WireShark Lab 7

Jennifer Hurst

Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file Wireshark_802_11.pcap. This trace was collected using AirPcap and Wireshark running on a computer in a home network consisting of a Linksys 802.11g combined access point/router, with two wired PCs and one wireless host PC attached to the access point/router. In this trace file, we'll see frames captured on channel 6. Since the host and AP that we are interested in are not the only devices using channel 6, we'll see a lot of frames that we're not interested in for this lab, such as beacon frames advertised by a neighbor's AP also operating on channel 6. The wireless host activities taken in the trace file are:

- • The host is already associated with the *30 Munroe St* AP when the trace begins.
- • At *t = 24.82*, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12.
- • At *t=32.82, t*he host makes an HTTP request to http://www.cs.umass.edu, whose IP address is 128.119.240.19.
- • At *t = 49.58,* the host disconnects from the *30 Munroe St* AP and attempts to connect to the *linksys_ses_24086*. This is not an open access point, and so the host is eventually unable to connect to this AP.
- • At *t=63.0* the host gives up trying to associate with the *linksys_ses_24086 AP,* and associates again with the *30 Munroe St* access point.

Once you have downloaded the trace, and unzip it, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the Wireshark_802_11.pcap trace file. The resulting display should look just like Figure 1.

Figure 1: Wireshark window, after opening the Wireshark_802_11.pcap file

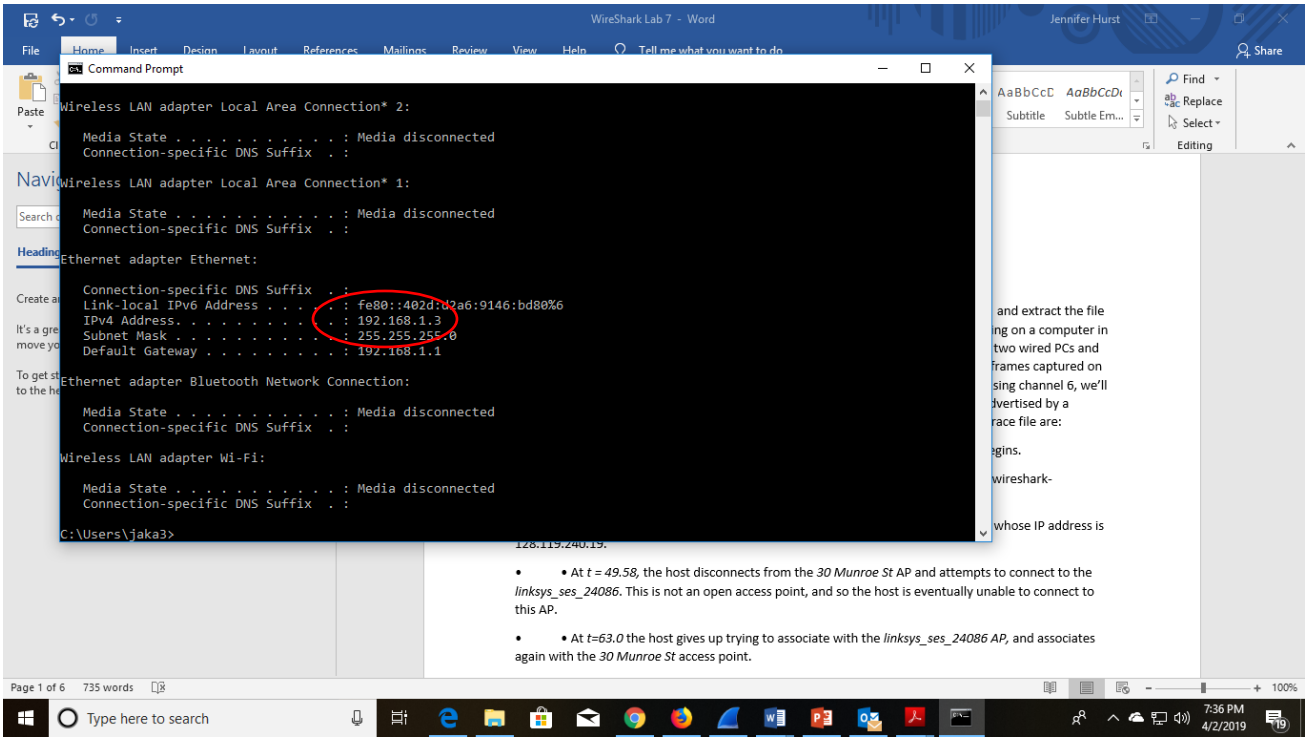
Recall that beacon frames are used by an 802.11 AP to advertise its existence. To answer some of the questions below, you'll want to look at the details of the "IEEE 802.11" frame and subfields in the middle Wireshark window.

- • (*For each of these questions, take a screenshot of Wireshark, and attach it to your answer*) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.

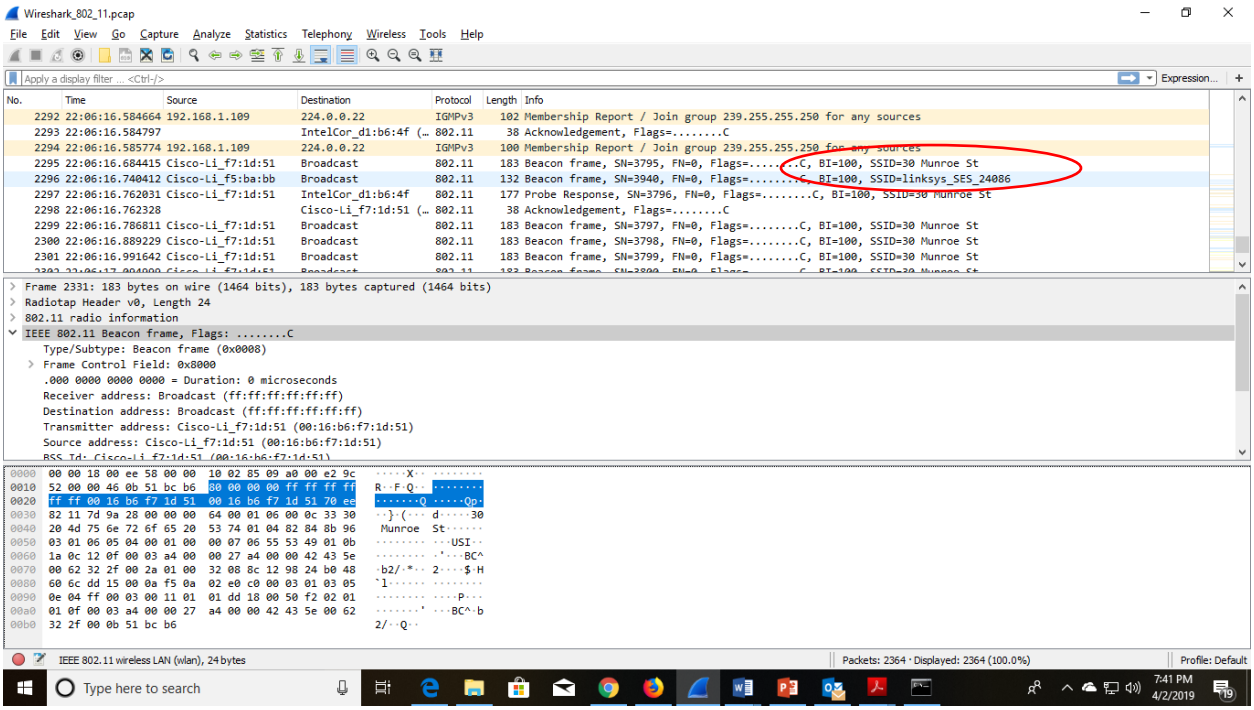
Questions:

What is the IP address of your computer? – **Wireshark screenshot not, Terminal**

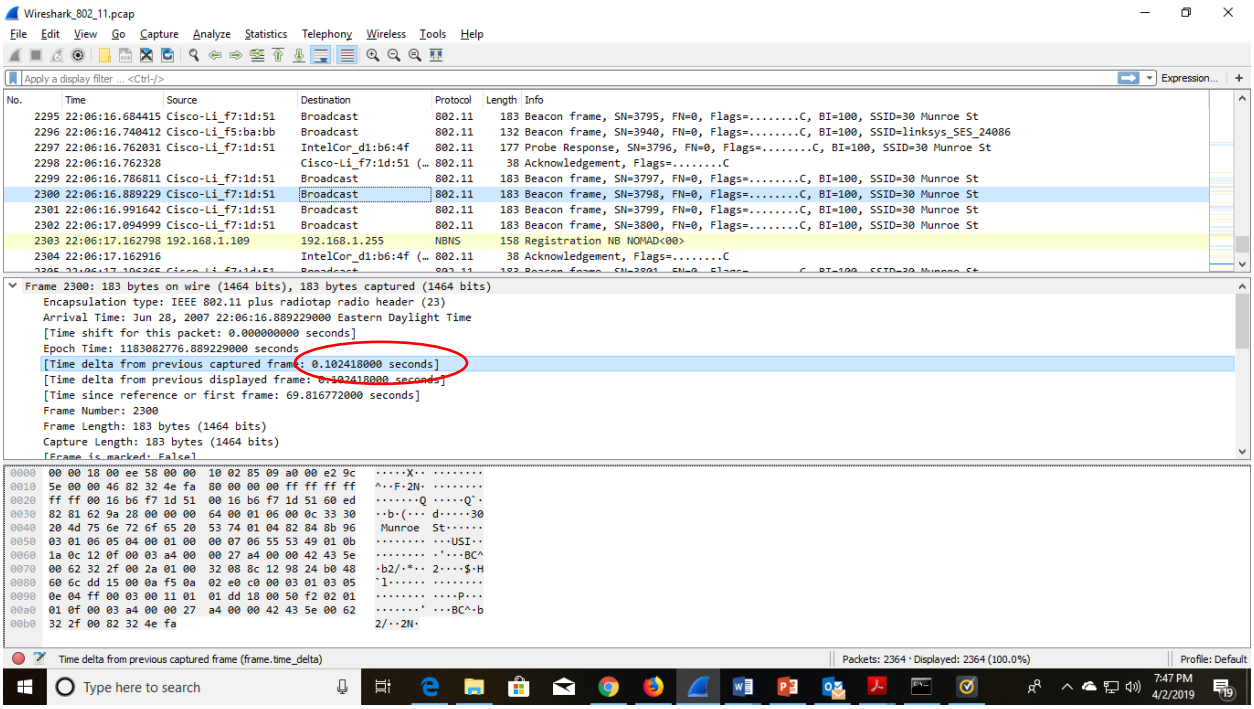
My IP address is 192.168.1.3



1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?
   The most beacon frames are from SSID of 30 Munroe St and linsys_SES_24086

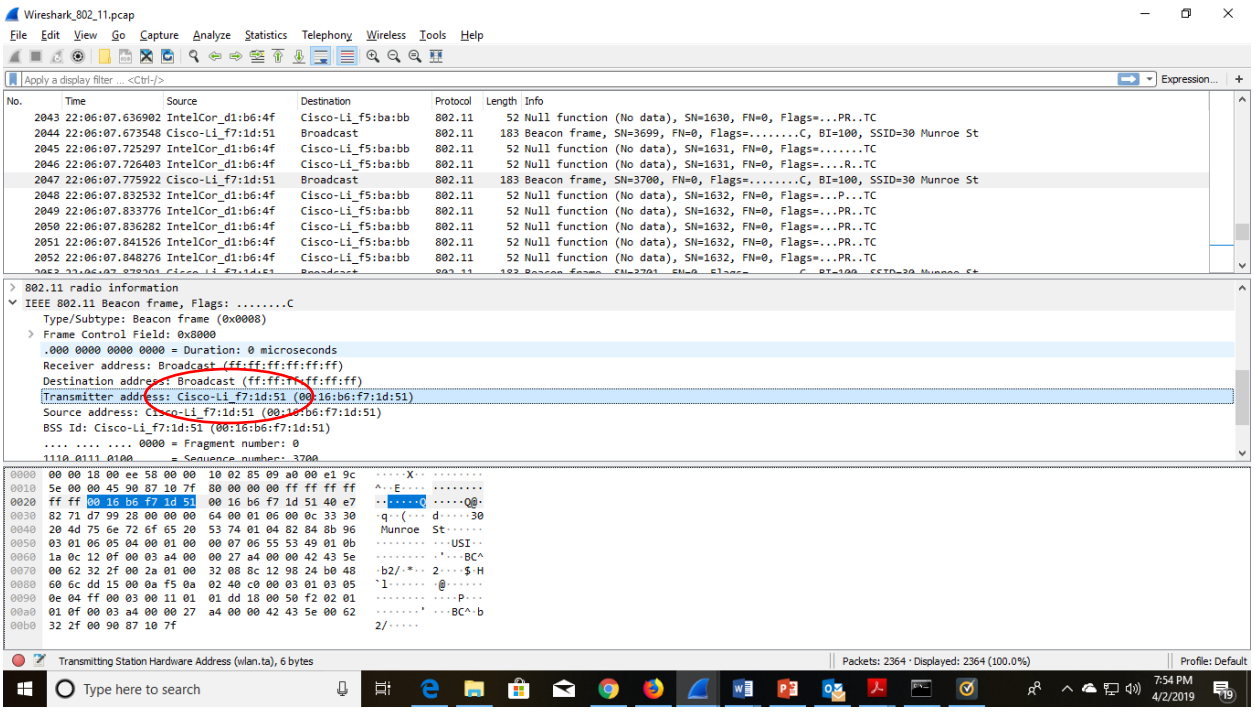


2. What are the intervals of time between the transmissions of the beacon frames the *linksys_ses_24086* access point? From the *30 Munroe St*. access point? (Hint: this interval of time is contained in the beacon frame itself).
   The beacon interval for both access points is .1024 seconds.



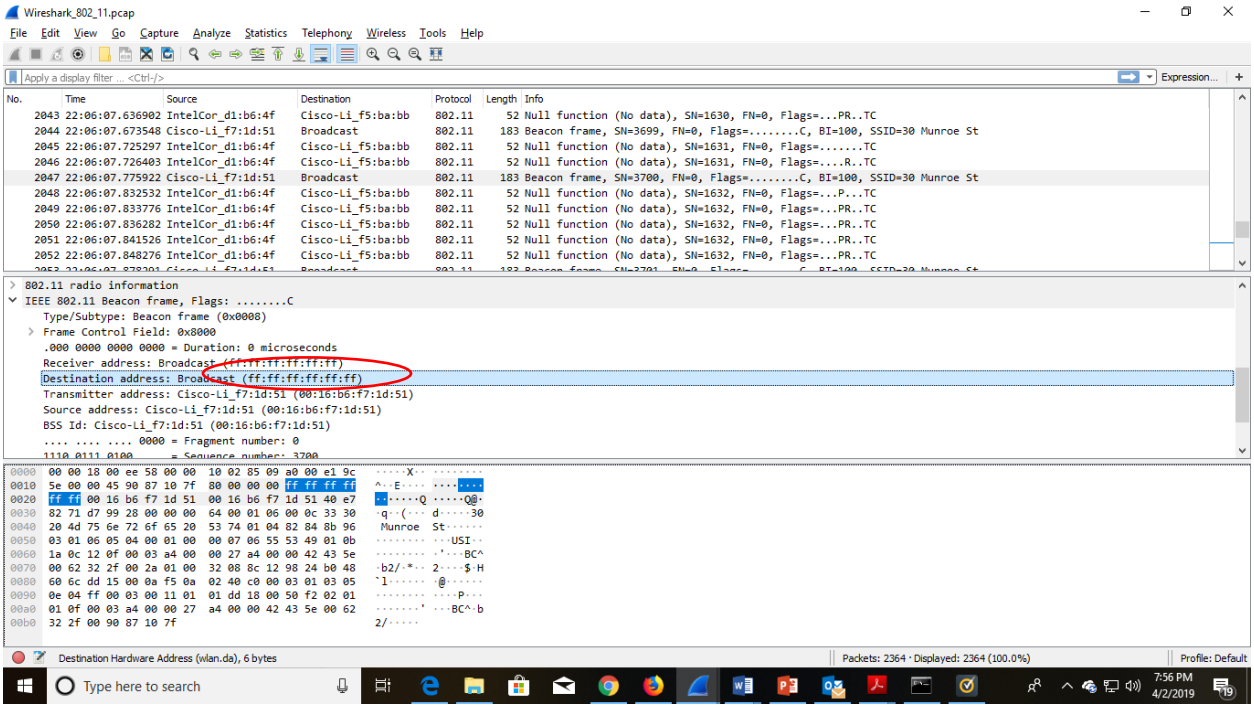
3. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE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

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



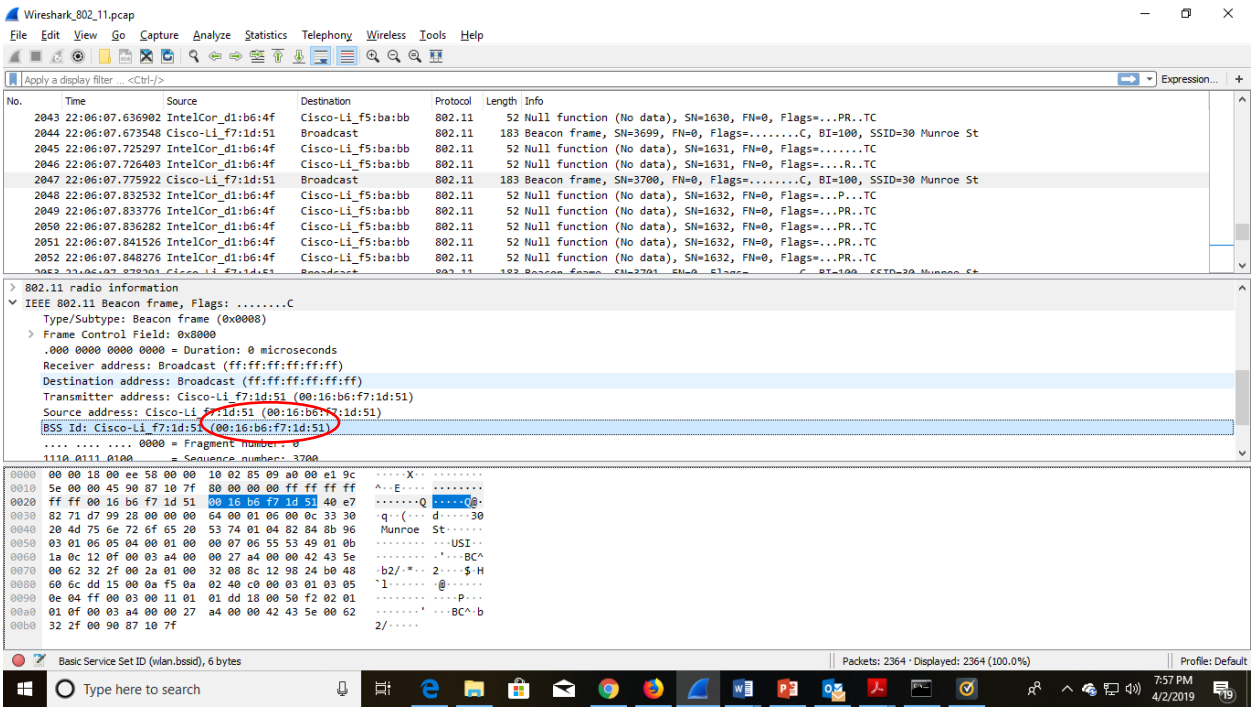
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*??

   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.



Screen print, final page