

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

Wireshark_802_11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

beacon

No.	Time	Source	Destination	Protocol	Length	Info
1456	40.224429	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3481, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1457	40.326864	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3482, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
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
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
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
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
1462	40.736666	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1562, FN=0, Flags=.....TC
1463	40.736765	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1562, FN=0, Flags=....R..TC
1464	40.736861	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1465	40.737572	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1563, FN=0, Flags=...P...TC
1466	40.737670	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
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
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

[Time shift for this packet: 0.00000000 seconds]

Epoch Time: 11-08-27 17:08:09.72000 seconds

[Time delta from previous captured frame: 0.102415000 seconds]

[Time delta from previous displayed frame: 0.102415000 seconds]

[Time since reference or first frame: 40.736515000 seconds]

Frame Number: 1461

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]

- > Radiotap Header v0, Length 24
- > 802.11 radio information
- > IEEE 802.11 Beacon frame, Flags:C
- ▼ IEEE 802.11 wireless LAN management frame

```

0000  00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e4 9c  ....X..
0010  52 00 00 48 0e ce a0 60 80 00 00 00 ff ff ff ff  R..H...
0020  ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 e0 d9  ....Q....
0030  82 c1 a6 98 28 00 00 00 64 00 01 06 00 0c 33 30  ....(....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 0b  .......USI..
0060  1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e  .......BC^
0070  00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48  .b2/.*. 2....$.H
  
```

Time delta from previous captured frame (frame.time_delta)

Packets: 2364 · Displayed: 2364 (100.0%) · Load time: 0:0.58

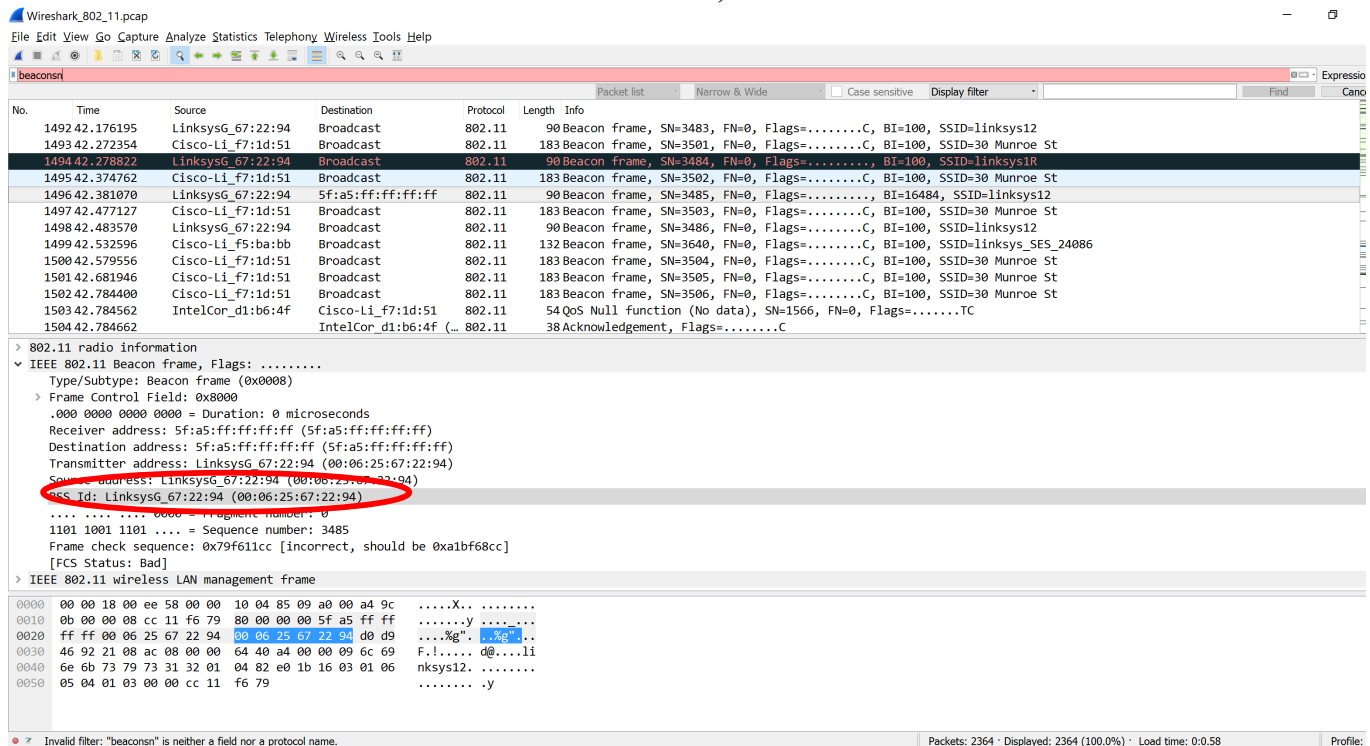
Profile:

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).



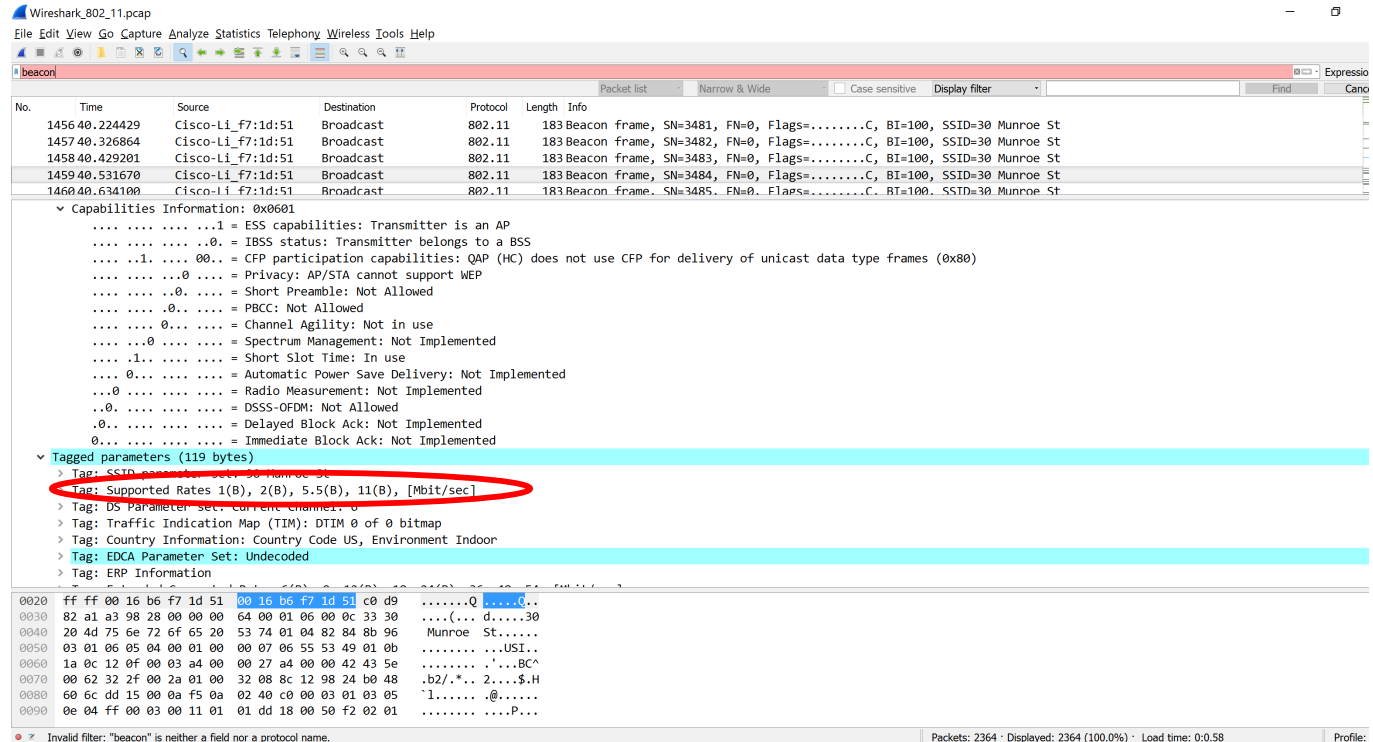
- The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff.

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



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)

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 AUTHENTICATION 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 AUTHENTICATION 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 == 11 and 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.

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.