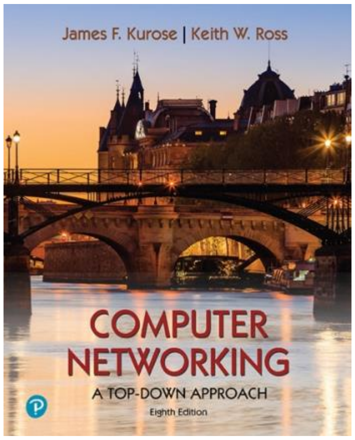
Faris Soepangat
1001374988
CSE 4344
Due April 29, 2024

Wireshark Lab: 802.11 WiFi v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.,* J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



In this lab, we'll investigate the 802.11 wireless network protocol. Before beginning this lab, you might want to re-read Section 7.3 in the text[1]. Since we'll be delving a bit deeper into 802.11 than is covered in the text, you might want to check out "A Technical Tutorial on the 802.11Protocol," by Pablo Brenner (Breezecom Communications), http://www.sss-mag.com/pdf/802_11tut.pdf And, of course, there is the "bible" of 802.11 - the 4,379-page standard itself, "ANSI/IEEE Std 802.11-2020," available here. But we've extracted out section 9.2.4.1 from the specification, and added in a handy cheat-sheet for 802.11 Wireshark display filters, here, both of which will be *very* useful for this lab.

In this lab, we'll capture a trace from a wireless 802.11 WiFi interface on our computer/laptop. Here are the actions taken, assuming you're already connected to a WiFi network (which we'll refer to as your *home* network), when trace collection starts:

1. Make an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt
2. Make a request to http://www.cs.umass.edu
3. Disconnect from your home network
4. (optional step) Try to connect to another 802.11 wireless network whose beacon advertisements are being received, and for which you do *not* have access, and therefore your connection attempt will fail.
5. Connect again (successfully) to you home network.

Figure 1 shows the general setup for this 802.11 Wireshark lab.

[1] References to figures and sections are for the 8th edition of our text, *Computer Networks, A Top-down Approach, 8h ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.* Our authors' website for this book is http://gaia.cs.umass.edu/kurose_ross You'll find lots of interesting open material there..

Faris Soepangat
1001374988
CSE 4344
Due April 29, 2024

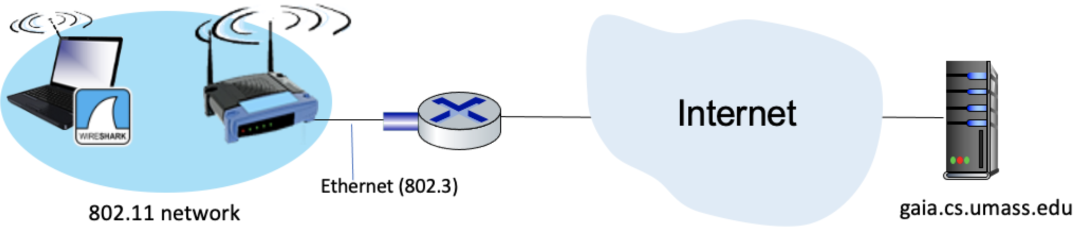


Figure 1: An 802.11 network, connected to a router, connected to the Internet

As usual, we've provided a trace file[2] of captured 802.11 frames for you to analyze in case you are not able to take the actions above. If you're doing this lab as part of a class, your teacher will provide details about how to hand in assignments, whether written or in an LMS.[3] The questions below assume you are analyzing this provided trace (in particular, with respect to access point (AP) names, and timings in the trace). Of course, you're encouraged to gather your own trace, taking the five actions above, and answering the questions below from your own trace.

1. Getting Started

Let's take a look at our trace file. This trace was collected using on a computer in the home network of one of the authors, 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. The author is fortunate to have other access points (APs) in neighboring houses available as well, so 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. You'll find the following wireless host activities in the trace file:

- The host is already associated with the *30 Munroe St* AP when the trace begins.
- At *t = 24.8282*, 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=32.8259, t*he host makes an HTTP request to http://www.cs.umass.edu, whose IP address is 128.119.240.19.

[2] If you're unable to run Wireshark on a live network connection, you can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip and extract the trace file Wireshark_801_11.pcapng.

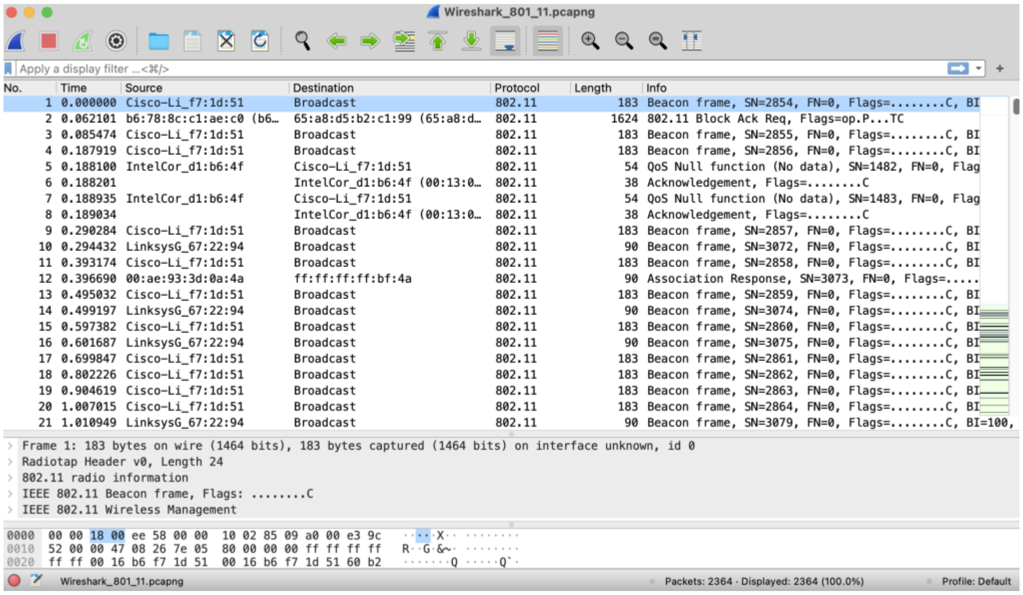
[3] For the author's class, when answering the following questions with hand-in assignments, students print out the GET and response messages (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the message they've found the information that answers a question. They do this by marking paper copies with a pen or annotating electronic copies with text in a colored font. There are LMS modules for teachers that allow students to answer these questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm

Faris Soepangat
1001374988
CSE 4344
Due April 29, 2024

- At *t = 49.5836*, the host disconnects from the *30 Munroe St* AP by issuing a DHCP Release message.
- At *t=63.0592* the host associates again with the *30 Munroe St* AP.

Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the Wireshark_801_11.pcapng trace file. The resulting display should look like Figure 2.

There are lots of captured frames in this trace, so we'll use display filters to display just selected types of frames as we analyze this trace. A handy reference for Wireshark Display filters for 802.11 frames is at http://gaia.cs.umass.edu/wireshark-labs/wireshark_802.11_filters_-_reference_sheet.pdf.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=........C, BI
2	0.062101	b6:78:8c:c1:ae:c0 (b6…	65:a8:d5:b2:c1:99 (65:a8:d…	802.11	1624	802.11 Block Ack Req, Flags=op.P...TC
3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=........C, BI
4	0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=........C, BI
5	0.188100	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flag
6	0.188201		IntelCor_d1:b6:4f (00:13:0…	802.11	38	Acknowledgement, Flags=........C
7	0.188935	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1483, FN=0, Flag
8	0.189034		IntelCor_d1:b6:4f (00:13:0…	802.11	38	Acknowledgement, Flags=........C
9	0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=........C, BI
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=........C, BI
11	0.393174	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=........C, BI
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....
13	0.495032	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=........C, BI
14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=........C, BI
15	0.597382	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2860, FN=0, Flags=........C, BI
16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=........C, BI
17	0.699847	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=........C, BI
18	0.802226	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2862, FN=0, Flags=........C, BI
19	0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=........C, BI
20	1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, FN=0, Flags=........C, BI
21	1.010949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=........C, BI=100,

```
> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
> IEEE 802.11 Wireless Management
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e3 9c   ·····X·· ········
0010  52 00 00 47 08 26 7e 05  80 00 00 00 ff ff ff ff   R··G·&~· ········
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 60 b2   ·······Q ·····Q`·
```

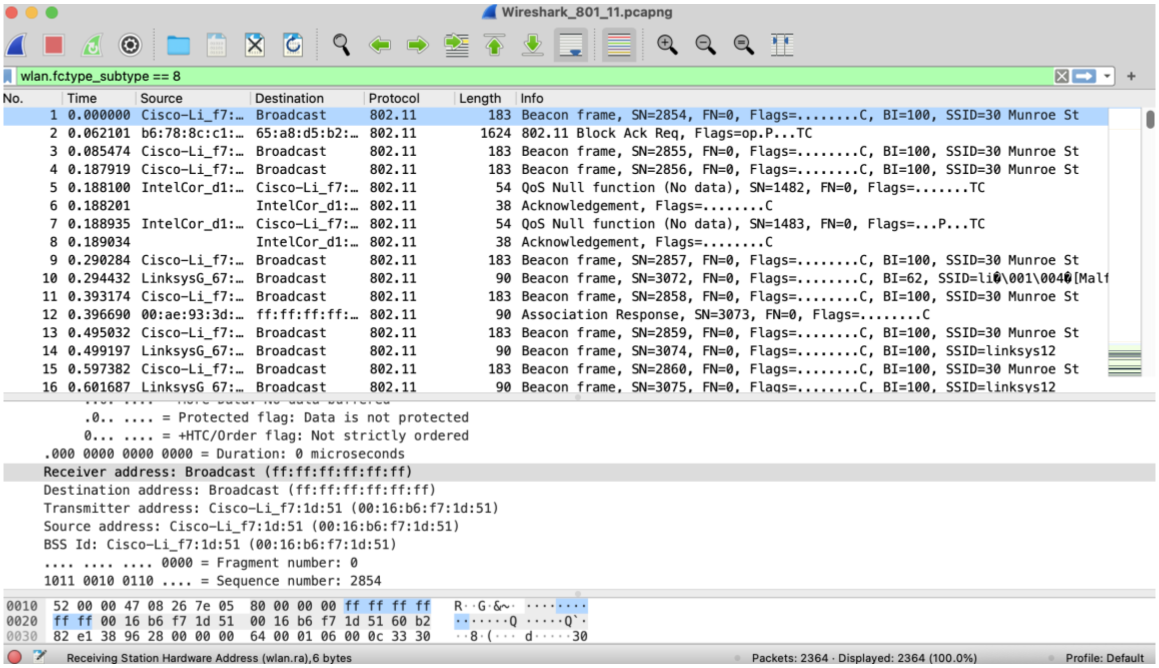
Wireshark_801_11.pcapng   Packets: 2364 · Displayed: 2364 (100.0%)   Profile: Default

Figure 2: Wireshark window, after opening the Wireshark_801_11.pcapng file

2. Beacon Frames

First, let's take a look at 802.11 beacon frames. Recall that beacon frames are used by an 802.11 AP to advertise its existence. Let's use our 802.11 filter cheat-sheet (here): enter `wlan.fc.type_subtype == 8` into Wireshark's display filter window, so that Wireshark only displays beacon frames (which have an 802.11 subtype of 8). Your Wireshark window should look similar to Figure 3.

Faris Soepangat
1001374988
CSE 4344
Due April 29, 2024



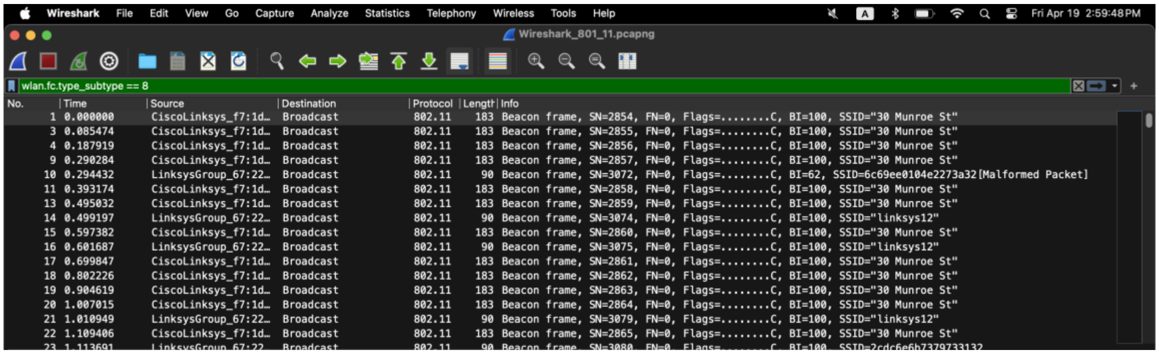
```
wlan.fctype_subtype == 8

No.  Time     Source           Destination      Protocol  Length  Info
   1 0.000000 Cisco-Li_f7:…    Broadcast        802.11     183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   2 0.062101 b6:78:8c:c1:…    65:a8:d5:b2:…    802.11    1624 802.11 Block Ack Req, Flags=op.P...TC
   3 0.085474 Cisco-Li_f7:…    Broadcast        802.11     183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   4 0.187919 Cisco-Li_f7:…    Broadcast        802.11     183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   5 0.188100 IntelCor_d1:…    Cisco-Li_f7:…    802.11      54 QoS Null function (No data), SN=1482, FN=0, Flags=.......TC
   6 0.188201                  IntelCor_d1:…    802.11      38 Acknowledgement, Flags=........C
   7 0.188935 IntelCor_d1:…    Cisco-Li_f7:…    802.11      54 QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
   8 0.189034                  IntelCor_d1:…    802.11      38 Acknowledgement, Flags=........C
   9 0.290284 Cisco-Li_f7:…    Broadcast        802.11     183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
  10 0.294432 LinksysG_67:…    Broadcast        802.11      90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=li�\001\004�[Malf
  11 0.393174 Cisco-Li_f7:…    Broadcast        802.11     183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
  12 0.396690 00:ae:93:3d:…    ff:ff:ff:ff:…    802.11      90 Association Response, SN=3073, FN=0, Flags=........C
  13 0.495032 Cisco-Li_f7:…    Broadcast        802.11     183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
  14 0.499197 LinksysG_67:…    Broadcast        802.11      90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID=linksys12
  15 0.597382 Cisco-Li_f7:…    Broadcast        802.11     183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
  16 0.601687 LinksysG_67:…    Broadcast        802.11      90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID=linksys12

        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
    .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)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    1011 0010 0110 .... = Sequence number: 2854

0010  52 00 00 47 08 26 7e 05  80 00 00 00 ff ff ff ff   R··G·&~· ········
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 60 b2   ·······Q ·····Q`·
0030  82 e1 38 96 28 00 00 00  64 00 01 06 00 0c 33 30   ··8·(··· d·····30

Receiving Station Hardware Address (wlan.ra),6 bytes    Packets: 2364 · Displayed: 2364 (100.0%)    Profile: Default
```

Figure3: Wireshark window, showing beacon frames

To answer some of the questions below, you'll want to look at the details in the *Info* field in the rightmost column of the Wireshark display; to answer other questions you'll need to dig into the "802.11 Protocol" frame and subfields in the middle Wireshark window.

1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace? [Hint: look at the *Info* field. To display only beacon frames, neter `wlan.fc.type_subtype == 8` into the Wireshark display filter].

   The SSIDs of the two access points that are issuing most of the beacon frames in this trace are '30 Munroe St' and 'linksys12'.

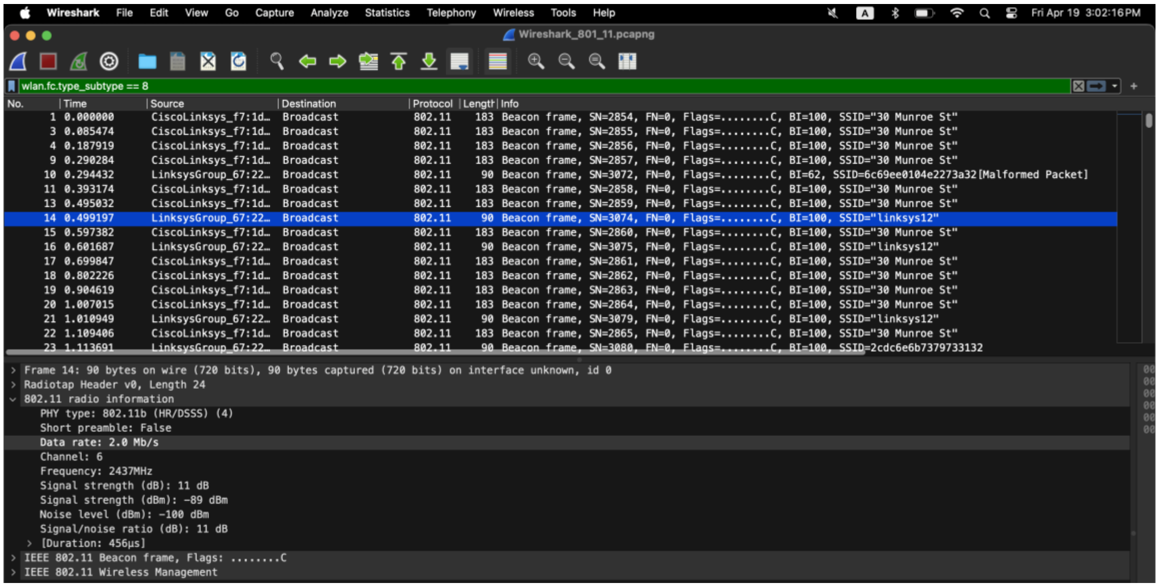


```
wlan.fc.type_subtype == 8

No.  Time      Source                Destination   Protocol  Length  Info
   1 0.000000  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   3 0.085474  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   4 0.187919  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   9 0.290284  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  10 0.294432  LinksysGroup_67:22…   Broadcast     802.11     90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=6c69ee0104e2273a32[Malformed Packet]
  11 0.393174  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  13 0.495032  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  14 0.499197  LinksysGroup_67:22…   Broadcast     802.11     90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID="linksys12"
  15 0.597382  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  16 0.601687  LinksysGroup_67:22…   Broadcast     802.11     90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID="linksys12"
  17 0.699847  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  18 0.802226  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  19 0.904619  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  20 1.007015  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  21 1.010949  LinksysGroup_67:22…   Broadcast     802.11     90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID="linksys12"
  22 1.109406  CiscoLinksys_f7:1d…   Broadcast     802.11    183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  23 1.113691  LinksysGroup_67:22…   Broadcast     802.11     90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=2cdc6e6b7379733132
```

2. What 802.11 channel is being used by both of these access points [Hint: you'll need to dig into the radio information in an 802.11 beacon frame]

Faris Soepangat
1001374988
CSE 4344
Due April 29, 2024

Channel 6 is being used by both of these access points.


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Fri Apr 19 3:02:16PM
Wireshark_801_11.pcapng

wlan.fc.type_subtype == 8

```
No.   Time      Source                Destination  Protocol Length Info
    1 0.000000  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    3 0.085474  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    4 0.187919  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    9 0.290284  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   10 0.294432  LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=6c69ee0104e2273a32[Malformed Packet]
   11 0.393174  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   13 0.495032  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   14 0.499197  LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID="linksys12"
   15 0.597382  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   16 0.601687  LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID="linksys12"
   17 0.699847  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   18 0.802226  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   19 0.904619  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   20 1.007015  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   21 1.010949  LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID="linksys12"
   22 1.109406  CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   23 1.113691  LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=2cdc6e6b7379733132
```

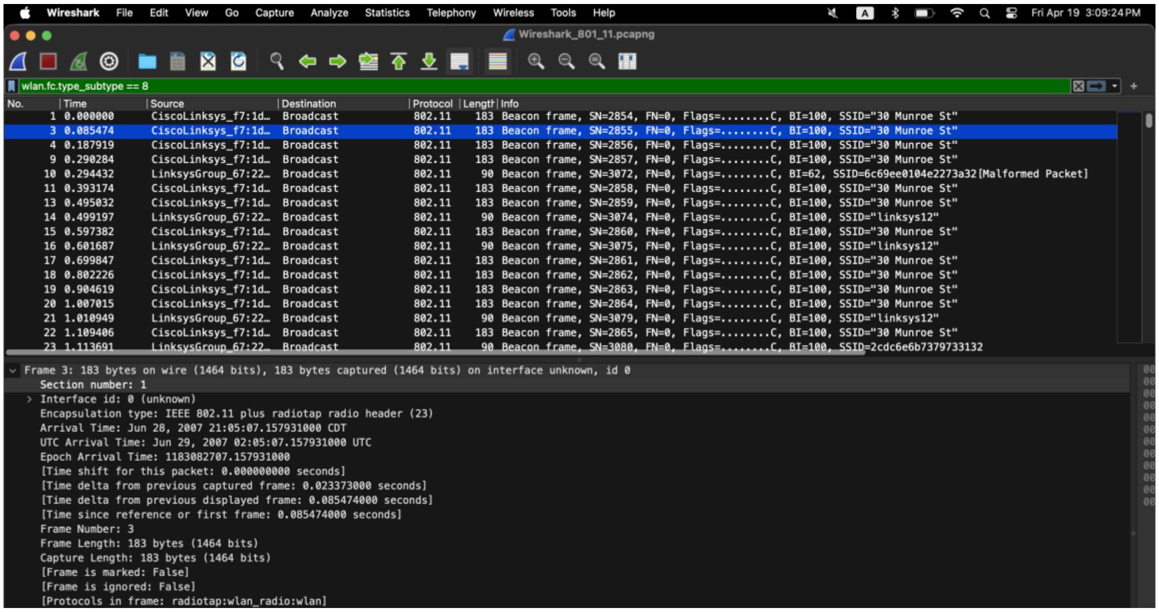
```
> Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
v 802.11 radio information
    PHY type: 802.11b (HR/DSSS) (4)
    Short preamble: False
    Data rate: 2.0 Mb/s
    Channel: 6
    Frequency: 2437MHz
    Signal strength (dB): 11 dB
    Signal strength (dBm): -89 dBm
    Noise level (dBm): -100 dBm
    Signal/noise ratio (dB): 11 dB
  > [Duration: 456µs]
> IEEE 802.11 Beacon frame, Flags: ........C
> IEEE 802.11 Wireless Management
```

Now let's take a look at the beacon frame sent at t=0.085474.

3. What is the interval of time between the transmissions of beacon frames from this access point (AP)? (Hint: this interval of time is contained in a field within the beacon frame itself).

   The interval of time between the transmissions of beacon frames from this access point (AP) is 0.1024 seconds.

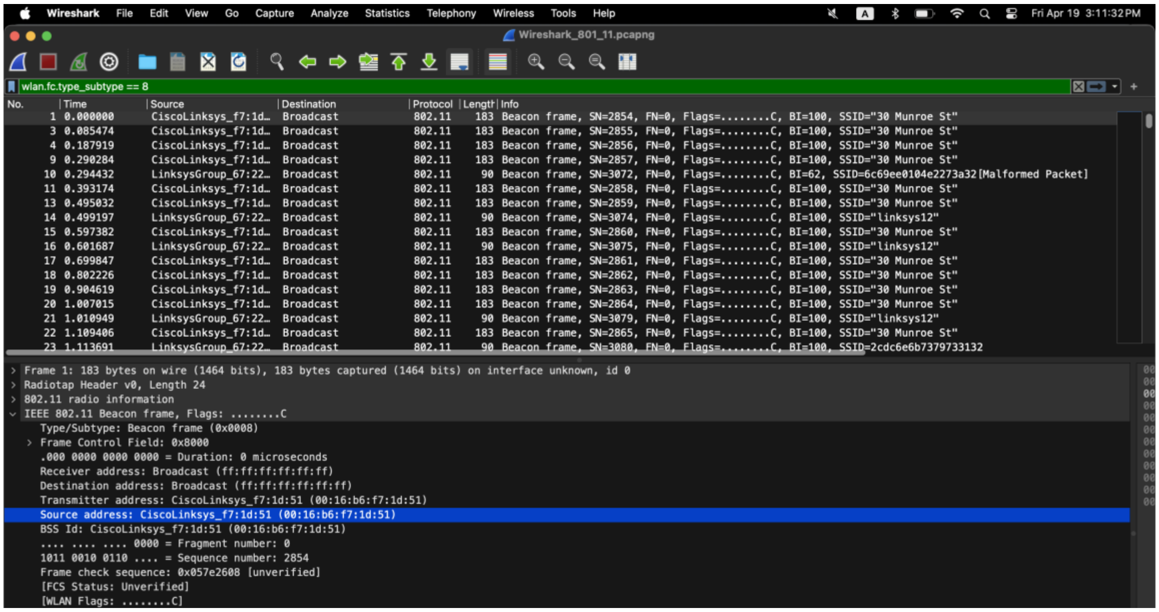
Faris Soepangat
1001374988
CSE 4344
Due April 29, 2024



```
wlan.fc.type_subtype == 8

No.  Time       Source                Destination  Protocol Length Info
  1 0.000000   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  3 0.085474   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  4 0.187919   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  9 0.290284   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 10 0.294432   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=6c69ee0104e2273a32[Malformed Packet]
 11 0.393174   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 13 0.495032   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 14 0.499197   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID="linksys12"
 15 0.597382   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 16 0.601687   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID="linksys12"
 17 0.699847   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 18 0.802226   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 19 0.904619   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 20 1.007015   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 21 1.010949   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID="linksys12"
 22 1.109406   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 23 1.113691   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=2cdc6e6b7379733132

v Frame 3: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
    Section number: 1
  > Interface id: 0 (unknown)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 28, 2007 21:05:07.157931000 CDT
    UTC Arrival Time: Jun 29, 2007 02:05:07.157931000 UTC
    Epoch Arrival Time: 1183082707.157931000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.023373000 seconds]
    [Time delta from previous displayed frame: 0.085474000 seconds]
    [Time since reference or first frame: 0.085474000 seconds]
    Frame Number: 3
    Frame Length: 183 bytes (1464 bits)
    Capture Length: 183 bytes (1464 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
```

4. What (in hexadecimal notation) is the source MAC address on the beacon frame from this access point? 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 9.2.3-9.2.4.1in the IEEE 802.11 standards document, excerpted here.

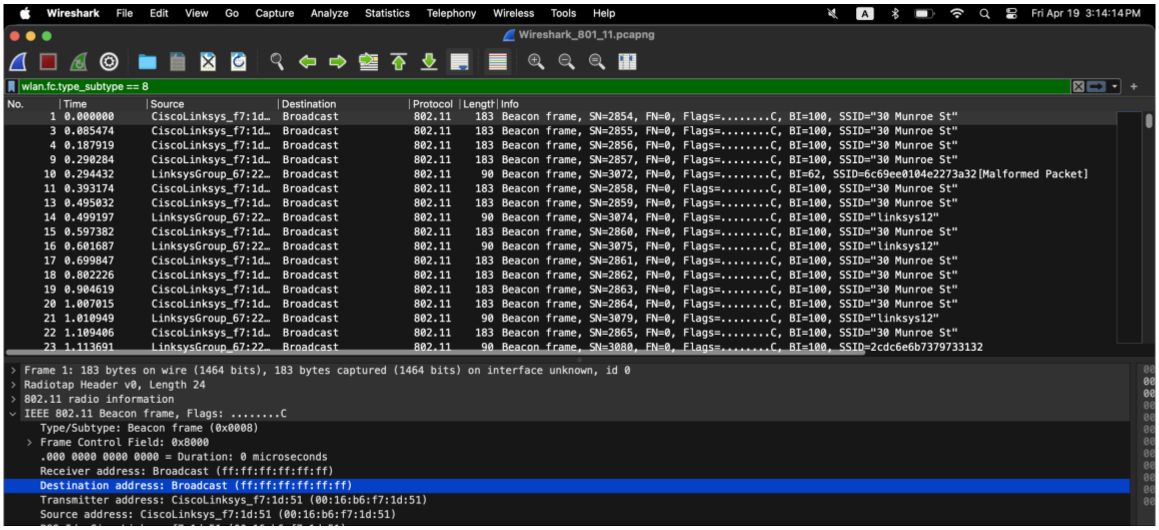
   The source MAC address on the beacon frame from this access point is 00:16:b6:f7:1d:51.



```
wlan.fc.type_subtype == 8

No.  Time       Source                Destination  Protocol Length Info
  1 0.000000   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  3 0.085474   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  4 0.187919   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  9 0.290284   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 10 0.294432   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=6c69ee0104e2273a32[Malformed Packet]
 11 0.393174   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 13 0.495032   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 14 0.499197   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID="linksys12"
 15 0.597382   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 16 0.601687   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID="linksys12"
 17 0.699847   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 18 0.802226   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 19 0.904619   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 20 1.007015   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 21 1.010949   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID="linksys12"
 22 1.109406   CiscoLinksys_f7:1d…   Broadcast    802.11   183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 23 1.113691   LinksysGroup_67:22…   Broadcast    802.11    90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=2cdc6e6b7379733132

> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .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: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    1011 0010 0110 .... = Sequence number: 2854
    Frame check sequence: 0x057e2608 [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ........C]
```

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

   The destination MAC address on the beacon frame from 30 Munroe St is ff:ff:ff:ff:ff:ff.



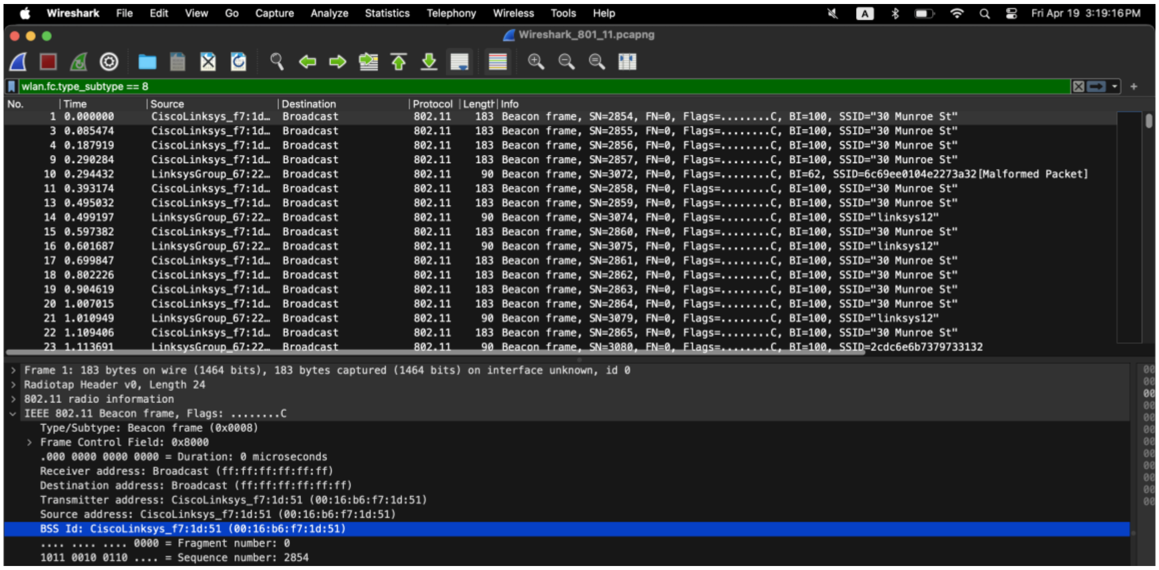
wlan.fc.type_subtype == 8

```
No.   |Time       |Source                 |Destination        |Protocol |Lengtt|Info
    1 0.000000     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    3 0.085474     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    4 0.187919     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    9 0.290284     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   10 0.294432     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=6c69ee0104e2273a32[Malformed Packet]
   11 0.393174     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   13 0.495032     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   14 0.499197     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID="linksys12"
   15 0.597382     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   16 0.601687     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID="linksys12"
   17 0.699847     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   18 0.802226     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   19 0.904619     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   20 1.007015     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   21 1.010949     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID="linksys12"
   22 1.109406     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   23 1.113691     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=2cdc6e6b7379733132
```

```
> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .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: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

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

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



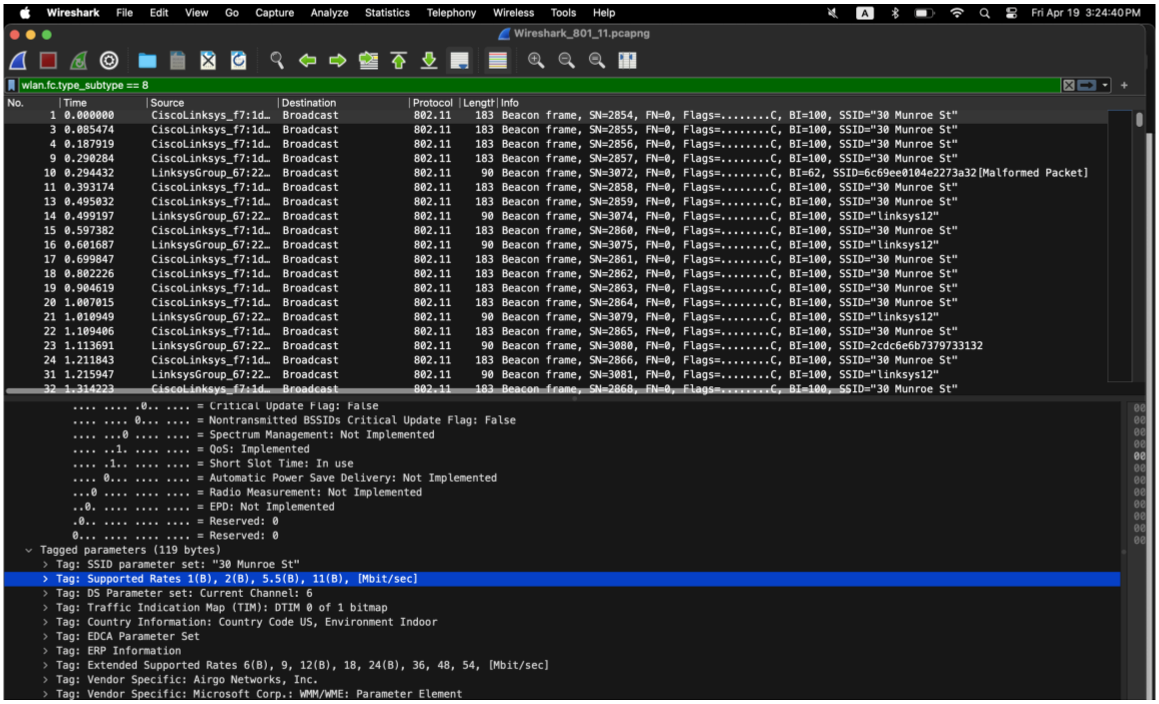
wlan.fc.type_subtype == 8

```
No.   |Time       |Source                 |Destination        |Protocol |Lengtt|Info
    1 0.000000     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    3 0.085474     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    4 0.187919     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    9 0.290284     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   10 0.294432     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=6c69ee0104e2273a32[Malformed Packet]
   11 0.393174     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   13 0.495032     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   14 0.499197     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID="linksys12"
   15 0.597382     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   16 0.601687     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID="linksys12"
   17 0.699847     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   18 0.802226     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   19 0.904619     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   20 1.007015     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   21 1.010949     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID="linksys12"
   22 1.109406     CiscoLinksys_f7:1d…    Broadcast           802.11    183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   23 1.113691     LinksysGroup_67:22…    Broadcast           802.11     90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=2cdc6e6b7379733132
```

```
> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .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: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    1011 0010 0110 .... = Sequence number: 2854
```

7. 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? [Note: the traces were taken on a rather old AP].

   The four data rates are 1(B), 2(B), 5.5(B) and 11(B) [Mbit/sec]. The eights additional "extended supported rates" are 6(B), 9, 12(B), 18, 24(B) 36, 48, and 54 [Mbit/sec].



```
wlan.fc.type_subtype == 8
No.   Time        Source                Destination      Protocol  Length Info
    1 0.000000    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    3 0.085474    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    4 0.187919    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
    9 0.290284    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   10 0.294432    LinksysGroup_67:22…   Broadcast        802.11     90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=6c69ee0104e2273a32[Malformed Packet]
   11 0.393174    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   13 0.495032    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   14 0.499197    LinksysGroup_67:22…   Broadcast        802.11     90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID="linksys12"
   15 0.597382    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   16 0.601687    LinksysGroup_67:22…   Broadcast        802.11     90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID="linksys12"
   17 0.699847    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   18 0.802226    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   19 0.904619    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   20 1.007015    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   21 1.010949    LinksysGroup_67:22…   Broadcast        802.11     90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID="linksys12"
   22 1.109406    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   23 1.113691    LinksysGroup_67:22…   Broadcast        802.11     90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=2cdc6e6b7379733132
   24 1.211843    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   31 1.215947    LinksysGroup_67:22…   Broadcast        802.11     90 Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID="linksys12"
   32 1.314223    CiscoLinksys_f7:1d…   Broadcast        802.11    183 Beacon frame, SN=2868, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"

        .... .... .0.. .... = Critical Update Flag: False
        .... .... 0... .... = Nontransmitted BSSIDs Critical Update Flag: False
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... ..1. .... .... = QoS: Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = EPD: Not Implemented
        .0.. .... .... .... = Reserved: 0
        0... .... .... .... = Reserved: 0
  ⌄ Tagged parameters (119 bytes)
    > Tag: SSID parameter set: "30 Munroe St"
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Indoor
    > Tag: EDCA Parameter Set
    > Tag: ERP Information
    > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Vendor Specific: Airgo Networks, Inc.
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

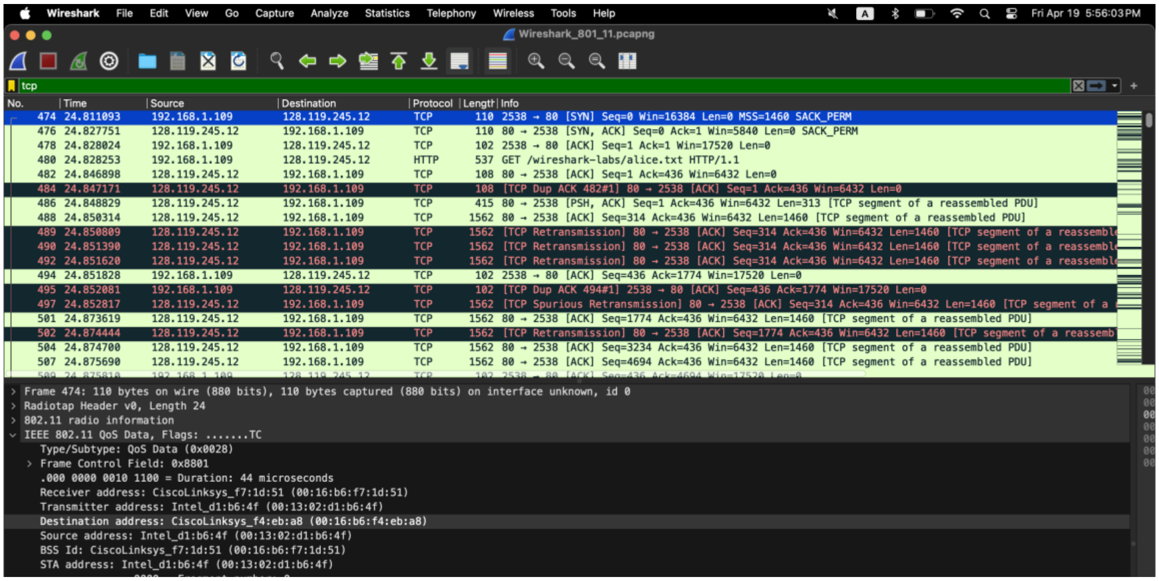
3. Data Transfer

Since the trace starts with the host already associated with the AP, let's next look at data transfer over an 802.11 association before looking at AP association/disassociation. Recall that in this trace, 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. Then, at *t=32.82*, the host makes an HTTP request to http://www.cs.umass.edu.

8. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt) at t=24.8110. 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 for the TCP syn segment?

Faris Soepangat
1001374988
CSE 4344
Due April 29, 2024

The three MAC address fields in the 802.11 frame are the Destination Address of 00:16:b6:f4:eb:a8, Source Address of 00:13:02:d1:b6:4f, and BSS Id of 00:16:b6:f7:1d:51. The Destination Address corresponds to the first-hop router. The Source Address corresponds to the host. The BSS Id corresponds to the access point. The IP address of the wireless host sending this TCP segment is 192.168.1.109. The destination IP address for the TCP syn segment is 128.199.245.12.



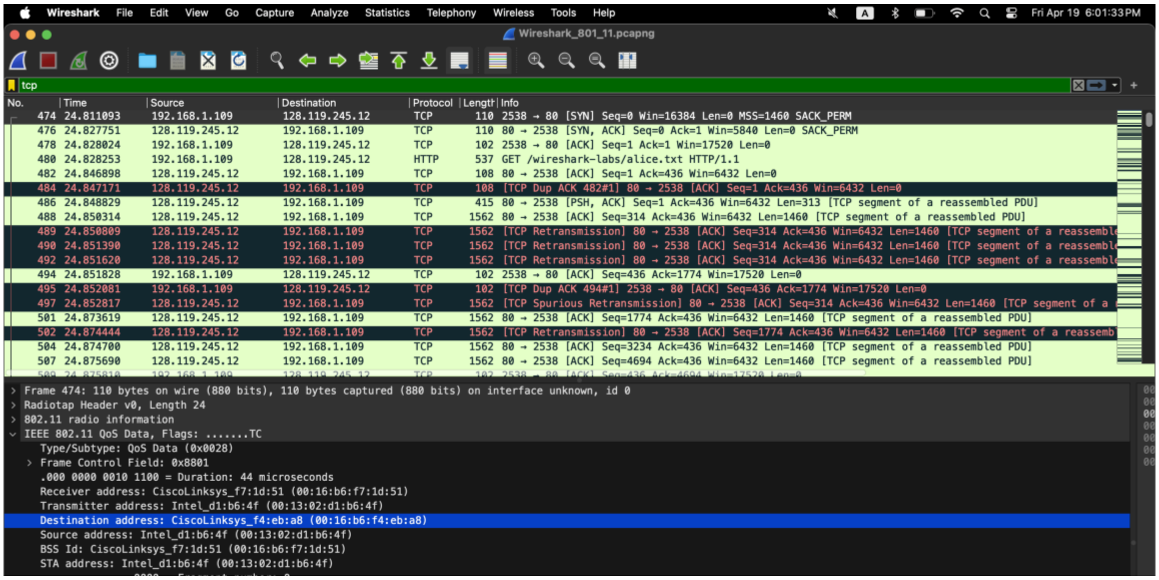
```
No.      |Time       |Source          |Destination     |Protocol |Length|Info
   474 24.811093  192.168.1.109   128.119.245.12  TCP       110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   476 24.827751  128.119.245.12  192.168.1.109   TCP       110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
   478 24.828024  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
   480 24.828253  192.168.1.109   128.119.245.12  HTTP      537 GET /wireshark-labs/alice.txt HTTP/1.1
   482 24.846898  128.119.245.12  192.168.1.109   TCP       108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
   484 24.847171  128.119.245.12  192.168.1.109   TCP       108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
   486 24.848829  128.119.245.12  192.168.1.109   TCP       415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
   488 24.850314  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
   489 24.850809  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemble
   490 24.851390  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemble
   492 24.851620  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemble
   494 24.851828  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
   495 24.852081  192.168.1.109   128.119.245.12  TCP       102 [TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
   497 24.852817  128.119.245.12  192.168.1.109   TCP      1562 [TCP Spurious Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a
   501 24.873619  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
   502 24.874444  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemb
   504 24.874700  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=3234 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
   507 24.875690  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=4694 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
   509 24.875810  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=436 Ack=4694 Win=17520 Len=0
```

```
> Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
```

9. Does the destination IP address of this TCP SYN correspond to the host, access point, first-hop router, or the destination web server?

   The destination IP address of this TCP SYN corresponds to the destination web server gaia.cs.umass.edu.

Faris Soepangat
1001374988
CSE 4344
Due April 29, 2024



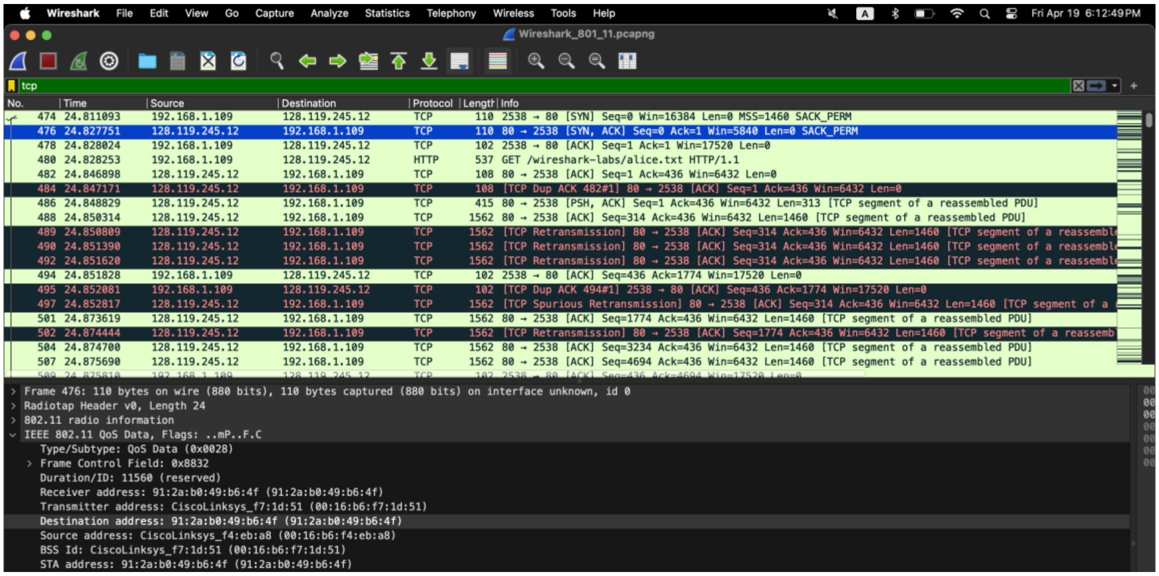
```
No.   Time       Source          Destination     Protocol Length Info
  474 24.811093  192.168.1.109   128.119.245.12  TCP       110  2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
  476 24.827751  128.119.245.12  192.168.1.109   TCP       110  80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
  478 24.828024  192.168.1.109   128.119.245.12  TCP       102  2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
  480 24.828253  192.168.1.109   128.119.245.12  HTTP      537  GET /wireshark-labs/alice.txt HTTP/1.1
  482 24.846898  128.119.245.12  192.168.1.109   TCP       108  80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  484 24.847171  128.119.245.12  192.168.1.109   TCP       108  [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  486 24.848829  128.119.245.12  192.168.1.109   TCP       415  80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
  488 24.850314  128.119.245.12  192.168.1.109   TCP      1562  80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
  489 24.850809  128.119.245.12  192.168.1.109   TCP      1562  [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemble
  490 24.851390  128.119.245.12  192.168.1.109   TCP      1562  [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemble
  492 24.851620  128.119.245.12  192.168.1.109   TCP      1562  [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemble
  494 24.851828  192.168.1.109   128.119.245.12  TCP       102  2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
  495 24.852081  192.168.1.109   128.119.245.12  TCP       102  [TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
  497 24.852817  128.119.245.12  192.168.1.109   TCP      1562  [TCP Spurious Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a
  501 24.873619  128.119.245.12  192.168.1.109   TCP      1562  80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
  502 24.874444  128.119.245.12  192.168.1.109   TCP      1562  [TCP Retransmission] 80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemb
  504 24.874700  128.119.245.12  192.168.1.109   TCP      1562  80 → 2538 [ACK] Seq=3234 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
  507 24.875690  128.119.245.12  192.168.1.109   TCP      1562  80 → 2538 [ACK] Seq=4694 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
  509 24.875810  192.168.1.109   128.119.245.12  TCP       102  2538 → 80 [ACK] Seq=436 Ack=4694 Win=17520 Len=0
```

```
> Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
```

10. Find the 802.11 frame containing the SYNACK segment for this TCP session received at t=24.8277 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 three MAC address fields in the 802.11 frame are the Destination Address of 91:2a:b0:49:b6:4f, Source Address of 00:16:b6:f4:eb:a8, and BSS Id of 00:16:b6:f7:1d:51. The Destination Address corresponds to the host. The Source Address corresponds to the first-hop router. The BSS Id corresponds to the access point. The sender MAC address in the frame does not correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram. The IP address of the wireless host sending this TCP segment is 128.119.245.12. The destination IP address for the TCP syn segment is 192.168.1.109.

Faris Soepangat
1001374988
CSE 4344
Due April 29, 2024



tcp

```
No.  Time       Source          Destination     Protocol Length Info
 474 24.811093  192.168.1.109   128.119.245.12  TCP       110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
 476 24.827751  128.119.245.12  192.168.1.109   TCP       110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
 478 24.828024  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
 480 24.828253  192.168.1.109   128.119.245.12  HTTP      537 GET /wireshark-labs/alice.txt HTTP/1.1
 482 24.846898  128.119.245.12  192.168.1.109   TCP       108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
 484 24.847171  128.119.245.12  192.168.1.109   TCP       108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
 486 24.848829  128.119.245.12  192.168.1.109   TCP       415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
 488 24.850314  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
 489 24.850809  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemble
 490 24.851390  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemble
 492 24.851620  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemble
 494 24.851828  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
 495 24.852081  192.168.1.109   128.119.245.12  TCP       102 [TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
 497 24.852817  128.119.245.12  192.168.1.109   TCP      1562 [TCP Spurious Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a
 501 24.873619  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
 502 24.874444  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP segment of a reassemb
 504 24.874700  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=3234 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
 507 24.875690  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=4694 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
 509 24.875810  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=436 Ack=4694 Win=17520 Len=0
```

```
> Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
```