

Wireshark LAB: 802.11

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

Answer: The SSID of the two access points that are issuing most of the beacons frames in this trace are `30 Munroe St` and `linksys_ses_24086`.

2. What are the intervals of time between the transmission of the beacon frames the `linksys_ses_24086` access point? From the `30 Munroe St` access point?

Answer: The intervals of time between the transmission of the beacon frames is
`Beacon intervals: 0.102400 [seconds].`

3. What (in hexadecimal notation) is the source MAC address on the beacon frame from `30 Munroe St`? Recall from figure 6.13 in the text that the source, destination, and BSS are the 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 standard documents (cited above).

Answer: The source MAC address on the beacon frame from `30 Munroe St` is
`Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)`

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

Answer: The destination MAC address on the beacon frame from `30 Munroe St` is
`Destination address: Broadcast (ff:ff:ff:ff:ff:ff)`

5. What (hexadecimal notation) is the MAC BSS id on the beacon frame from `30 Munroe St`?

Answer: The MAC BDD id on beacon frame from `30 Munroe St` is
`BSS Id: Cisco-Li_f7:1d:51 (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?

Answer: 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”, these rates are...

Extended Supported Rates: 6 (B)
Extended Supported Rates: 9
Extended Supported Rates: 12 (B)
Extended Supported Rates: 18
Extended Supported Rates: 24 (B)
Extended Supported Rates: 36
Extended Supported Rates: 48
Extended Supported Rates: 54 [Mbit/sec]

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=100, SSID=30 Munroe St
2	0.062101	b6:78:8c:c1:ae:c0	(65:a8:d5:b2:c1:99)	802.11	1624	802.11 Block Ack Req, Flags=op.P...T.
3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	0.188100	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	0.188201	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	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, Flags=...P...TC
8	0.189034	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C

+	RadioTap Header v0, Length 24
+	IEEE 802.11 Beacon frame, Flags:C
+	Type/Subtype: Beacon frame (0x08)
+	Frame Control: 0x0080 (Normal)
+	Duration: 0
+	Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
+	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)
+	Fragment number: 0
+	Sequence number: 2854
+	Frame check sequence: 0x08267e05 [correct]
+	IEEE 802.11 wireless LAN management frame
+	Fixed parameters (12 bytes)
+	Timestamp: 0x000000289638e182
+	Beacon Interval: 0.102400 [Seconds]
+	Capabilities Information: 0x0601
+	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 0 bitmap

BEACON FRAME

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that

downloads alice.text). At what time is the TCP SYN sent? What are three MAC address field 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 this 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 corresponds to the host, access points, first-hop-router, some other network-attached device? Explain. (Hint: review Figure 5.19 in the text if you are unsure of how to answer this question, or the corresponding part of the next question. It's particularly important that you understand this).

Answer: The TCP SYN was sent at $t = 24.811093000$ seconds. The three MAC addresses fields in the 802.11 frame are 1. MAC address whose sending the TCP SYN or the Source address: IntelCor_d1:b6:4f(00:13:02:d1:b6:4f) 2. MAC address Destination: Cisco-Li_f4:eb:a8(00:16:b6:f4:eb:a8) 3. MAC address BSS Id: Cisco-Li_f7:1a:51(00:16:b6:f7:1d:51). The IP address of the wireless host sending the TCP SYN is 192.168.1.109, and the destination IP address is 128.119.245.12. It corresponds with the server gaia.cs.umass.edu, the destination MAC address of the frame containing the first TCP segment is different from the destination IP address (containing the IP packet).

8. Find the 802.11 frame containing the SYNACK segment for this TCP session. At what time is the TCP SYNACK received? What are three MAC address field in the 802.11 frame containing the SYNACK? Which MAC address in this frame corresponds to the host? To the access points? 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?

Answer: The TCP SYNACK was received at $t = 24.827751000$ seconds. The three MAC addresses fields in the 802.11 frame are 1. MAC Source address: Cisco-Li_f4:eb:a8(00:16:b6:f4:eb:a8) .2. MAC Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f) .3. MAC BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) . The MAC address for the destination (91:2a:b0:49:b6:4f) is different from the MAC address of the host used that sends the TCP SYN.

9. What two actions are taken (e.i., 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 the trace

collection began, and at what are these frames were sent? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there any other frame that you might have expected to see, but don't see here?

Answer: The two actions taken by the host in the trace just after $t = 49$ are 1.DHCP (an IP-layer protocol) with a time of $t = 49.583615000$ seconds and 2. Deauthentication (802.11 protocol) with a time of $t = 49.609617000$ seconds. One might have expected to see a DISASSOCIATION request to have been sent.

10. Examine the trace file and look for AUTHENTICATION frames sent from the host to an AP and vice versa. When is the first AUTHENTICATION frame 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 $t=49$?

Answer: The first AUTHENTICATION frame sent from the wireless host to the *linksys_ses_24086* is...
[Time since reference or first frame; 49.638857000 seconds]

11. Does the host want the authentication to require a key or be open?

Answer: By specifying Authentication Algorithm -Open System, 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?

Answer: A request for open access is being ignored because AP is configured to require a key when associating. That is why there is no reply shown in the frame from the AP.

13. Now let's consider what happens as the host gives up (sometimes after $t=63.0$) 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 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==1` and `wlan.fc.type==0` and `wlan.addr==IntelCo_d1:b6:4f` to display only the AUTHENTICATION frames in this trace for this wireless host.)

Answer: The AUTHENTICATION frame from host to the 30 Munroe St AP is at $t = 63.168087000$ seconds and the reply was sent to the host at $t = 63.16907100$ seconds.

2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication,
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication,
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication,
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication,
2274	68.662233	83:17:c6:ae:cd:9c	72:8e:bb:91:31:97	LLC	1586	I, N(R)=12, N(S)

```

Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Arrival Time: Jun 28, 2007 19:06:10.240544000 Pacific Daylight Time
Epoch Time: 1183082770.240544000 seconds
[Time delta from previous captured frame: 0.006815000 seconds]
[Time delta from previous displayed frame: 0.994017000 seconds]
[Time since reference or first frame: 63.168087000 seconds]
Frame Number: 2156

```

Authentication time after 63.0

2156	63.168087	IntelCor_d1:b6:4f	CISCO-Li_T/:1d:51	802.11	58	Authentication, SN
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN
2274	68.662233	83:17:c6:ae:cd:9c	72:8e:bb:91:31:97	LLC	1586	I, N(R)=12, N(S)=1

```

Frame 2158: 58 bytes on wire (464bits), 58 bytes captured (464 bits) on interface 0
Arrival Time: Jun 28, 2007 19:06:10.241528000 Pacific Daylight Time
Epoch Time: 1183082770.241528000 seconds
[Time delta from previous captured frame: 0.000849000 seconds]
[Time delta from previous displayed frame: 0.000984000 seconds]
[Time since reference or first frame: 63.169071000 seconds]
Frame Number: 2158

```

Authentication time of reply

14. Let's continue on with the association between the wireless host and the 30 Munroe St. AP that happens after $t=63.0$. An ASSOCIATION from host to AP, and a corresponding

ASSOCIATE RESPONSE frame from an 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.)

Answer: The time of the ASSOCIATE REQUEST from host to the 30 Munroe ST was sent is at $t = 63.169910000$ seconds and the reply was sent at $t = 63.192101000$ seconds.

2127	62.178194	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	107	Association Request
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response
2201	65.721718	DellComp_4f:36:23	Broadcast	ARP	106	who has 192.168.1.1

Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
 Arrival Time: Jun 28, 2007 19:06:10.242367000 Pacific Daylight Time
 Epoch Time: 1183082770.242367000 seconds
 [Time delta from previous captured frame: 0.000096000 seconds]
 [Time delta from previous displayed frame: 0.991716000 seconds]
 [Time since reference or first frame: 63.169910000 seconds]
 Frame Number: 2162

Association Request after 63.0

2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94 Association Response,
2201	65.721718	DellComp_4f:36:23	Broadcast	ARP	106 who_has 192.168.1.103

Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
 Arrival Time: Jun 28, 2007 19:06:10.264558000 Pacific Daylight Time
 Epoch Time: 1183082770.264558000 seconds
 [Time delta from previous captured frame: 0.021101000 seconds]
 [Time delta from previous displayed frame: 0.022191000 seconds]
 [Time since reference or first frame: 63.192101000 seconds]
 Frame Number: 2166

Association time of Reply

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.

Answer: The transmission rates that the host and the AP are willing to use are as follows...

Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18 [Mbit/sec]

Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec].

2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89 Association Request
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94 Association Response
2201	65.721718	DellComp_4f:36:23	Broadcast	ARP	106 who has 192.168.1.103
2216	66.235947	IntelCor_d1:b6:4f	Broadcast	LLC	388 U, func=UI; SNAP, OUI
2217	66.239199	IntelCor_d1:b6:4f	Broadcast	LLC	394 U, func=UI; SNAP, OUI
2218	66.240070	IntelCor_d1:b6:4f	Broadcast	ARP	88 Gratuitous ARP for 192.168.1.103

+	Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
+	Radiotap Header v0, Length 24
+	IEEE 802.11 Association Request, Flags:C
-	IEEE 802.11 wireless LAN management frame
+	Fixed parameters (4 bytes)
-	Tagged parameters (33 bytes)
+	Tag: SSID parameter set: 30 Munroe St
+	Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
+	Tag: QoS Capability
+	Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]

ASSOCIATION REQUEST Parameters Field

2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94 Association Response
2201	65.721718	DellComp_4f:36:23	Broadcast	ARP	106 who has 192.168.1.103
2216	66.235947	IntelCor_d1:b6:4f	Broadcast	LLC	388 U, func=UI; SNAP, OUI
2217	66.239199	IntelCor_d1:b6:4f	Broadcast	LLC	394 U, func=UI; SNAP, OUI
2218	66.240070	IntelCor_d1:b6:4f	Broadcast	ARP	88 Gratuitous ARP for 192.168.1.103

+	Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
+	Radiotap Header v0, Length 24
+	IEEE 802.11 Association Response, Flags:C
-	IEEE 802.11 wireless LAN management frame
+	Fixed parameters (6 bytes)
-	Tagged parameters (36 bytes)
+	Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
+	Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
+	Tag: EDCA Parameter Set: Tag 12 Len 18

ASSOCIATION RESPONSE Parameters Field.

16. Consider the first PROBE REQUEST and soonest subsequent PROBE RESPONSE PAIR

occurs after $t=2.0$ seconds in the trace. When are these frames sent and what are the sender, receiver and BSS ID MAC addresses for 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).

Answer: The frame request was sent at $t = 2.297613000$ seconds with

Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13),
 it's Destination address: Broadcast (ff:ff:ff:ff:ff:ff) and
 BSS Id: Broadcast (ff:ff:ff:ff:ff:ff). The frame response
 was sent at $t = 2.300697000$ seconds with

Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51). A
 PROBE REQUEST is used by a host in active scanning to find an Access
 Point. A PROBE RESPONSE is sent by the Access Point to the host sending
 the request.

49	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, S
50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, S
51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, S
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, S

[Time since reference or first frame: 2.297613000 seconds]
 Frame Number: 50
 Frame Length: 79 bytes (632 bits)
 Capture Length: 79 bytes (632 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: radiotap:wlan]
 Radiotap Header v0, Length 24
 IEEE 802.11 Probe Request, Flags:C
 Type/Subtype: Probe Request (0x04)
 Frame Control: 0x0040 (Normal)
 Duration: 0
 Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
 Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
 BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)

PROBE REQUEST after $t = 2.0$ seconds

50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN
51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, S
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, S

[Time since reference or first frame: 2.300697000 seconds]
 Frame Number: 51
 Frame Length: 177 bytes (1416 bits)
 Capture Length: 177 bytes (1416 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: radiotap:wlan]
 Radiotap Header v0, Length 24
 IEEE 802.11 Probe Response, Flags:C
 Type/Subtype: Probe Response (0x05)
 Frame Control: 0x0050 (Normal)
 Duration: 314
 Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
 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)

PROBE RESPONSE after $t = 2.0$ seconds