

**Instructions:**

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/wiresharklabs/alice.txt>. The IP address of [gaia.cs.umass.edu](http://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.

No.	Time	Source	Destination	Protocol	Lenet Info
1	0.000000	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2854, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
2	0.000013	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2854, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
3	0.001474	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2855, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
4	0.187919	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2856, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
5	0.188100	IntelCor_d1:b6:4	Cisco-L1-F7:1d:51	802.11	54 QoS Null Function (No data), Sh=1402, Pw=0, Flags=.....TC
6	0.188201	IntelCor_d1:b6:4	Cisco-L1-F7:1d:51	802.11	38 Acknowledgement, Flags=.....C
7	0.188935	IntelCor_d1:b6:4	Cisco-L1-F7:1d:51	802.11	54 QoS Null Function (No data), Sh=1403, Pw=0, Flags=.....P...TC
8	0.189034	IntelCor_d1:b6:4	Cisco-L1-F7:1d:51	802.11	38 Acknowledgement, Flags=.....C
9	0.200204	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2857, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
10	0.204433	Linksys_67:12:94	Broadcast	802.11	90 Beacon frame, Sh=3072, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
11	0.393174	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2858, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
12	0.400000	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2859, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
13	0.409932	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2859, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
14	0.409932	Linksys_67:12:94	Broadcast	802.11	90 Beacon frame, Sh=3071, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
15	0.597382	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2860, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
16	0.601687	Linksys_67:12:94	Broadcast	802.11	90 Beacon frame, Sh=3075, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
17	0.699047	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2861, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
18	0.802226	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2862, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
19	0.904619	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2863, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
20	1.007915	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2864, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
21	1.007915	Linksys_67:12:94	Broadcast	802.11	90 Beacon frame, Sh=3076, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
22	1.109406	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2865, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
23	1.113093	Linksys_67:12:94	Broadcast	802.11	90 Beacon frame, Sh=3080, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
24	1.211043	Cisco-L1-F7:1d:51	Broadcast	802.11	183 Beacon frame, Sh=2866, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
25	1.211392	IntelCor_d1:b6:4	Cisco-L1-F7:1d:51	802.11	54 QoS Null Function (No data), Sh=1404, Pw=0, Flags=.....TC
26	1.212089	IntelCor_d1:b6:4	Cisco-L1-F7:1d:51	802.11	38 Acknowledgement, Flags=.....C
27	1.212185	Cisco-L1-F7:1d:51	IntelCor_d1:b6:4	802.11	177 Probe Response, Sh=2867, Pw=0, Flags=.....C, B1=100, S1D=30 Munroe St
28	1.212202	Cisco-L1-F7:1d:51	Cisco-L1-F7:1d:51	802.11	38 Acknowledgement, Flags=.....C

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.
- Include a terminal screenshot showing your computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

Lab will NOT be graded if either of these two is missing.

Questions:

IP of my terminal: 10.0.0.2

```

Command Prompt

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : hsd1.va.comcast.net
    IPv6 Address. . . . . : 2601:140:8100:88fe:9a86
    IPv6 Address. . . . . : 2601:140:8100:88fe:b4c9:bdea:e111:c8c6
    Temporary IPv6 Address. . . . . : 2601:140:8100:88fe:cd9d:81b7:f3eb:c444
    Link-local IPv6 Address . . . . . : fe80::b4c9:bdea:e111:c8c6%17
    IPv4 Address. . . . . : 10.0.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::f60e:83ff:fed5:1245%17
                             10.0.0.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\ariel>

```

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

<i>Access Point</i>	<i>SSID</i>
Cisco-Li_f7:1d:51	30 Munroe St
LinksysG_67:22:94	linksys12

```

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

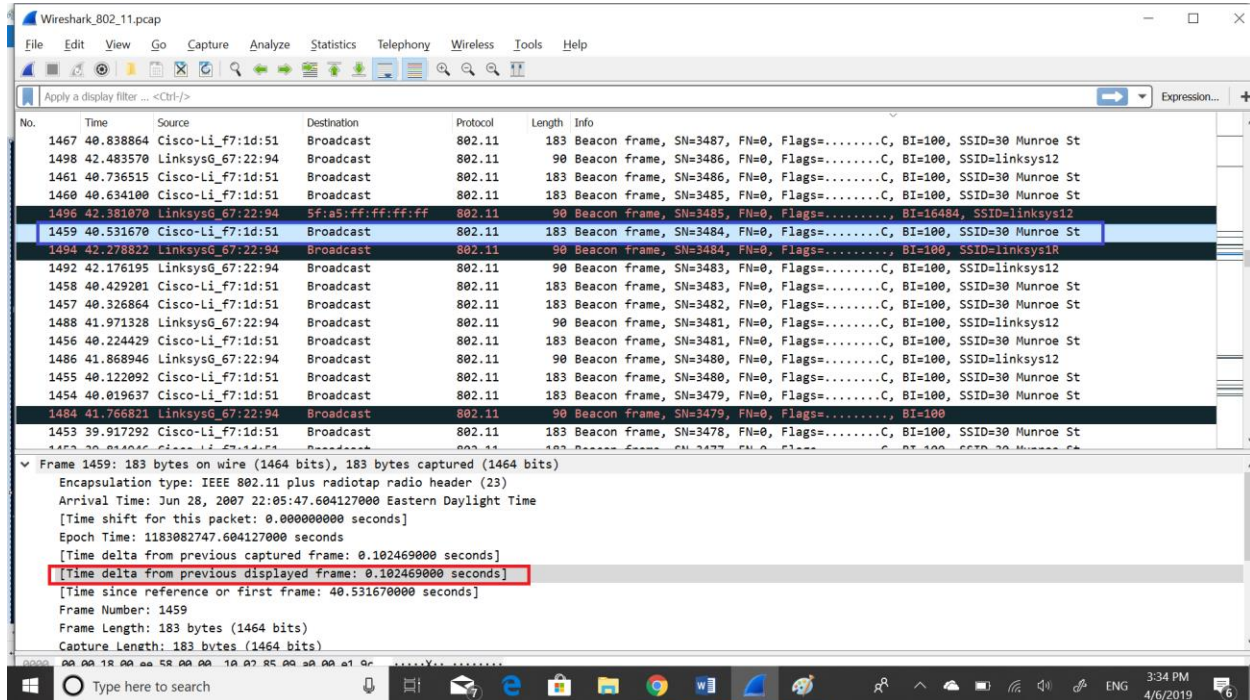
No. Time Source Destination Protocol Length Info
1519 43.097945 LinksysG_67:22:94 Broadcast 802.11 90 Beacon frame, SN=3492, FN=0, Flags=pm..M...
1472 41.350876 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3492, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1517 42.995445 LinksysG_67:22:94 Broadcast 802.11 90 Beacon frame, SN=3491, FN=0, Flags=.....C, BI=100, SSID=linksys12
1471 41.248450 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3491, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1470 41.146040 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3490, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1515 42.892973 LinksysG_67:22:94 ff:ff:ff:ff:5f:a5 802.11 90 Beacon frame, SN=3490, FN=0, Flags=.....C, BI=100, SSID=linksys12
1469 41.045174 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3489, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1468 40.941240 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3488, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1467 40.838864 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3487, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1498 42.483570 LinksysG_67:22:94 Broadcast 802.11 90 Beacon frame, SN=3486, FN=0, Flags=.....C, BI=100, SSID=linksys12
1461 40.736515 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3486, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1460 40.634100 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3485, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1496 42.381070 LinksysG_67:22:94 5f:a5:ff:ff:ff:ff 802.11 90 Beacon frame, SN=3485, FN=0, Flags=.....C, BI=16404, SSID=linksys12
1459 40.531670 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3484, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1494 42.278822 LinksysG_67:22:94 Broadcast 802.11 90 Beacon frame, SN=3484, FN=0, Flags=.....C, BI=100, SSID=linksys1R
1492 42.176195 LinksysG_67:22:94 Broadcast 802.11 90 Beacon frame, SN=3483, FN=0, Flags=.....C, BI=100, SSID=linksys12
1458 40.429201 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3483, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1457 40.320264 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=3483, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> Frame 480: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....TC
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 1, Ack: 1, Len: 435
> Hypertext Transfer Protocol

```

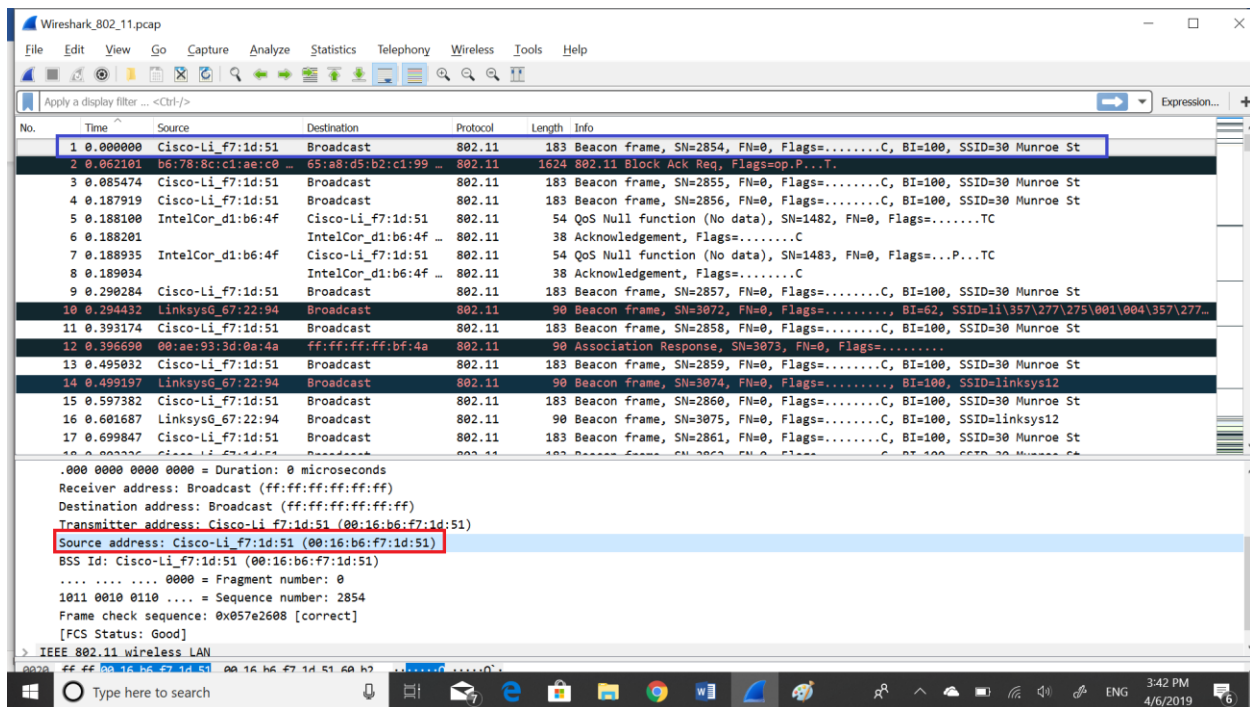
2. What are the intervals of time between the transmissions of the beacon frames the linksys\_ses\_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).

The intervals of time is approximately 0.102469 seconds



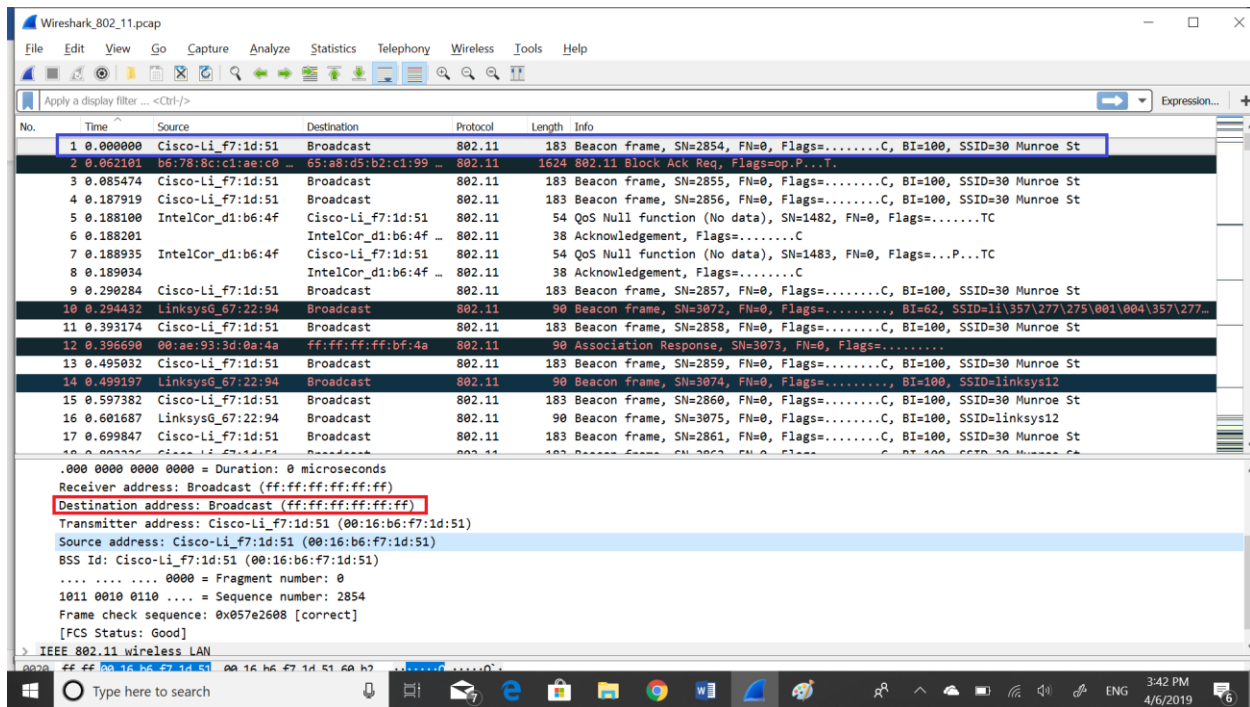
3. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE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

The source MAC 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 BBS id on the beacon frame from 30 Munroe St is Cisco-Li\_f7:1d (00:16:b6:f7:1d:51)

