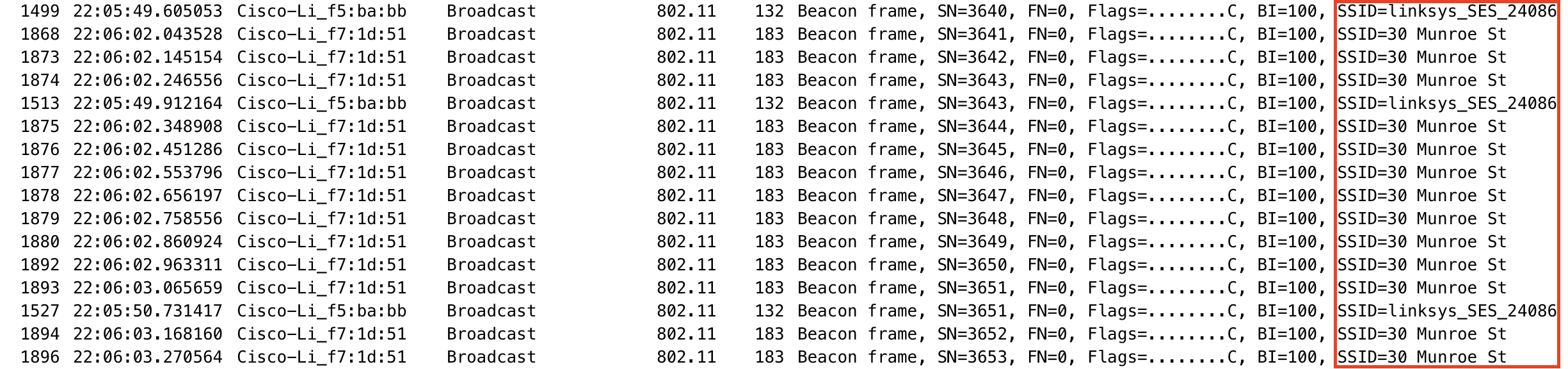
CSCE 560

2nd Lt David Crow

Wireshark Lab 6

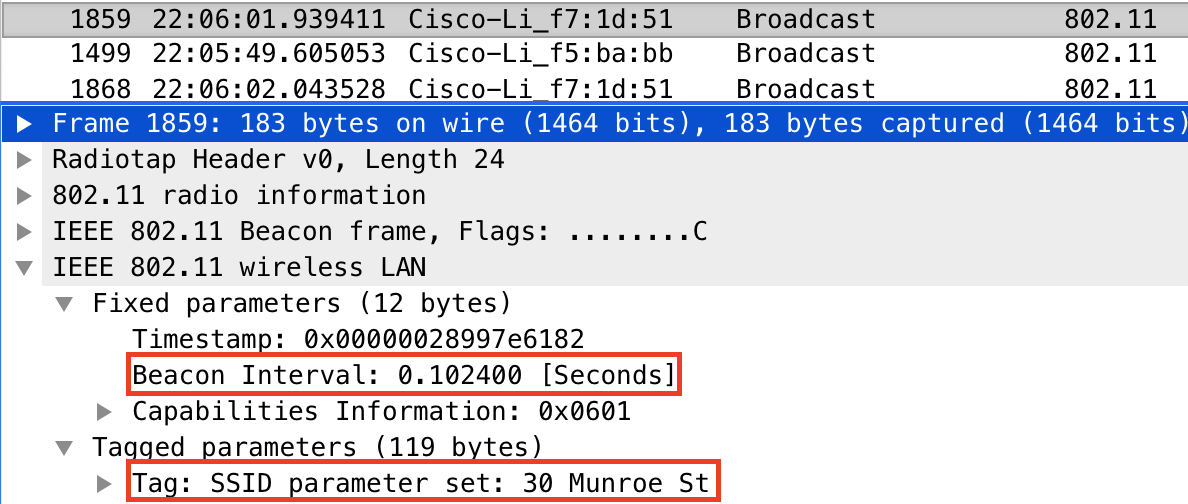
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

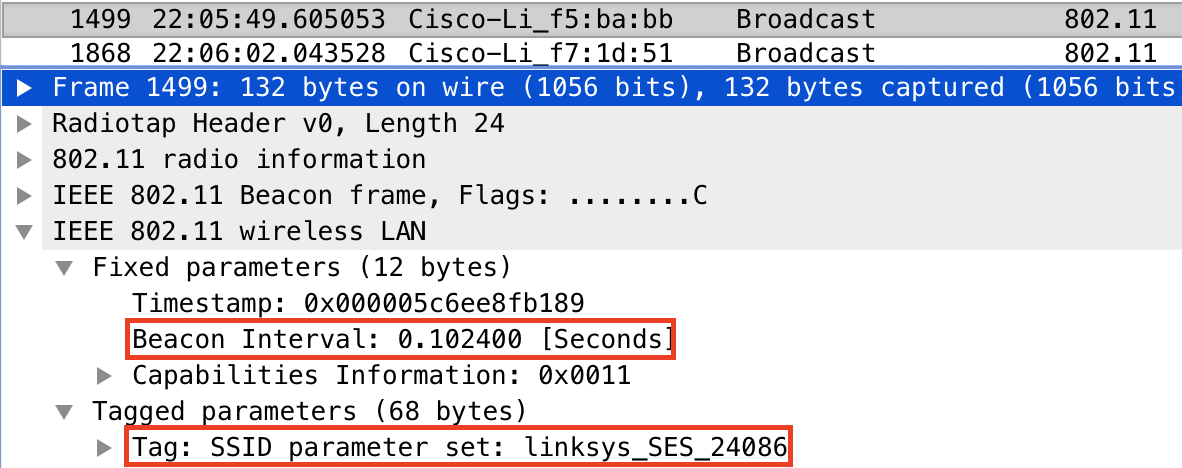
The SSIDs are “30 Munroe St” and “linksys\_SES\_24086.”



1. 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.)

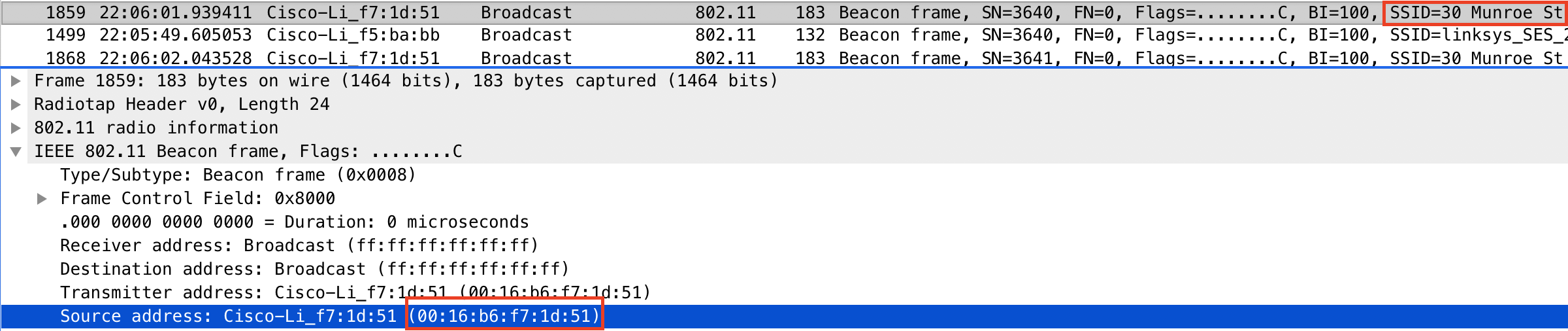
The intervals are both set to 0.1024 seconds.





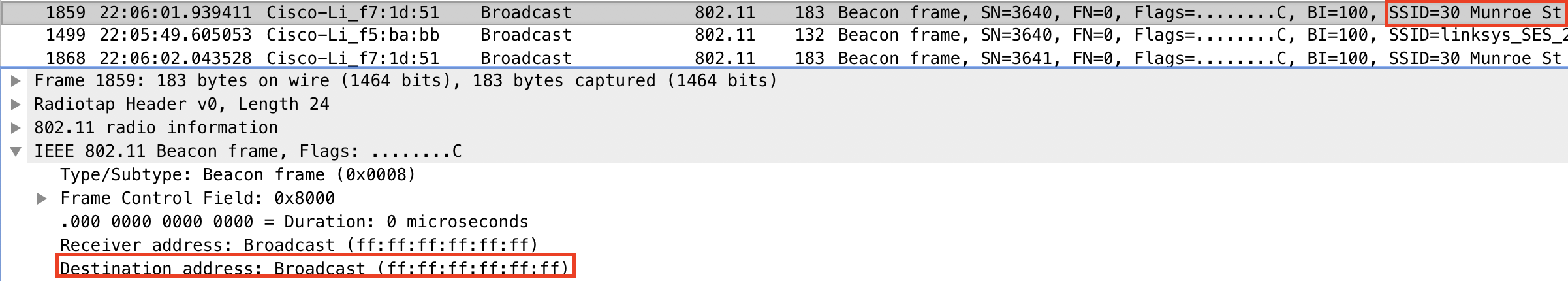
1. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).

The source MAC address is 00:15:b6:f7:1d:51.



1. 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.



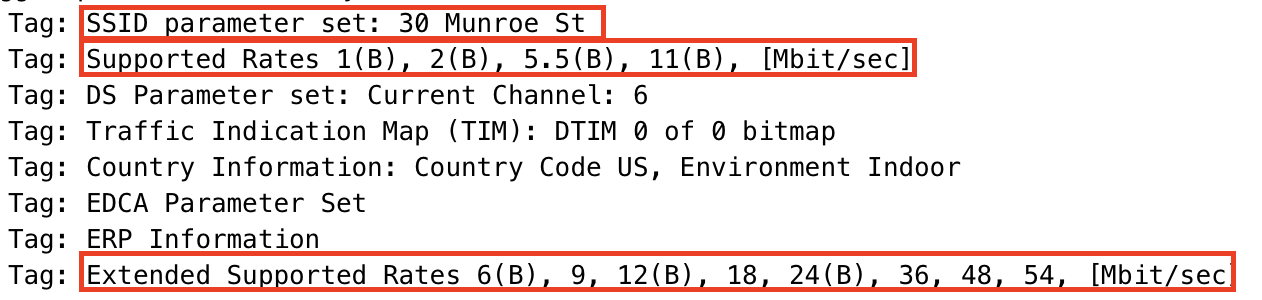
1. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *30 Munroe St*?

The MAC BSS id is 00:16:b6:f7:1d:51.



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?

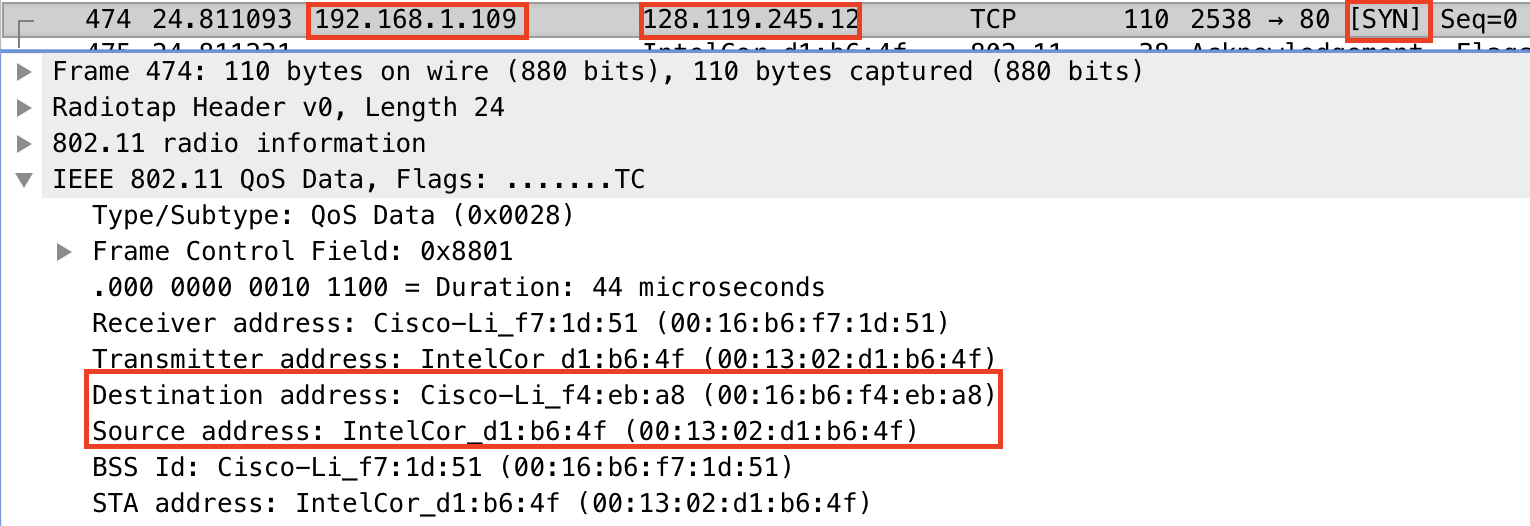
The four supported data rates are 1.0, 2.0, 5.5, and 11.0 Mbps. The eight extended supported rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, and 54.0 Mbps.



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

The frame contains, among others, MAC addresses for the source, the destination, and the receiver. The host’s MAC address is 00:13:02:d1:b6:4f. The access point’s (the destination’s) MAC address is 00:16:b6:f4:eb:e8. The first-hop router is necessarily the access point, so its MAC address is also 00:16:b6:f4:eb:e8.

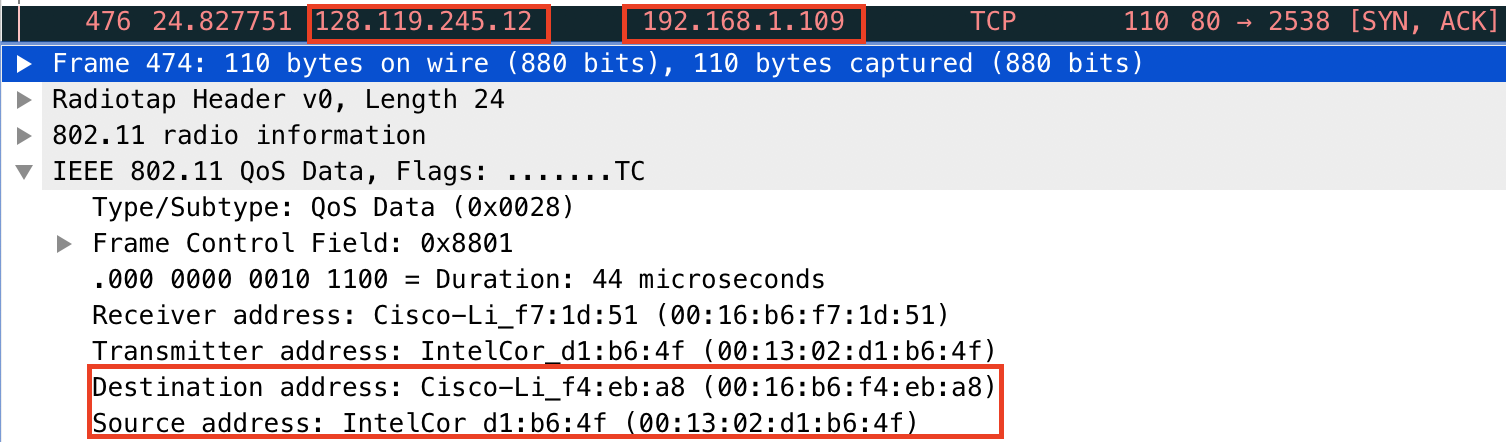
The host’s IP address is 192.168.1.109. The destination’s IP address is 128.119.245.12. This is the IP address for gaia.cs.umass.edu, and it doesn’t correspond to any of the network-attached devices (or the associated MAC addresses) previously defined. This is because MAC addresses are used to route packets to/from immediate adapters, but IP addresses are used to route packets across the network.



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 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).

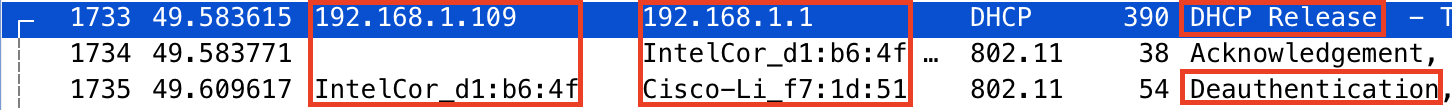
The frame contains, among others, MAC addresses for the source, the destination, and the receiver. The destination MAC address (91:2a:b0:49:b6:4f) corresponds to the host; note that this is the inconsistency mentioned at the bottom of Homework 6. The source MAC address (00:16:b6:f4:eb:a8) corresponds to the first-hop router.

The source MAC address corresponds to the first-hop router; the source IP address (128.119.245.12) corresponds to the gaia.cs.umass.edu. Note that the source MAC address thus does not correspond to the source IP address.



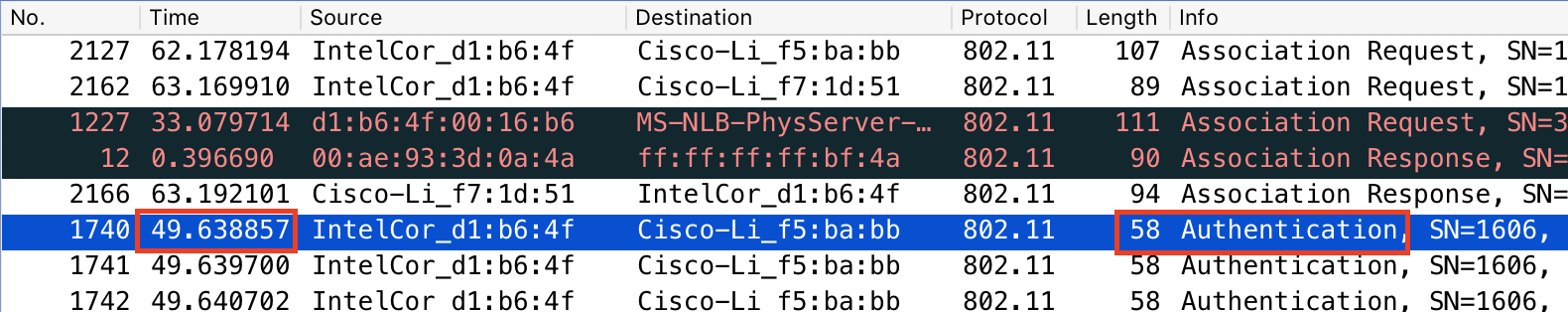
1. What two actions are taken (i.e., frames are sent) by the host in the trace just after *t=49*, to end the association with the *30 Munroe St* AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification,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

At the IP layer, we see that the host sends a DHCP release to the DHCP server. We then see that the host sends a deauthentication frame.



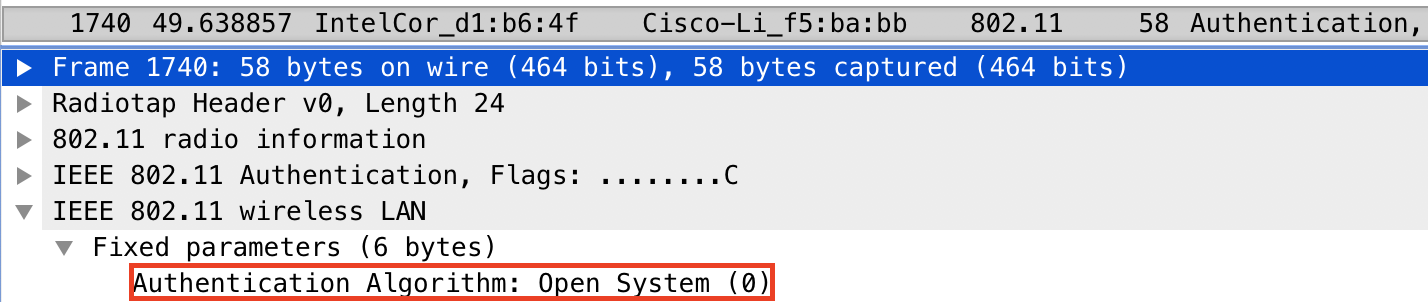
1. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. When is the first AUTHENTICATION message sent from the wireless host to the *linksys\_ses\_24086* AP (which has a MAC address of Cisco\_Li\_f5:ba:bb) starting at around *t=49?*

The first authentication is sent at time seconds.



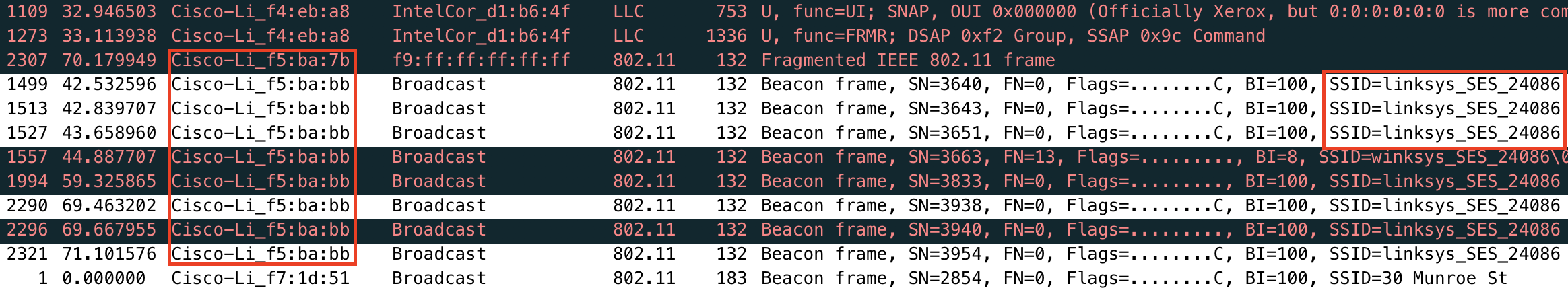
1. Does the host want the authentication from question 10 to require a key or be open?

Because the host specified “Open System” for the Authentication Algorithm, it’s clear that the host wants the authentication to be open.



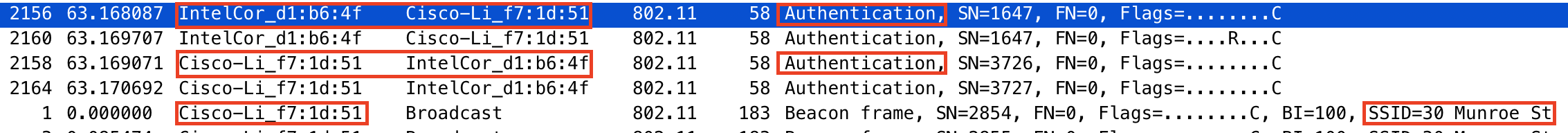
1. Do you see a reply AUTHENTICATION from the *linksys\_ses\_24086* AP in the trace?

In sorting the trace alphabetically by source, we see that Cisco-Li\_f5:ba:bb didn’t send an authentication reply. We also see that Cisco-Li\_f5:ba:bb corresponds to linksys\_SES\_24086. Thus, linksys\_SES\_24086 did not send an authentication reply.



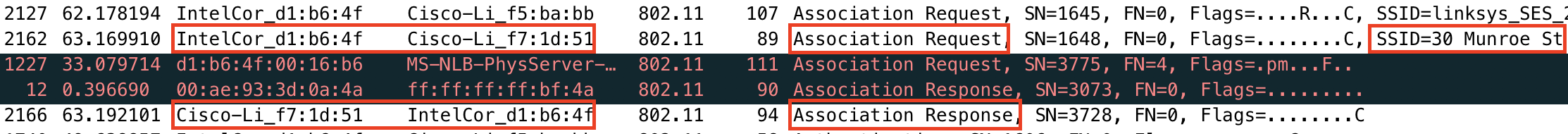
1. Now let’s consider what happens as the host gives up trying to associate with the *linksys\_ses\_24086* AP and now tries to associate with the *30 Munroe St* AP. Look for AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host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

We can see (at the bottom of the below screenshot) that 30 Munroe St corresponds to Cisco-Li\_f7:1d:51. Additionally, we see that the host sent an authentication to Cisco-Li\_f7:1d:51 (and thus to the 30 Munroe St AP) at time seconds. We also see that Cisco-Li\_f7:1d:51 (that is, the 30 Munroe St AP) sends a reply authentication at time seconds.



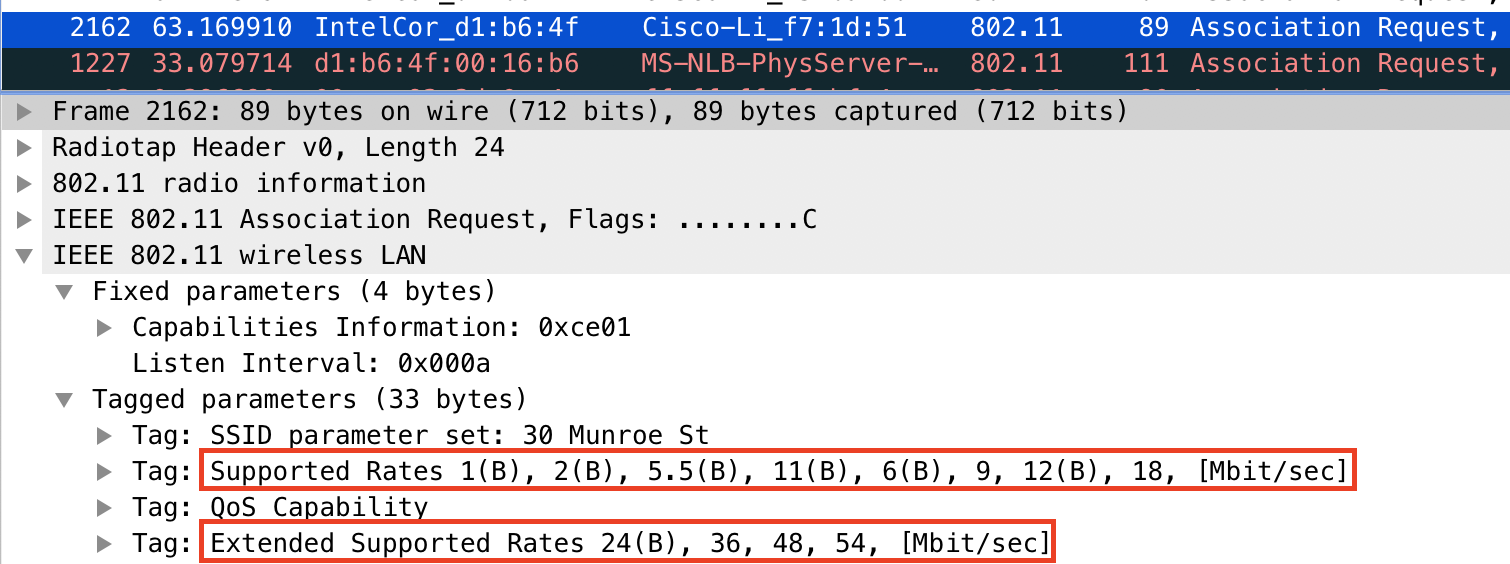
1. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host, are used for the host to associate with an AP. At what time is there an ASSOCIATE REQUEST from host to the *30 Munroe St* AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the 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 host sends an associate request to the 30 Munroe St AP at time seconds. The corresponding associate reply is sent at time seconds.



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.

In the association request, we see that the host supports 1.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, and 54.0 Mbps. In the association response, we see that the AP is willing to support the exact same rates.





1. 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.)

In the probe request, we see MAC addresses of 00:12:f0:1f:57:13, ff:ff:ff:ff:ff:ff, and ff:ff:ff:ff:ff:ff for the sender, receiver, and BSS ID, respectively. In the probe response, we see MAC addresses of 00:16:b6:f7:1d:51, 00:12:f0:1f:57:13, and 00:16:b6:f7:1d:51 for the sender, receiver, and BSS ID, respectively.

A host sends probe requests to scan for an access point. An access point sends probe responses to reply to the host.

