East West University

Department of CSE

Lab Report 03

CSE 453

Wireless Networking

Submitted To:

Md. Mahir Ashhab

Lecturer

Department of Computer Science and Engineering

Submitted By:

Adri Saha

ID: 2019-1-60-024

Submission Date: 31 August 2022

Wireshark Traces Answers

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

Ans: 30 Munroe St is issuing most of the beacon frames in this trace. And then 'linsys_SES_24086' are also seen which is issuing the same.

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	8c:c1:ae:c0:ea:2c	8c:c1:ae:c0:ea:2c (…	802.11	1624	PV1 Management[Malformed Packet]
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 (…	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 (…	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=100, SSID=30 Munroe St
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=li\001\004[Malformed Packet]
11	0.393174	Cisco-Li_f7:1d:51	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:0a:4a	00:ae:93:3d:0a:4a (…	802.11	90	PV1 Reserved
13	0.495032	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID=linksys12
15	0.597382	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID=30 Munroe St

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? (Hint: this interval of time is contained in the beacon frame itself).**

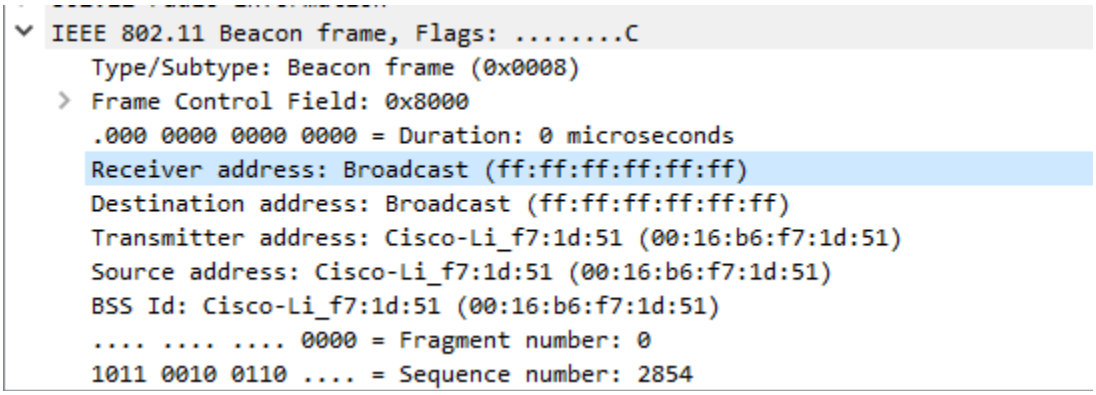
Ans: We see, beacon interval from both 'linksys_ses_24086' and '30 Munroe St.' is: 0.102400 Seconds.

```
> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
      Timestamp: 174319001986
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  > Tagged parameters (119 bytes)
```

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 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).**

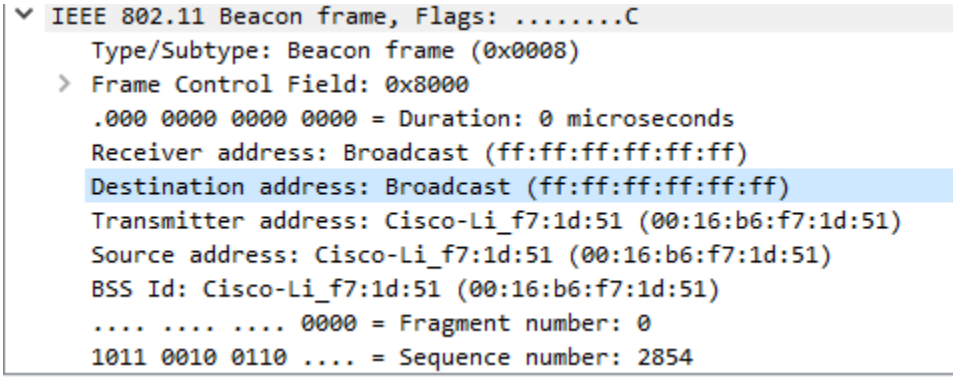
Ans: Receiver address: Broadcast (ff: ff: ff: ff: ff: ff)

Source MAC address: *00:16:b6:f7:1d:51*



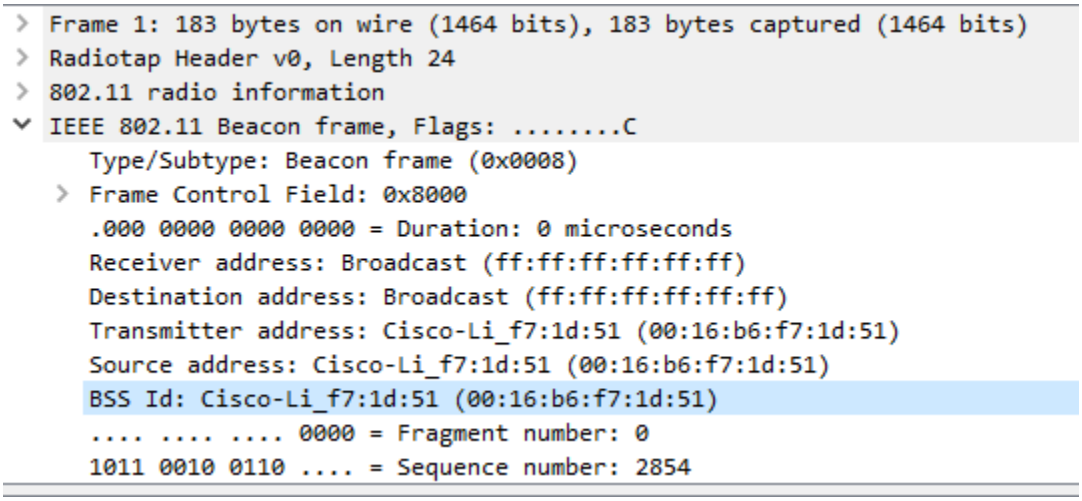
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??

Ans: Destination MAC address: Broadcast (ff:ff:ff:ff:ff:ff)



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

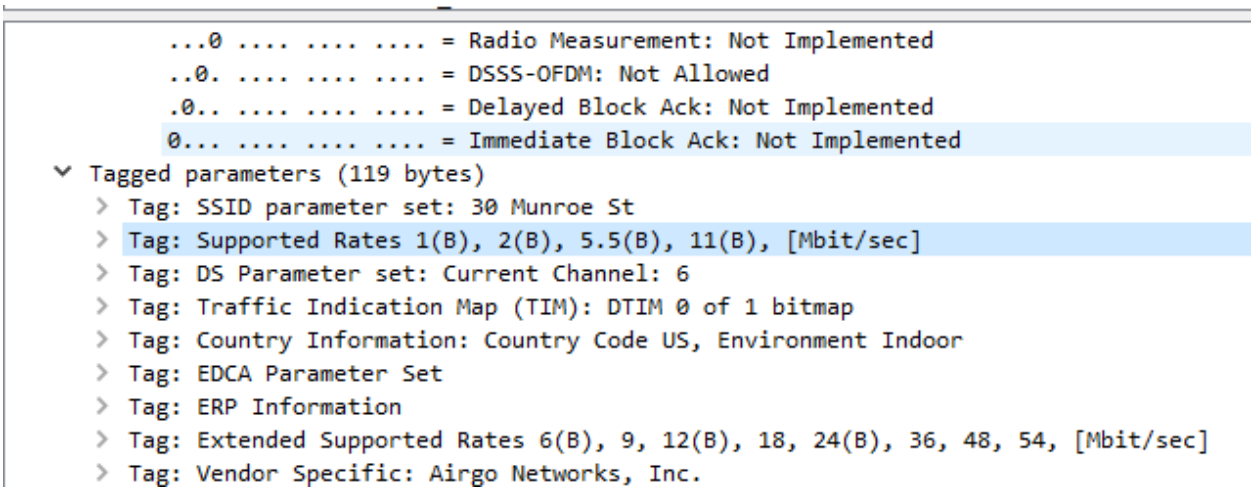
Ans: MAC BSS id on beacon frame: Cisco-Li_f7:1d:51 (00: 16: b6: f7: 1d: 51)



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?**

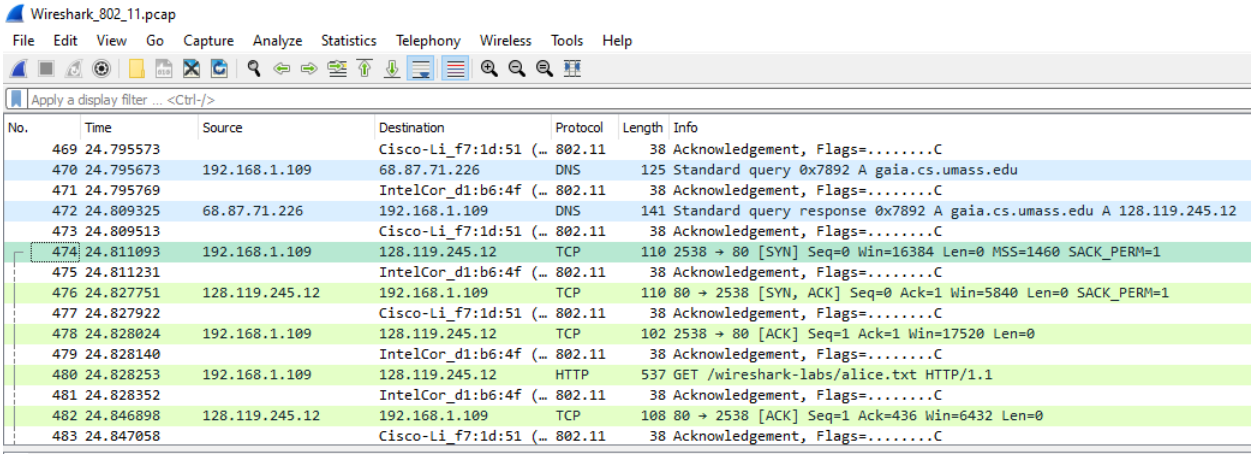
Ans: Supported 4 data rates are: 1(B), 2(B), 5.5(B), 11(B) Mbps and

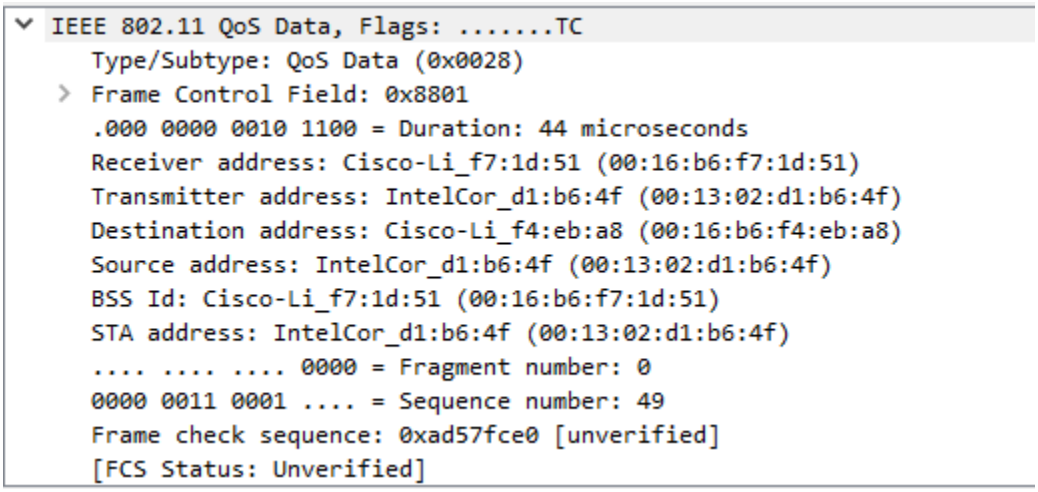
Eight additional extended supported rates are: 6(B), 9, 12(B), 18, 24(B), 36, 48, 54 Mbps.



7. **Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). At what time is the TCP SYN sent? 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. (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).**

Ans: The TCP SYN is sent at t = 24.811093 seconds into the trace. The MAC address for the host sending the TCP SYN is transmitter address: 00:13:02:d1:b6:4f.
The MAC address for the destination: which the first hop router to which the host is connected, is 00:16:b6:f4:eb:a8.
The MAC address for the BSS is 00:16:b6:f7:1d:51.
The IP address of the host sending the TCP SYN is 192.168.1.109.





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 fields in the 802.11 frame containing the SYNACK? 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?**

Ans: At time t = 24.827751 seconds into the trace, a TCP SYNACK is received.
The first hop router to which the host is connected is identified by the MAC address 00:16:b6:f4:eb:a8 as the sender of the 802.11 frame containing the TCP SYNACK segment.
The host itself, the destination, and its MAC address are 91:2a:b0:49:b6:4f.
The BSS's MAC address is 00:16:b6:f7:1d:51.
The server sending the TCP SYNACK has the IP address 128.199.245.12.

No.	Time	Source	Destination	Protocol	Length	Info
472	24.809325	68.87.71.226	192.168.1.109	DNS	141	Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
473	24.809513		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
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=1
475	24.811231		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
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=1
477	24.827922		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1
481	24.828352		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
482	24.846898	128.119.245.12	192.168.1.109	TCP	108	80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
483	24.847058		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
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
485	24.847267		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
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]

```
▼ 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: Cisco-Li_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: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124
    Frame check sequence: 0xecdc407d [unverified]
    [FCS Status: Unverified]
```

9.

10. 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, and at what times are these frames sent? (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?

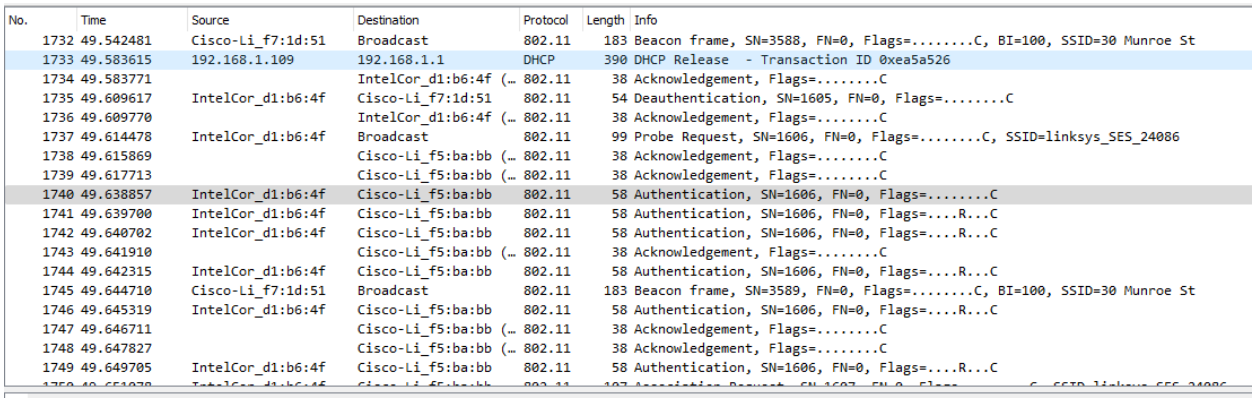
Ans: At 49.583615 sec, we see the host transmits DHCP release to the DHCP server in the network they are leaving (whose IP address is 192.168.1.1).
At time 49.609617, the host transmits a DEAUTHENTICATION frame (subframe type 12 [Deauthentication]; frametype 00 [Management]). A DISASSOCIATION request might have been anticipated to have been sent, for example.

No.	Time	Source	Destination	Protocol	Length	Info
1729	49.440041	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1730	49.440146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
1731	49.440243		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	49.583771		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=........C
1736	49.609770		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=........C, SSID=linksys_SES_24086
1738	49.615869		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1739	49.617713		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1743	49.641910		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C

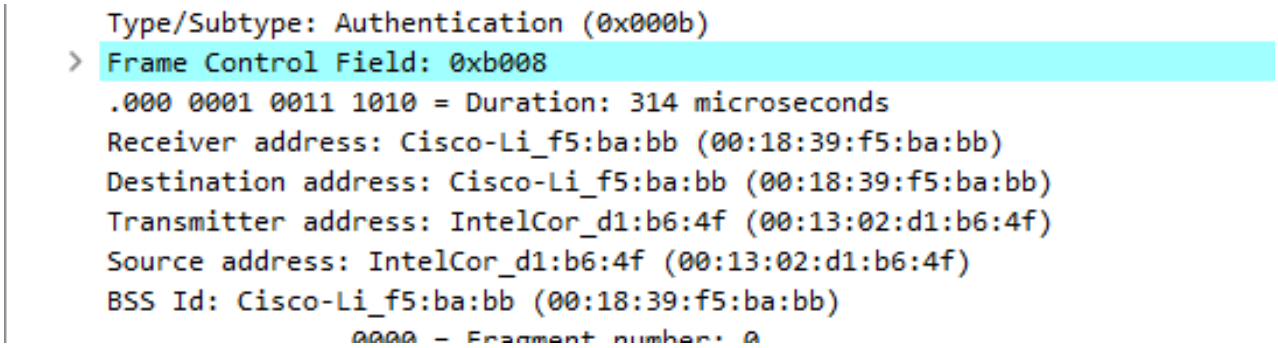
11. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. When is the first AUTHENTICATION frame sent from the wireless

host to the linksys_ses_24086 AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around t=49?

Ans: The host authenticates for the first time to the AP at time = 49.638857.



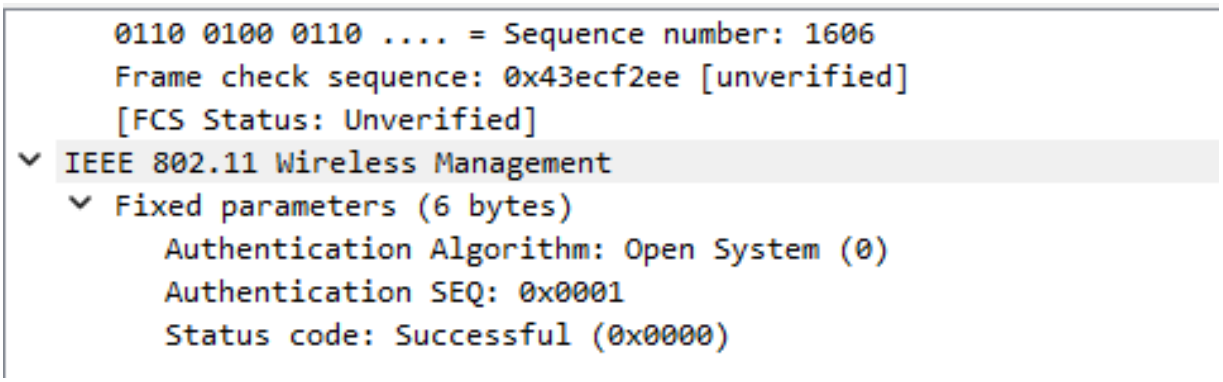
No.	Time	Source	Destination	Protocol	Length	Info
1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	49.583771		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=........C
1736	49.609770		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=........C, SSID=linksys_SES_24086
1738	49.615869		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1739	49.617713		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1743	49.641910		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1745	49.644710	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3589, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1747	49.646711		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1748	49.647827		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C



```
Type/Subtype: Authentication (0x000b)
> Frame Control Field: 0xb008
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
Destination address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
                0000 = Fragment number: 0
```

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

Ans: Yes. The host requests that the association be open by giving the authentication algorithm.



```
    0110 0100 0110 .... = Sequence number: 1606
    Frame check sequence: 0x43ecf2ee [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

13. Do you see a reply to AUTHENTICATION from the linksys_ses_24086 AP in the trace?

Ans: I am unable to find a reply from the AP. This is most likely because the AP is set up to require a key before connecting to it, and as a result, it is probably disregarding requests for open access.

14. Now let's consider what happens as the host gives up (sometime 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 AUTHENICATION 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 == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

Ans: AUTHENTICATION frame is transmitted from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 at t=63.168087 sec (the BSS).
An AUTHENTICATION is transmitted from the BSS to the wireless host in the reverse direction at t = 63.169071.

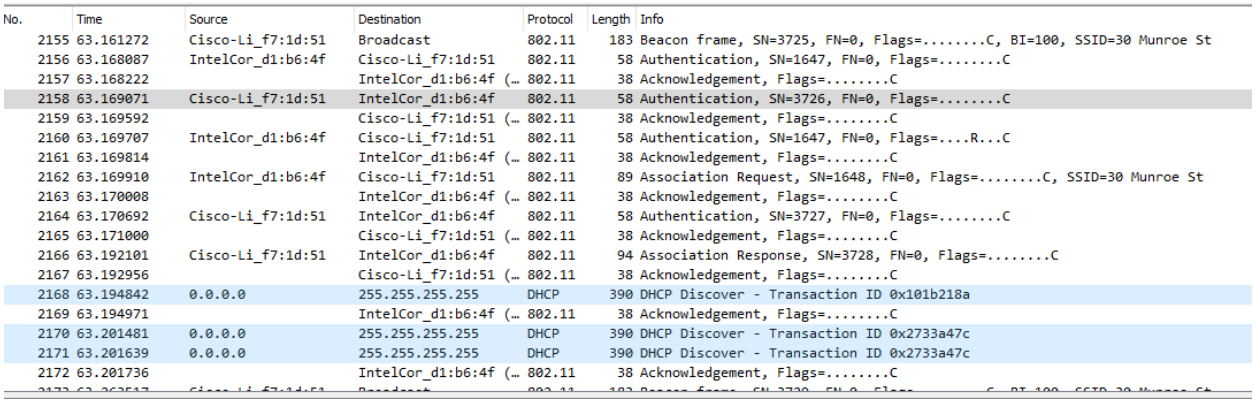
No.	Time	Source	Destination	Protocol	Length	Info
2149	63.094985	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2150	63.116231	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2151	63.135362	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2152	63.140106	IntelCor_d1:b6:4f	Broadcast	802.11	94	Probe Request, SN=1647, FN=0, Flags=........C, SSID=30 Munroe St
2153	63.142451	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3724, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2154	63.142860		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
2155	63.161272	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3725, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=........C
2157	63.168222		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=........C
2159	63.169592		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2161	63.169814		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=........C, SSID=30 Munroe St
2163	63.170008		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=........C
2165	63.171000		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=........C

```
Type/Subtype: Authentication (0x000b)
> Frame Control Field: 0xb000
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
.... .... .... 0000 = Fragment number: 0
0110 0110 1111 .... = Sequence number: 1647
Frame check sequence: 0x47e8cbe0 [unverified]
[FCS Status: Unverified]
```

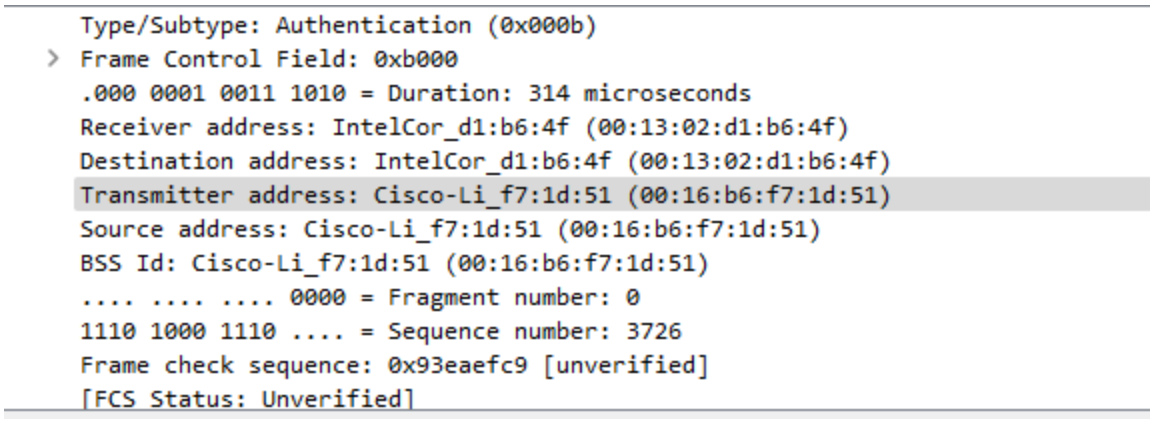
15. Let's continue on with the association between the wireless host and the 30 Munroe St AP that happens after t = 63.0. An ASSOCIATE from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associate with an AP. At what time is there an ASSOCIATE REQUEST 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.)

Ans: At time t = 63.169910, an ASSOCIATE REQUEST frame is sent from the wireless host, 00:13:02:d1:b6:4f, to 00:16:b7:f7:1d:51 (the BSS).
At time t = 63.192101, an ASSOCIATE RESPONSE is sent from the BSS to the wireless host in the other way.



No.	Time	Source	Destination	Protocol	Length	Info
2155	63.161272	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3725, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=........C
2157	63.168222		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=........C
2159	63.169592		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2161	63.169814		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=........C, SSID=30 Munroe St
2163	63.170008		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=........C
2165	63.171000		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=........C
2167	63.192956		Cisco-Li_f7:1d:51 (…	802.11	38	Acknowledgement, Flags=........C
2168	63.194842	0.0.0.0	255.255.255.255	DHCP	390	DHCP Discover - Transaction ID 0x101b218a
2169	63.194971		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C
2170	63.201481	0.0.0.0	255.255.255.255	DHCP	390	DHCP Discover - Transaction ID 0x2733a47c
2171	63.201639	0.0.0.0	255.255.255.255	DHCP	390	DHCP Discover - Transaction ID 0x2733a47c
2172	63.201736		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=........C



```
Type/Subtype: Authentication (0x000b)
> Frame Control Field: 0xb000
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
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
1110 1000 1110 .... = Sequence number: 3726
Frame check sequence: 0x93eaefc9 [unverified]
[FCS Status: Unverified]
```

16. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameter's fields of the 802.11 wireless LAN management frame.

Ans: The supported rates are given as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps in the ASSOCIATION REQUEST frame.
The ASSOCIATION RESPONSE also lists the same rates.

17. Consider the first PROBE REQUEST and the 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).

Ans: A PROBE REQUEST with the source 00:12:f0:1f:57:13, destination ff:ff:ff:ff:ff, and BSSID ff:ff:ff:ff:ff:ff is issued at t = 2.297613.
A PROBE RESPONSE with the source and destination of 00:16:b6:f7:1d:51 and a BSSID of 00:16:b6:f7:1d:51 is transmitted at t = 2.300697.
A host uses a PROBE REQUEST during active scanning to identify an Access Point. The access point responds to the host making the request by issuing a PROBE RESPONSE.