

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 $t=32.82$, the 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

The screenshot shows a Windows desktop with a Command Prompt window open, displaying network configuration details for various adapters. The Ethernet adapter Ethernet0 is highlighted, showing its IP address as 192.168.1.3. A Word document titled 'WireShark Lab 7 - Word' is also visible, containing text about extracting files from a capture.

```
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet0:
Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::402d:d2a6:9146:bd80%6
IPv4 Address. . . . . : 192.168.1.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

C:\Users\jaka>
```

and extract the file
ing on a computer in
two wired PCs and
frames captured on
sing channel 6, we'll
diverted by a
race file are:
egins.
wireshark-
whose IP address is

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

The screenshot shows the Wireshark network traffic analysis tool. The packet list pane displays a list of captured packets, including several beacon frames from 30 Munroe St and linsys_SES_24086. The packet details pane shows the structure of a selected beacon frame, including the IEEE 802.11 header and the frame control field.

No.	Time	Source	Destination	Protocol	Length	Info
2292	22:06:16.584664	192.168.1.109	224.0.0.22	IGMPv3	102	Membership Report / Join group 239.255.255.250 for any sources
2293	22:06:16.584797	IntelCor_d1:b6:4f	224.0.0.22	IGMPv3	38	Acknowledgement, Flags=.....C
2294	22:06:16.585774	192.168.1.109	224.0.0.22	IGMPv3	100	Membership Report / Join group 239.255.255.250 for any sources
2295	22:06:16.684415	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3795, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2296	22:06:16.740412	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3940, FN=0, Flags=.....C, BI=100, SSID=linsys_SES_24086
2297	22:06:16.762031	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3796, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2298	22:06:16.762328	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
2299	22:06:16.766811	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3797, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2300	22:06:16.889229	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3798, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2301	22:06:16.991642	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3799, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Frame 2331: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags:C
Type/Subtype: Beacon frame (8x0008)
Frame Control Field: 0x0000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
RSSI: 100 (00:16:b6:f7:1d:51)

- 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.

The image shows a Wireshark packet capture of an 802.11 network. The packet list on the left shows several beacon frames from source 00:16:b6:f7:1d:51 (30 Munroe St). The details pane for packet 2300 is expanded, showing the 'Time delta from previous captured frame: 0.102418000 seconds' circled in red. The hex dump at the bottom shows the raw data of the beacon frame.

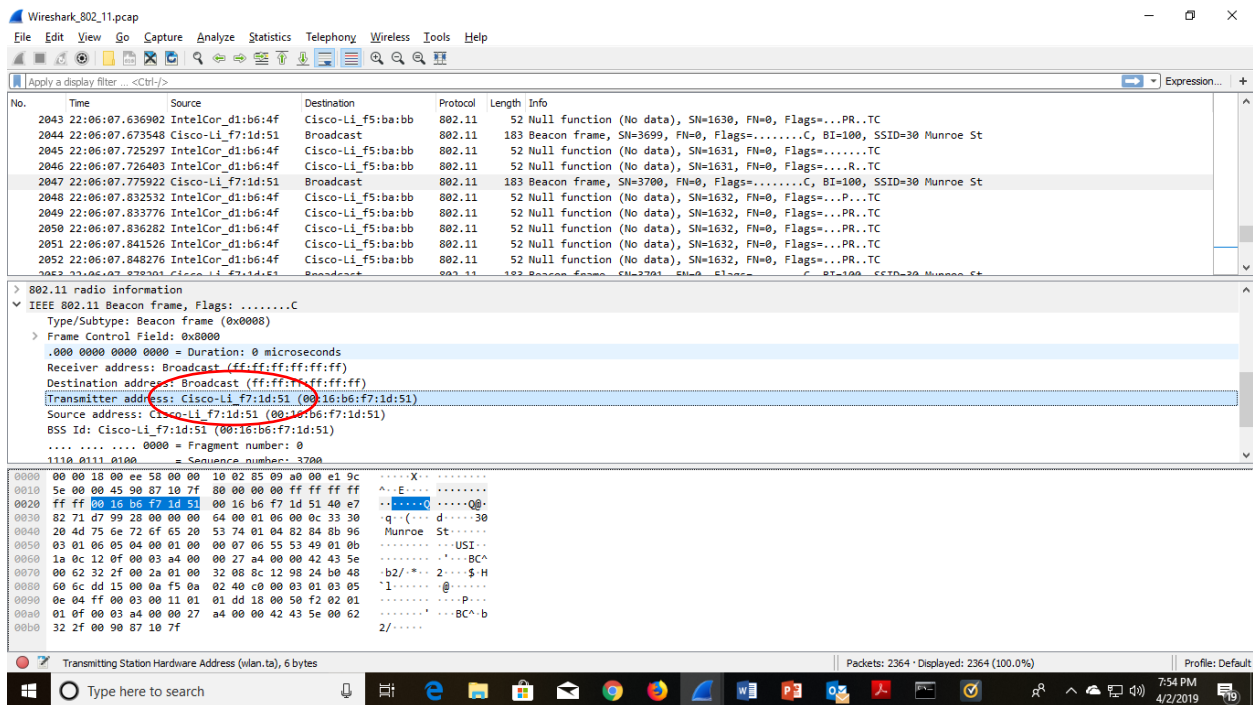
No.	Time	Source	Destination	Protocol	Length	Info
2295	22:06:16.684415	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3795, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2296	22:06:16.740412	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3948, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
2297	22:06:16.762831	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3796, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2298	22:06:16.762828	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
2299	22:06:16.786811	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3797, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2300	22:06:16.889229	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3798, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2301	22:06:16.991642	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3799, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2302	22:06:17.094999	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3800, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2303	22:06:17.162798	192.168.1.109	192.168.1.255	NBNS	158	Registration NB NOWAD<00>
2304	22:06:17.162916	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C

Frame 2300: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface 0
 Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
 Arrival Time: Jun 28, 2007 22:06:16.889229000 Eastern Daylight Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1183082776.889229000 seconds
 [Time delta from previous captured frame: 0.102418000 seconds]
 [Time delta from previous displayed frame: 0.102418000 seconds]
 [Time since reference or first frame: 69.816772000 seconds]
 Frame Number: 2300
 Frame Length: 183 bytes (1464 bits)
 Capture Length: 183 bytes (1464 bits)
 [Frame is marked: False]

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e2 9cX.....
 0010 5e 00 00 46 82 32 4e fa 00 00 00 ff ff ff ffF.2N.....
 0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 00 edQ.....
 0030 82 81 62 9a 28 00 00 00 64 00 01 06 00 0c 33 30 ..b(....d....30
 0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St.....
 0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0bUSI.....
 0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5eBCA.....
 0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48 ..b2/*...2....\$-H
 0080 60 6c dd 15 00 0a f5 0a 02 e0 c0 00 03 01 03 05 ..l.....
 0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01P.....
 00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62BC^b
 00b0 32 2f 00 82 32 4e fa 2/..2N..

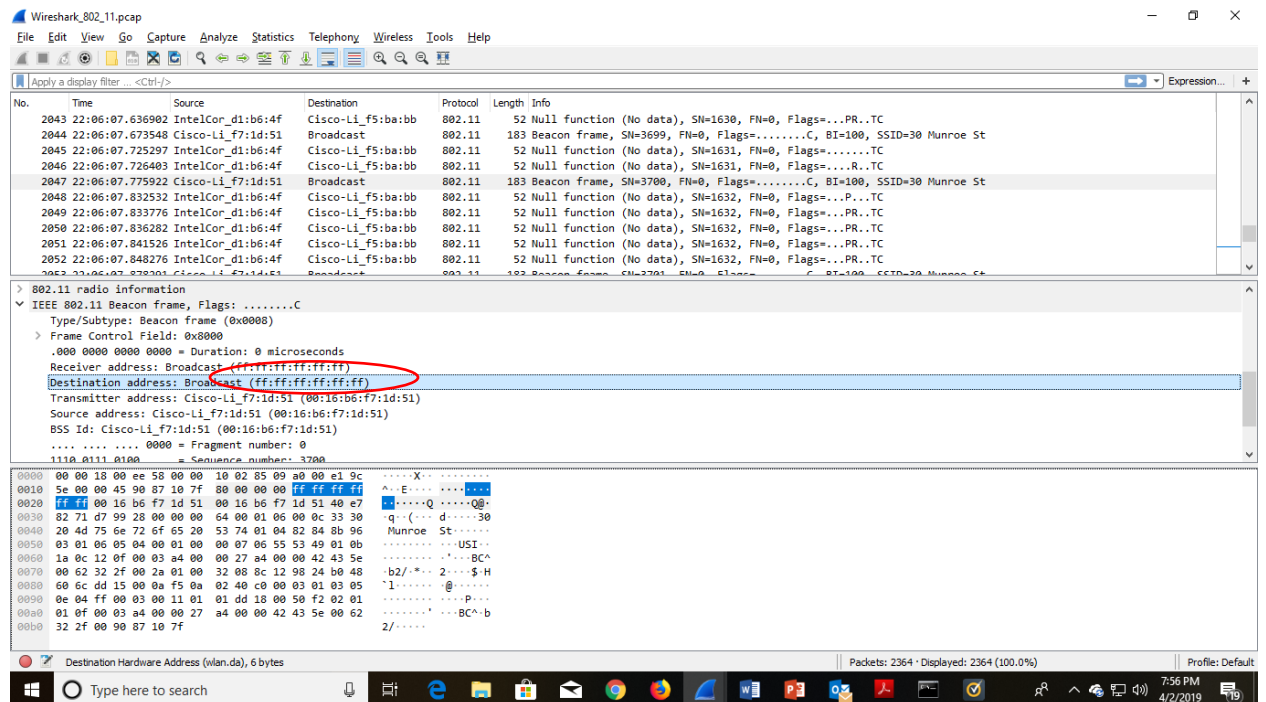
- What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE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



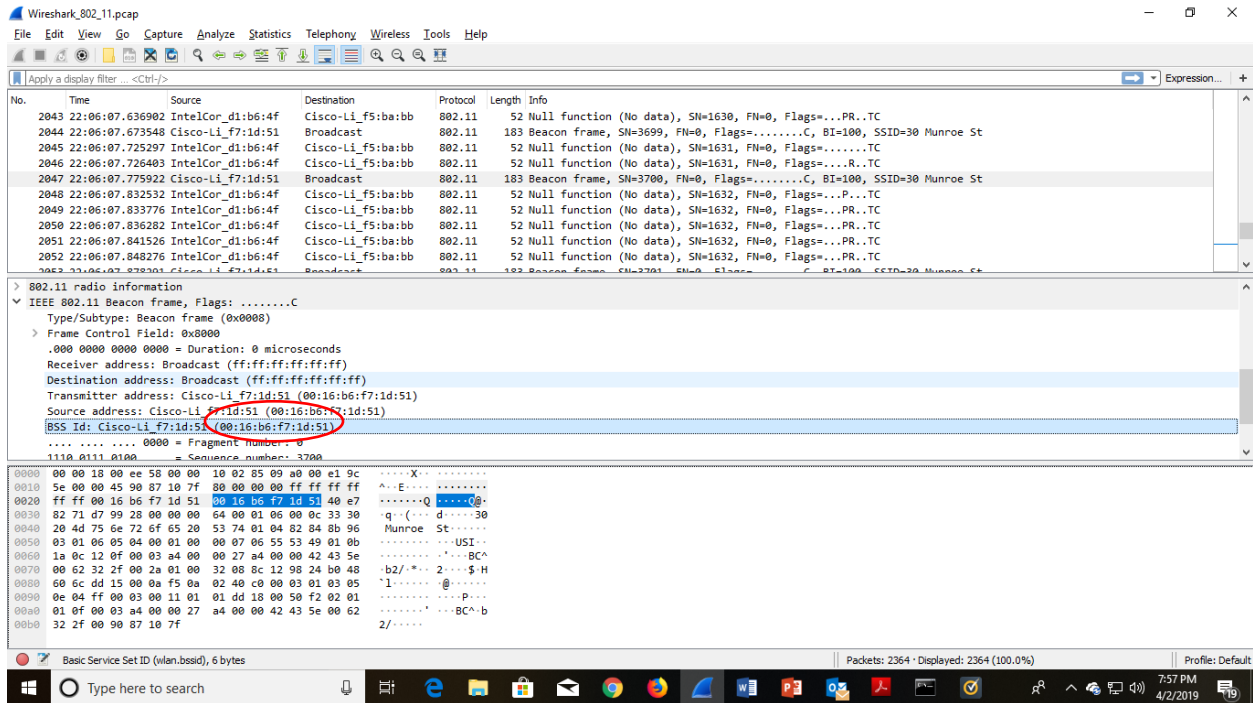
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??

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

