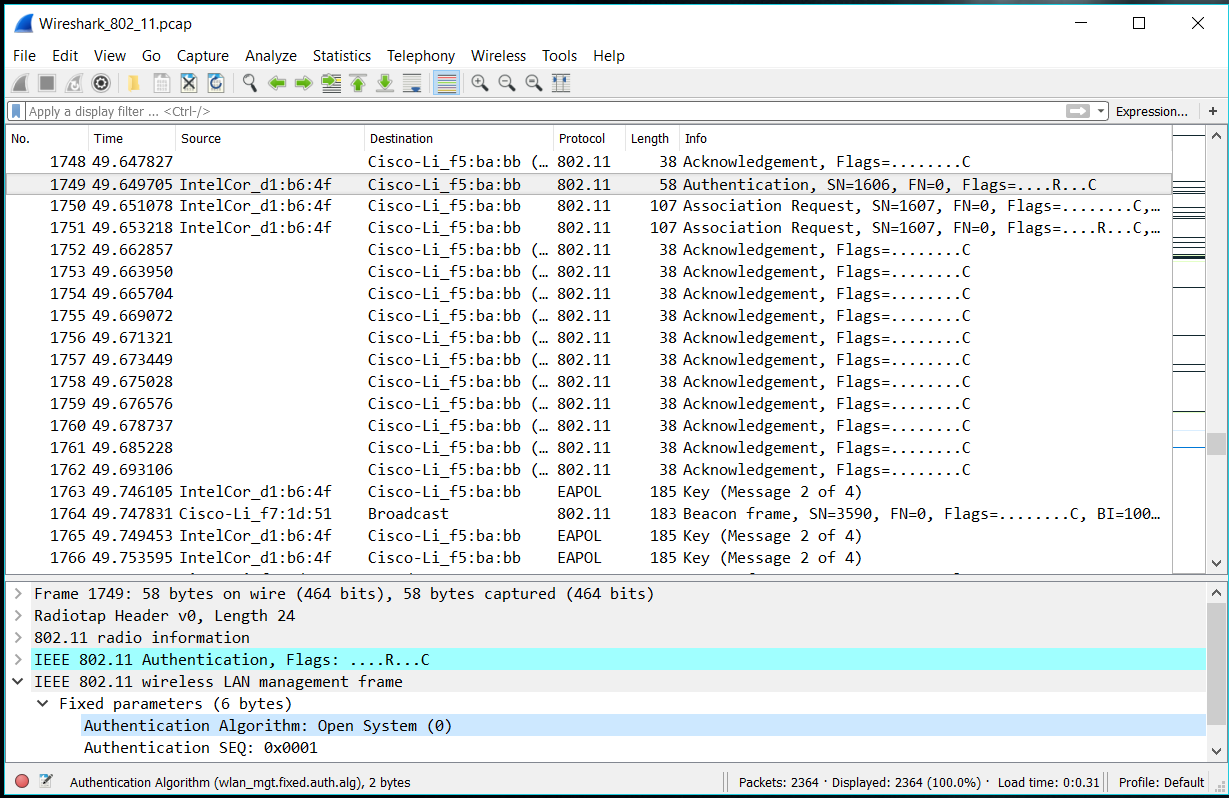
10. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the *linksys\_ses\_24086* AP (which has a MAC address of Cisco\_Li\_f5:ba:bb) starting at around *t=49?*

I counted 10 but there could be more.



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

The host wants the authentication to be an open system

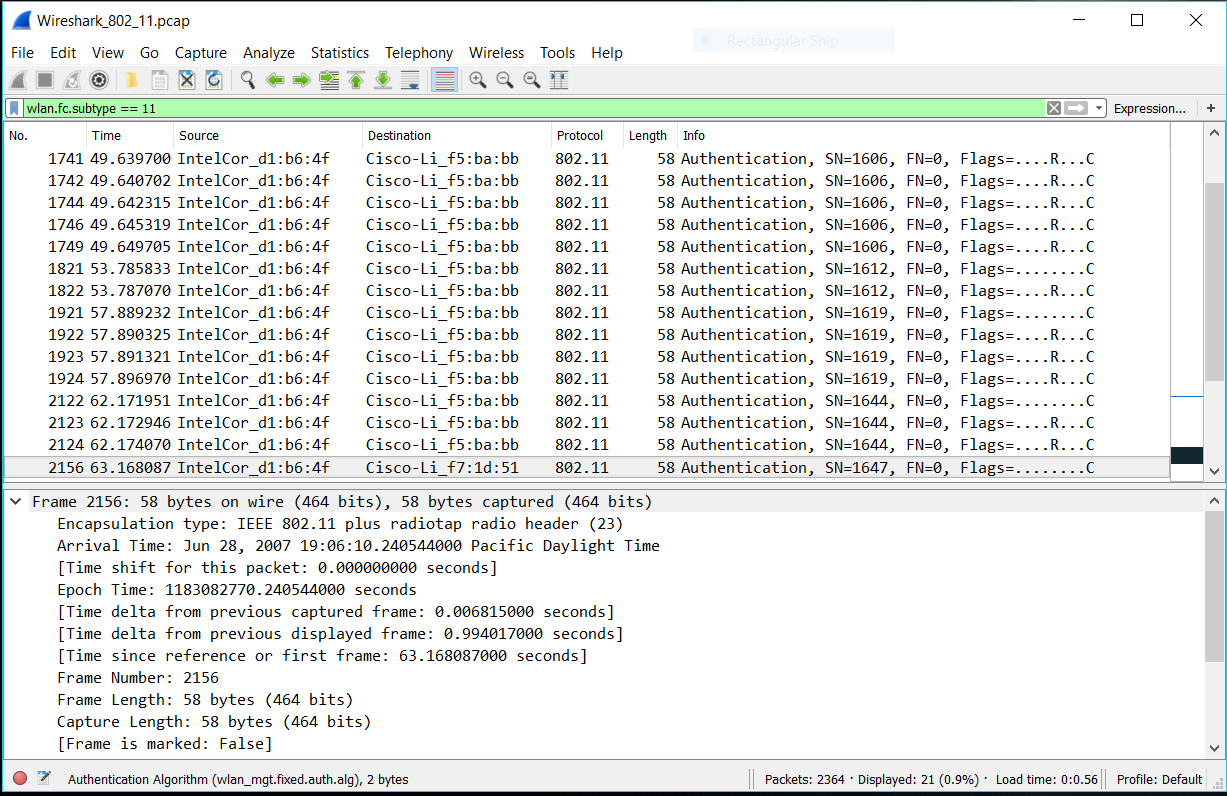


12. Do you see a reply AUTHENTICATION from the *linksys\_ses\_24086* AP in the trace?

I don’t see a reply authentication from *linksys\_ses\_24086*

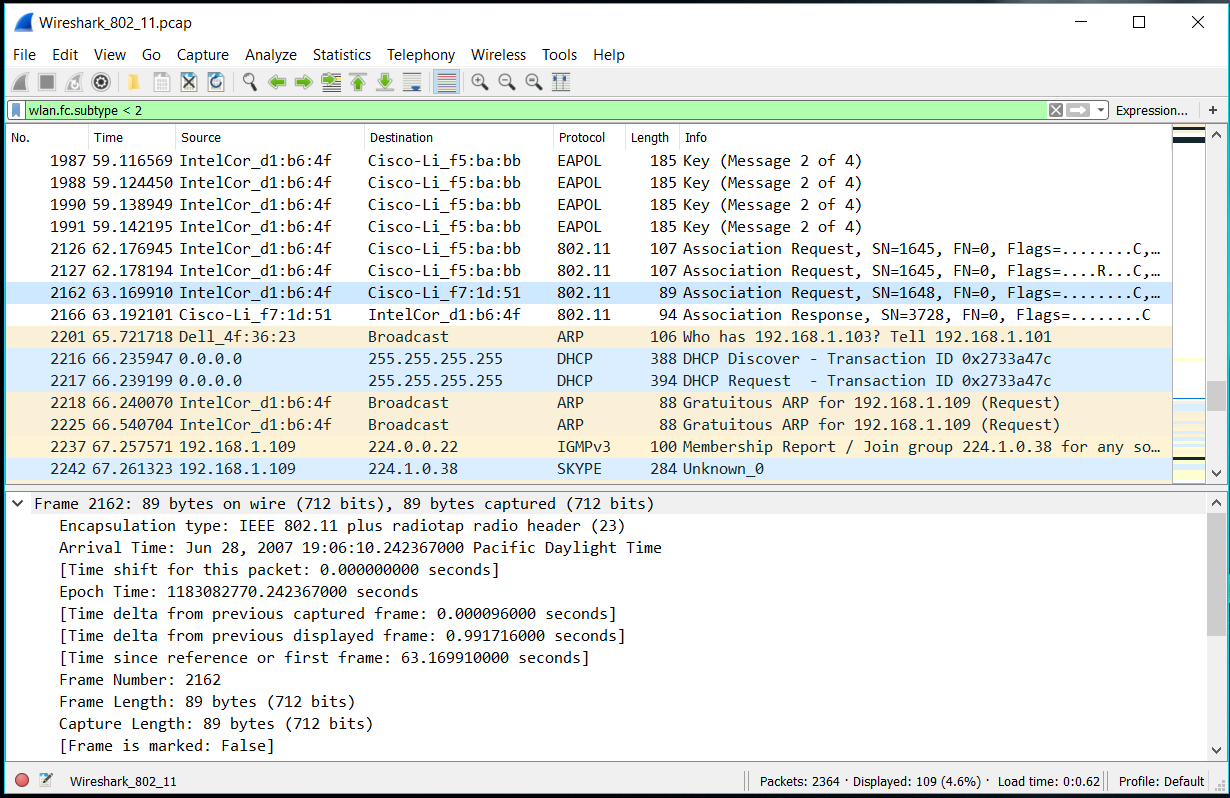
13. Now let’s consider what happens as the host gives up trying to associate with the *linksys\_ses\_24086* AP and now tries to associate with the *30 Munroe St* AP. Look for AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the *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.)

When the time is 63.169071 there is a frame sent from the bss to the host, when the time is 63.168087 there is a frame in the opposite direction.



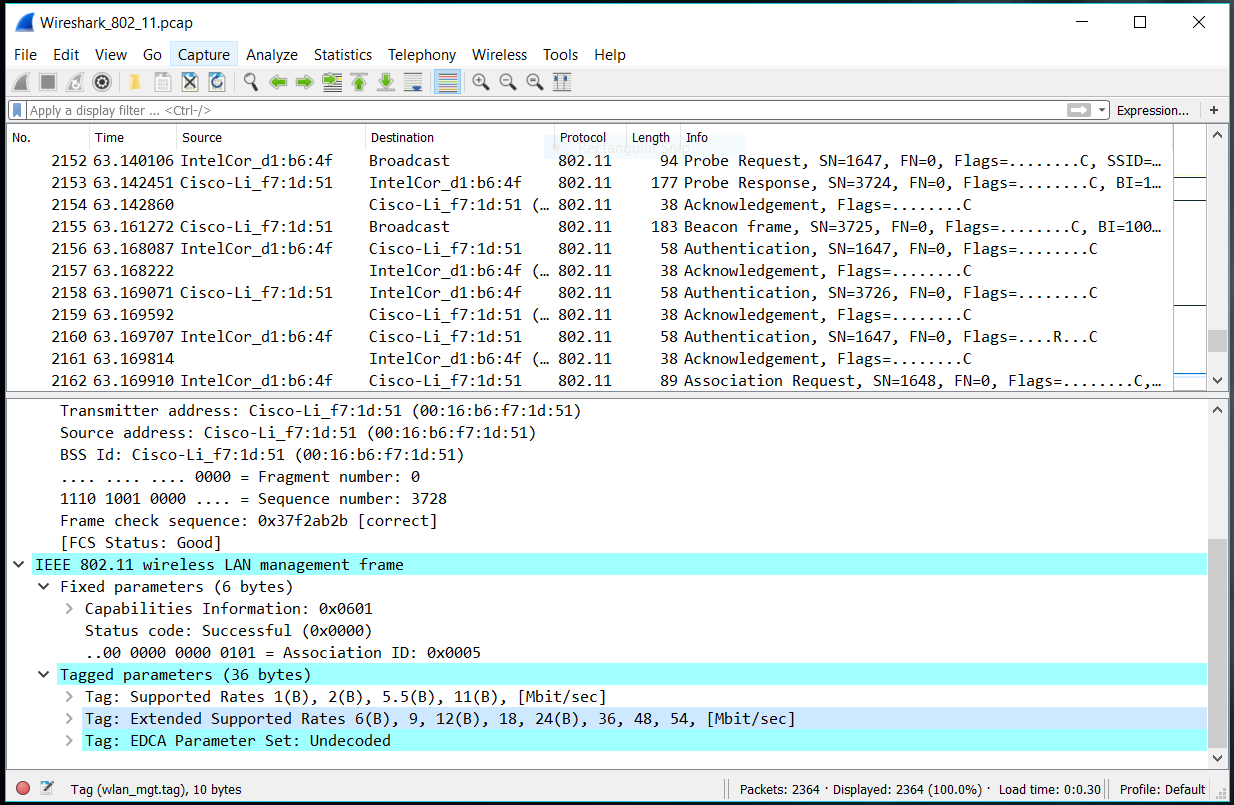
14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the *30 Munroe St* AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use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

The associate request from host to 30 Munroe St happens at time 63.169910 and replied at time 63.192101



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.

The rates are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, 54 mbps



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).

A probe request is sent with a source of 00:12:f0:1f:57:13, a destination of ff:ff:ff:ff:ff:ff, and a bss of ff:ff:ff:ff:ff:ff . A probe request is used to find an access point. A probe response is then sent back to the host.

