Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

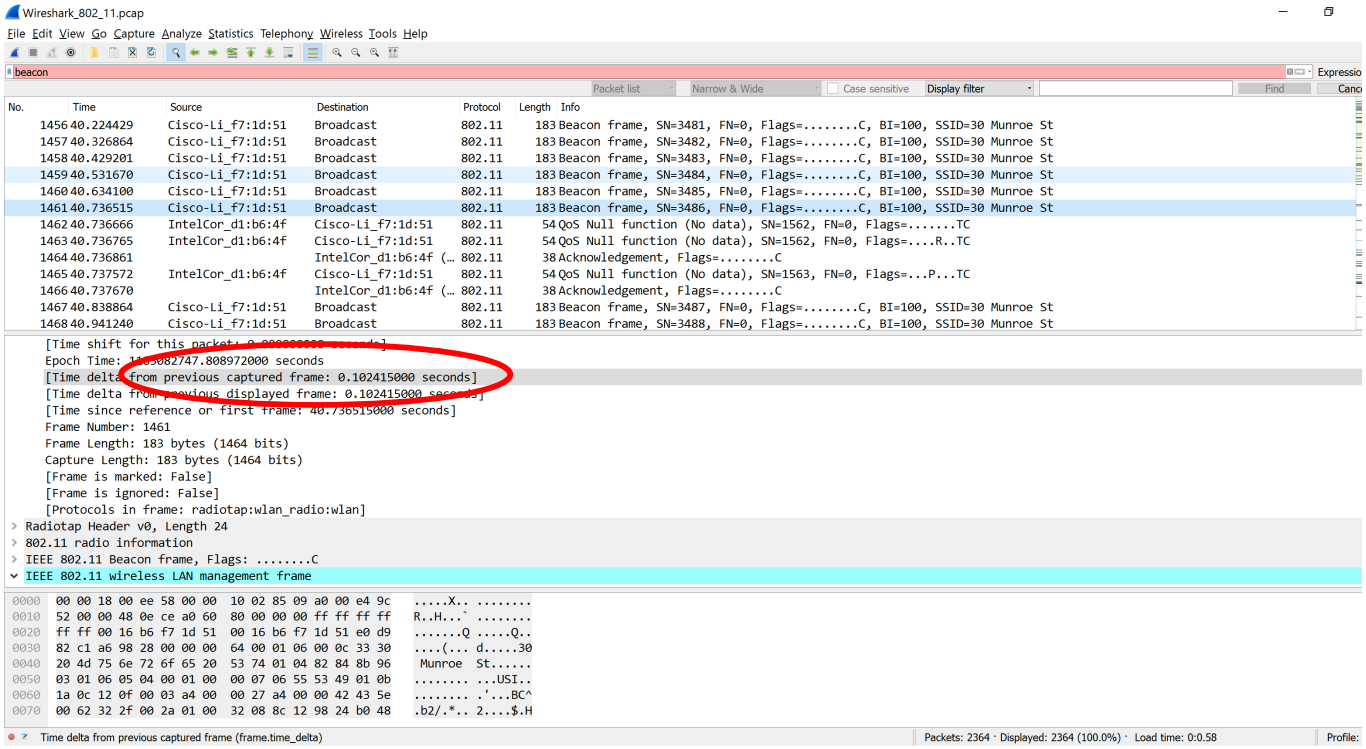
Wireshark 802.11

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

   SSIDs are 30 Munroe St and linsys12

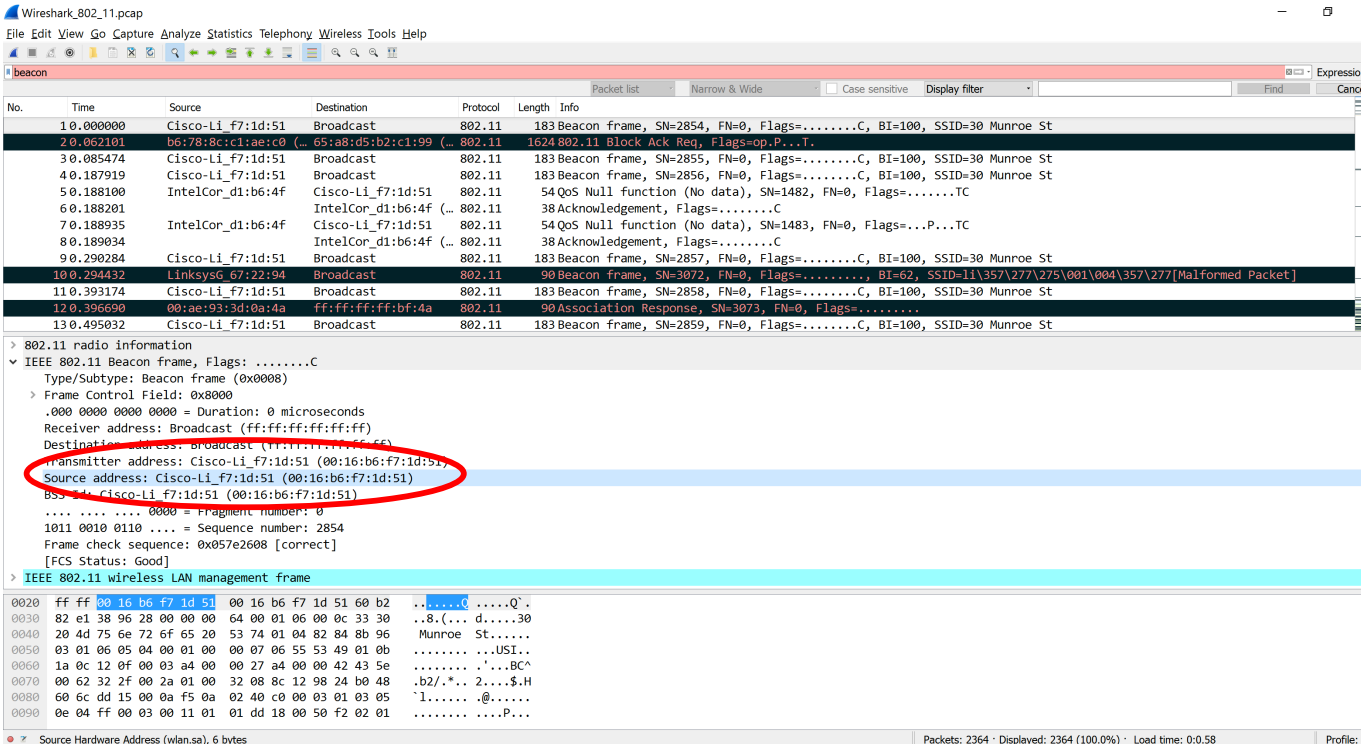
2. **What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).**

   0.1024 seconds



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).**

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060



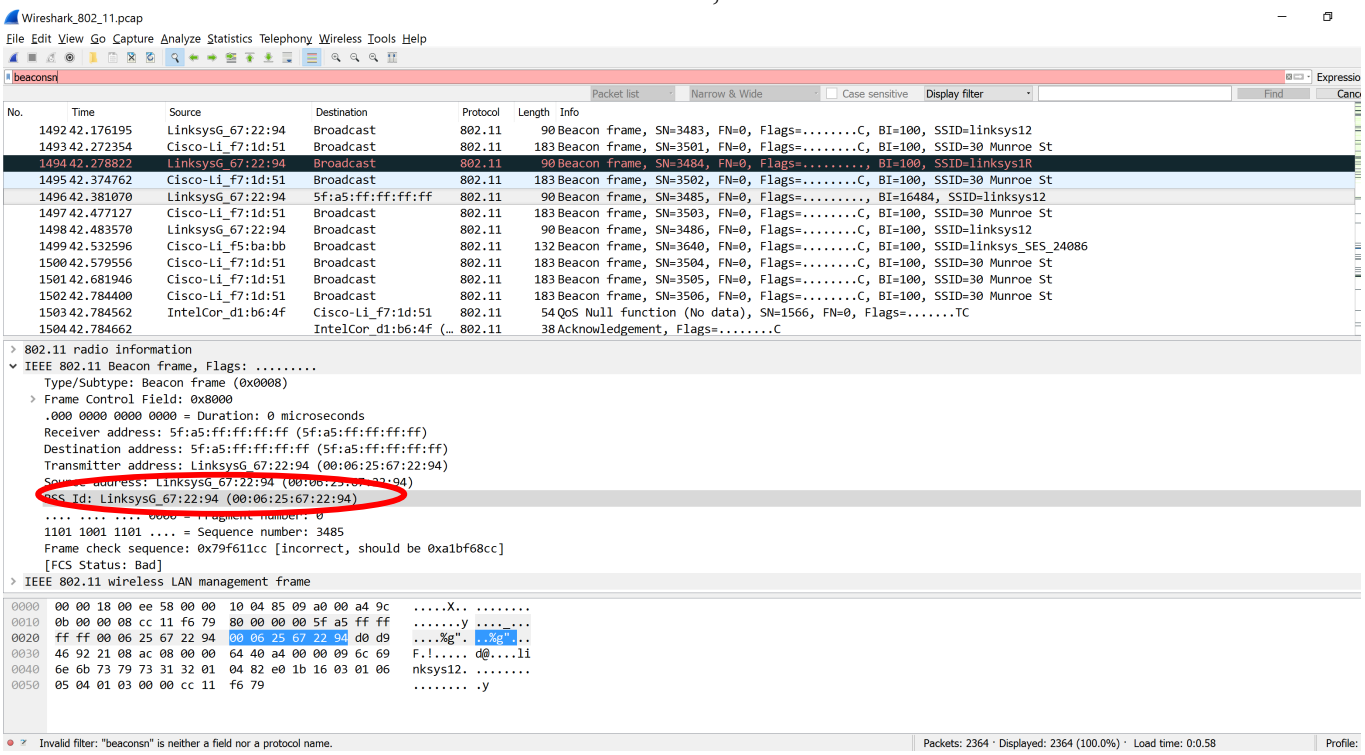
The source MAC address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51

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

The destination MAC address on the 30 Munroe St, beacon frame 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?**

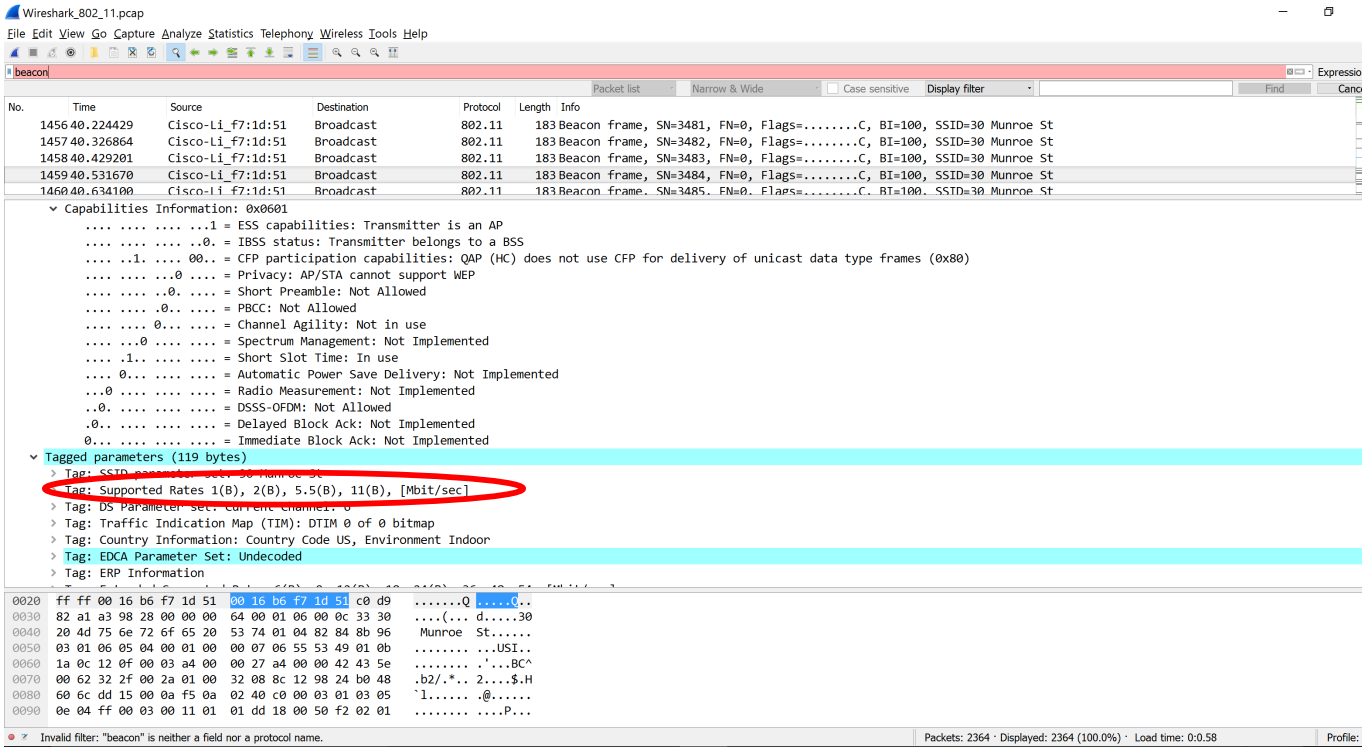
The MAC BSS ID address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51.



Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

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 support rates are 1.0, 2.0, 5.5, 11.0 Mbps. The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 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 frame that contains this is No. 488, at time t = 24.850314. The three MAC addresses are the Destination Address of 00:13:02:d1:b6:4f, as well as the Source Address & BSS Id, both having a value of 00:16:b6:f7:1d:51. The host is 00:13:02:d1:b6:4f. The access point is 00:16:b6:f7:1d:51, which is also the first hop router.

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).**

The TCP SYNACK is received at t = 24.827751 seconds into the trace. The MAC address for the sender of the 802.11 frame containing the TCP SYNACK segment is 00:16:b6:f4:eb:a8, which is the 1st hop router to which the host is attached . The MAC address for the destination, which the host itself, is 91:2a:b0:49:b6:4f.

The MAC address for the BSS is 00:16:b6:f7:1d:51. The IP address of the server sending the TCP SYNACK is 128.199.245.12 (gaia.cs.umass.edu) The destination address is 192.168.1.109 (PC)

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

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?**

   At t = 49.583615 a DHCP release is sent by the host to the DHCP server (whose IP address is 192.168.1.1) in the network that the host is leaving. At t = 49.609617, the host sends a DEAUTHENTICATION frame

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?**

    The first AUTHENTICATION from the host to the AP is at t = 49.638857.

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

    The host is requesting that the association be open

12. **Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?**

    No.

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.)**

    At t = 63.168087 there is a AUTHENTICATION from host to 30 Munroe.
    At t = 63.169071 there is a reply from AP to host.

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.)**

    At t = 63.169910 there is a ASSOCIATE REQUEST.
    At t = 63.192101 there is an ASSOCIATE RESPONSE.

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.**

    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 for AP.

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)**

    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.

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

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 to find an Access Point (see Figure 6.9 on page 531 in the text). A PROBE RESPONSE is sent by the access point to the host sending the request.