

Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

LAB 7

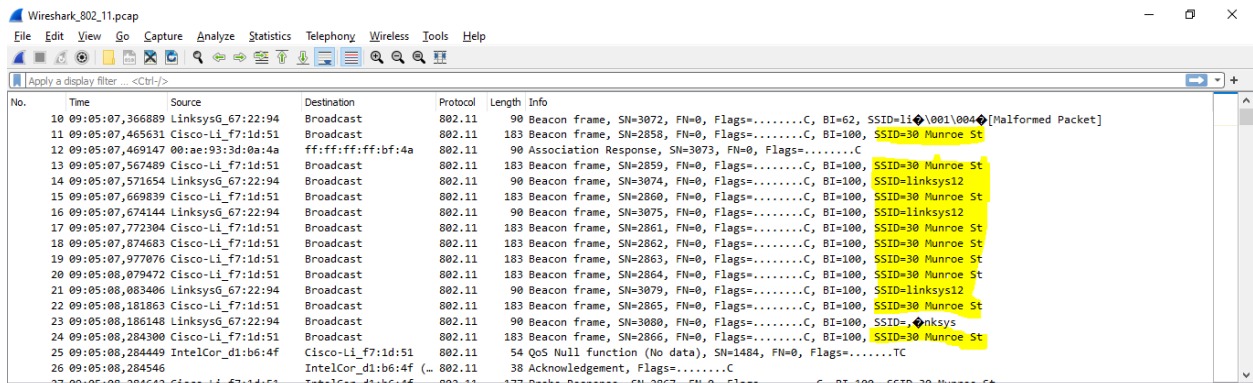
(using the file Wireshark_802_11.pcap)

2. Beacon Frames

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

ANSWER:

30 Munroe St
linsys_SES_24086



The screenshot shows a Wireshark packet capture of 802.11 beacon frames. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
10	09:05:07.366889	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=11001\0040 [Malformed Packet]
11	09:05:07.465631	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
12	09:05:07.469147	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C
13	09:05:07.567489	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
14	09:05:07.571654	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=linsys12
15	09:05:07.669839	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2860, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
16	09:05:07.674144	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=linsys12
17	09:05:07.772304	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
18	09:05:07.874683	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2862, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
19	09:05:07.977876	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
20	09:05:08.079472	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
21	09:05:08.083406	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=.....C, BI=100, SSID=linsys12
22	09:05:08.181863	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2865, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
23	09:05:08.186148	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID=linsys
24	09:05:08.284300	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
25	09:05:08.284449	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1484, FN=0, Flags=.....TC
26	09:05:08.284546	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C

Question 2: What are the intervals of time between the transmissions of the beacon frames the *linsys_ses_24086* access point? From the *30 Munroe St.* access point? (Hint: this interval of time is contained in the beacon frame itself).

ANSWER:

0.1024 s

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	09:05:07.072457	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2	09:05:07.134558	b6:78:8c:c1:a8:c0	(... 65:a8:d5:b2:c1:99 (... 802.11	1624	802.11 Block Ack Req, Flags=op.P...TC	
3	09:05:07.157931	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	09:05:07.260376	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	09:05:07.260557	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	09:05:07.260658	IntelCor_d1:b6:4f	(... 802.11	38	Acknowledgement, Flags=.....C	
7	09:05:07.261392	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	09:05:07.261491	IntelCor_d1:b6:4f	(... 802.11	38	Acknowledgement, Flags=.....C	
9	09:05:07.362741	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	09:05:07.366889	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=110010040 [Malformed Packet]
11	09:05:07.465631	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
12	09:05:07.469147	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C
13	09:05:07.567489	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
14	09:05:07.571654	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=linksys12
15	09:05:07.669839	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2860, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
16	09:05:07.674144	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12
17	09:05:07.772304	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> 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

> IEEE 802.11 Wireless Management

- Fixed parameters (12 bytes)
 - Timestamp: 174319001986
 - Beacon Interval: 0.102400 [Seconds]
 - Capabilities Information: 0x0001
- Tagged parameters (119 bytes)

0030 82 e1 38 96 28 00 00 00 64 00 01 06 00 0c 33 30 --8-(...d...30

0040 20 4d 75 64 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 0bUSI-

0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5eBCN

0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 4b -b2/*-2...\$H

0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 '1.....@.....

0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01P...

Beacon Interval (wlan.fixed.beacon), 2 byte(s) | Packets: 2364 - Displayed: 2364 (100.0%) | Profile: Default

Question 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).

ANSWER:

00:16:b6:f7:1d:51

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	09:05:07.072457	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2	09:05:07.134558	b6:78:8c:c1:a8:c0	(... 65:a8:d5:b2:c1:99 (... 802.11	1624	802.11 Block Ack Req, Flags=op.P...TC	
3	09:05:07.157931	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	09:05:07.260376	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	09:05:07.260557	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	09:05:07.260658	IntelCor_d1:b6:4f	(... 802.11	38	Acknowledgement, Flags=.....C	
7	09:05:07.261392	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	09:05:07.261491	IntelCor_d1:b6:4f	(... 802.11	38	Acknowledgement, Flags=.....C	
9	09:05:07.362741	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	09:05:07.366889	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=110010040 [Malformed Packet]
11	09:05:07.465631	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:C

Type/Subtype: Beacon frame (0x0008)

Frame Control Field: 0x0000

0000 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

Frame check sequence: 0x057e2608 [unverified]

[FCS Status: Unverified]

> IEEE 802.11 Wireless Management

0030 82 e1 38 96 28 00 00 00 64 00 01 06 00 0c 33 30 --8-(...d...30

0040 20 4d 75 64 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 0bUSI-

0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5eBCN

0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 4b -b2/*-2...\$H

0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 '1.....@.....

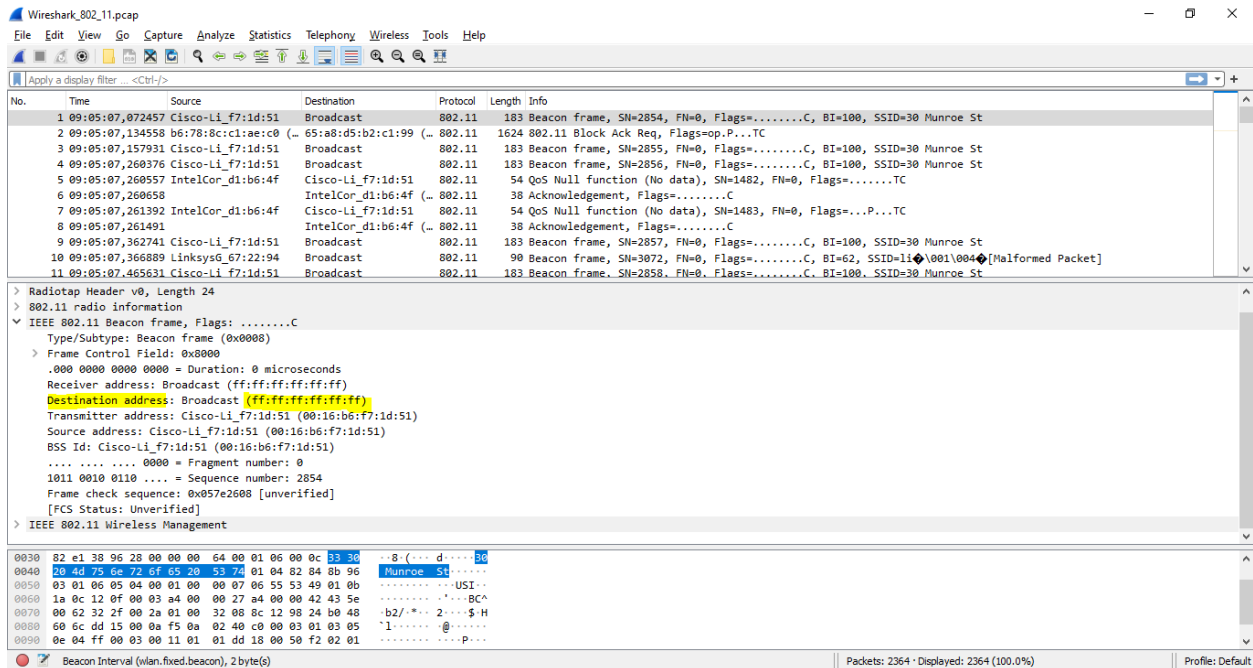
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01P...

Beacon Interval (wlan.fixed.beacon), 2 byte(s) | Packets: 2364 - Displayed: 2364 (100.0%) | Profile: Default

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

ANSWER:

ff:ff:ff:ff:ff:ff



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

ANSWER:

00:16:b6:f7:1d:51

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Question 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:

4 data rates: 1.0, 2.0, 5.5, 11 Mbps

8 additional “extended supported rates” : 6, 9, 12, 18, 24, 36, 48, 54 Mbps

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	09:05:07.072457	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2	09:05:07.134558	b6:78:8c:c1:a6:c0 (- 65:a8:d5:b2:c1:99 (-	802.11	1624	802.11 Block Ack Req, Flags=op.P...TC	
3	09:05:07.157931	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	09:05:07.260376	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	09:05:07.260557	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	09:05:07.260658	IntelCor_d1:b6:4f (-	802.11	38	Acknowledgement, Flags=.....C	
7	09:05:07.261392	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	09:05:07.261491	IntelCor_d1:b6:4f (-	802.11	38	Acknowledgement, Flags=.....C	
9	09:05:07.362741	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	09:05:07.366889	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=1100100400 [Malformed Packet]
11	09:05:07.465631	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

.... 0... .. = Automatic Power Save Delivery: Not Implemented

...0

..0

..0

0... .. = Delayed Block Ack: Not Implemented

0... .. = Immediate Block Ack: Not Implemented

> Tagged parameters (119 bytes)

> Tag: SSID parameter set: 30 Munroe St

> Tag: Supported Rates 1(0), 2(0), 5-5(0), 11(0), [Mbit/sec]

> Tag: DS Parameter set: Current Channel: 6

> Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap

> Tag: Country Information: Country Code US, Environment Indoor

> Tag: EDCA Parameter Set

> Tag: ERP Information

> Tag: Extended Supported Rates 6(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]

> Tag: Vendor Specific: Airogo Networks, Inc.

> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

0030 82 e1 38 96 28 00 00 00 64 00 01 06 00 0c 33 30 --8-(...d-...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 0bUSI--

0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5eBC-

0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 4b -b2/-* 2-...\$-H

0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 ^1-...@-...P--

0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01P--

Tagged parameters (wlan.tagged.all), 119 byte(s)

Packets: 2364 · Displayed: 2364 (100.0%)

Profile: Default

3. Data Transfer

Question 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.

ANSWER:

Those MAC addresses are BSSId, source address, destination.

The MAC address corresponds to:

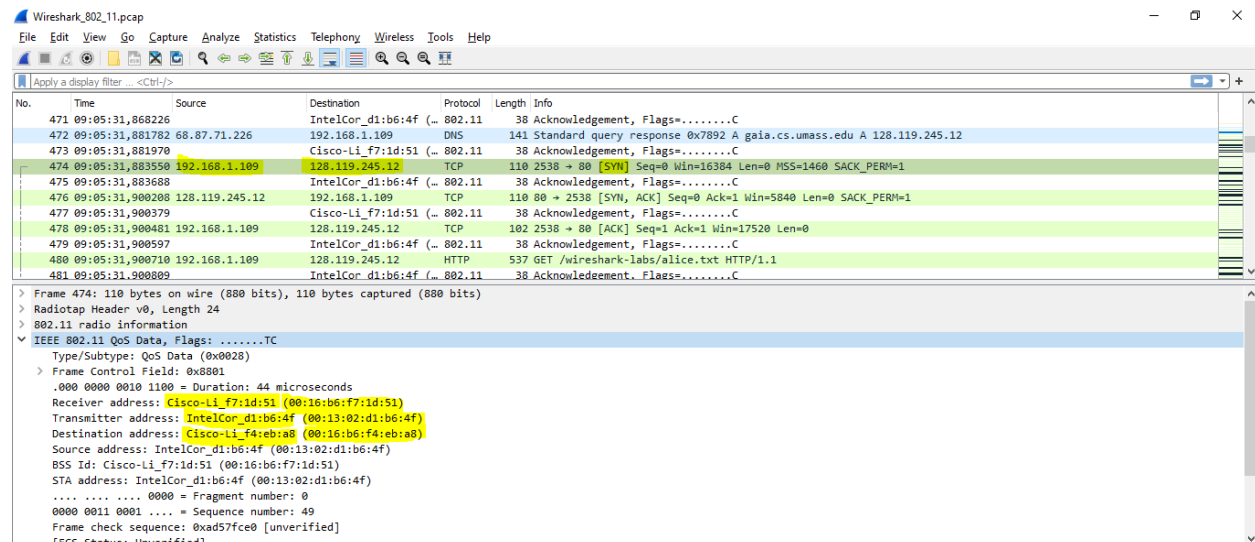
+ The wireless host: **00:13:02:d1:b6:4f**.

+ The 1st hop router: **00:16:b6:f4:eb:a8**.

+ The wireless host sending this TCP segment: **00:16:b6:f7:1d:51**.

The corresponding IP of the wireless host: **192.168.1.109**.

Destination IP: **128.199.245.12** (corresponds to the host)



Question 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)

ANSWER:

Three MAC address fields in the 802.11 frame:

+ BSS id: **00:16:b6:f7:1d:51**

+ Destination: **00:13:02:d1:b6:4f**

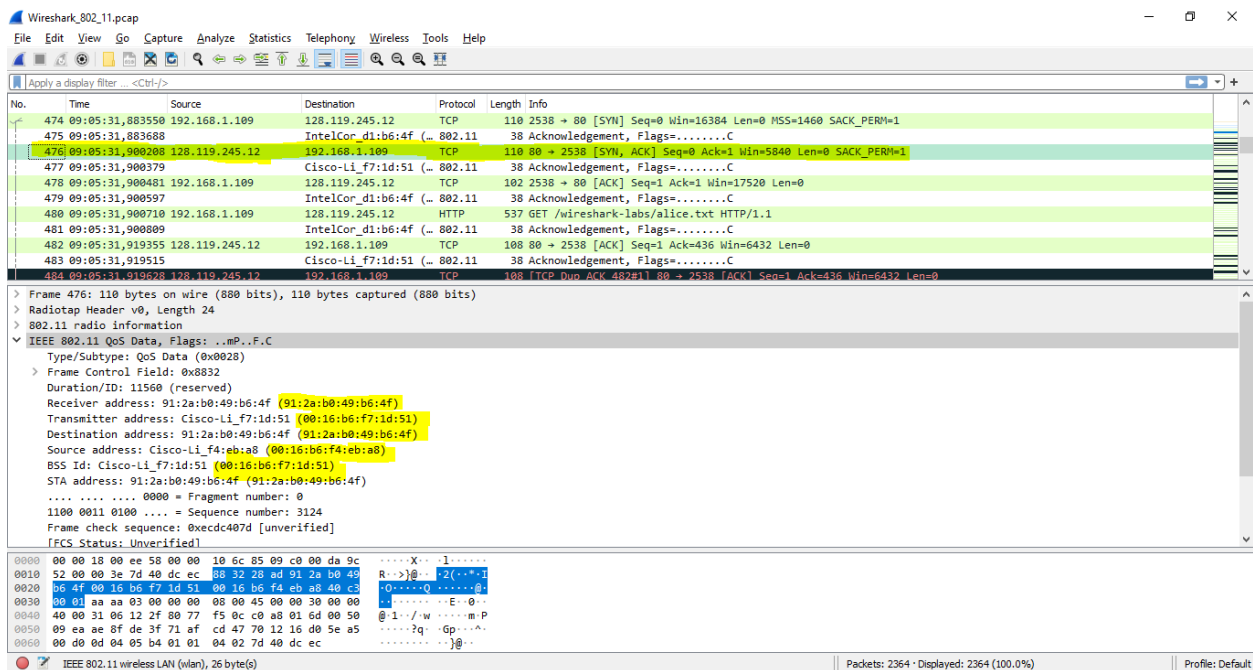
+ Source address: **00:16:b6:f4:eb:a8**

The MAC corresponds to

+ The host: 00:13:02:d1:b6:4f (destination)

+ The first hop is 00:16:b6:f4:eb:a8 (source)

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 (because the TCP SYNACK's IP address is **128:199:245:12** but the destination IP address is **192.168.1.109**)



3. Association/Disassociation

Question 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?

ANSWER:

1. A DHCP is sent to 192.168.1.1
2. The host sends a DEAUTHENTICATION frame after 0.02

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1731	49.4440243		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 0xae5a526
1734	49.583771		IntelCor_d1:b6:4f (-	802.11	38	Acknowledgement, Flags=.....C
1735	49.680617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.680770		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_SE5_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=.....C

Question 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 $t=49$?

ANSWER:

There are **17** AUTHENTICATION messages from the wireless host to the *linksys_ses_24086* AP

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

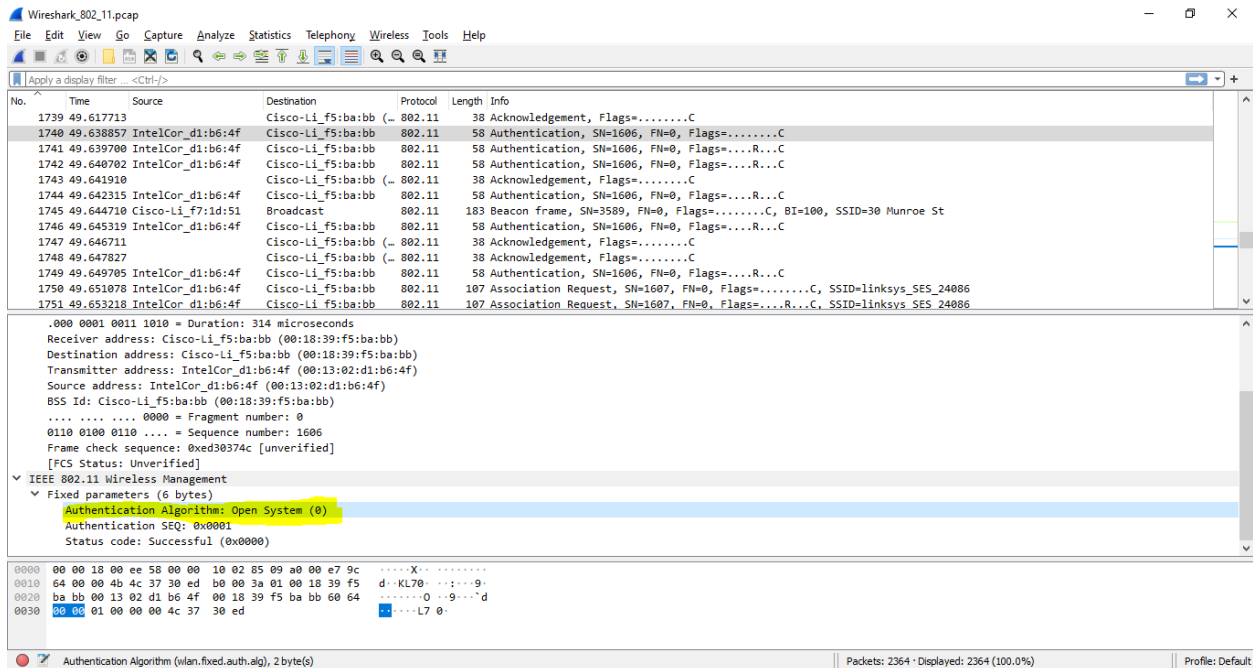
Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
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
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....R...C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....R...C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....R...C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R...C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C
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

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

ANSWER:

It's open



Question 12: Do you see a reply AUTHENTICATION from the *linksys_ses_24086* AP in the trace?

ANSWER:

No

Question 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 == 1 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.)

ANSWER:

There is an AUTHENTICATION frame from 00:13:02:d1:b6:4f to 00:16:b7:f7:1d:51 when **t = 63.168087**.

The AUTHENTICATION sent back at **t = 63.169071**

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
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	IntelCor_d1:b6:4f	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	63.169887	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	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	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
2160	63.169787	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	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	63.170088	IntelCor_d1:b6:4f	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	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C

> Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Authentication, 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: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)

 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]

0000 00 00 18 00 ee 58 00 00 10 6c 85 09 c0 00 e4 9c [.....]l.....

0010 59 00 00 48 e0 cb e8 47 00 00 2c 00 00 16 b6 f7 Y..H..G ..,.....

0020 1d 51 00 13 02 d1 b6 4f 00 16 b6 f7 1d 51 f0 66 Q.....Q..f.....

0030 00 00 01 00 00 00 e0 cb e8 47G.....

Destination Hardware Address (wlan.da), 6 byte(s)

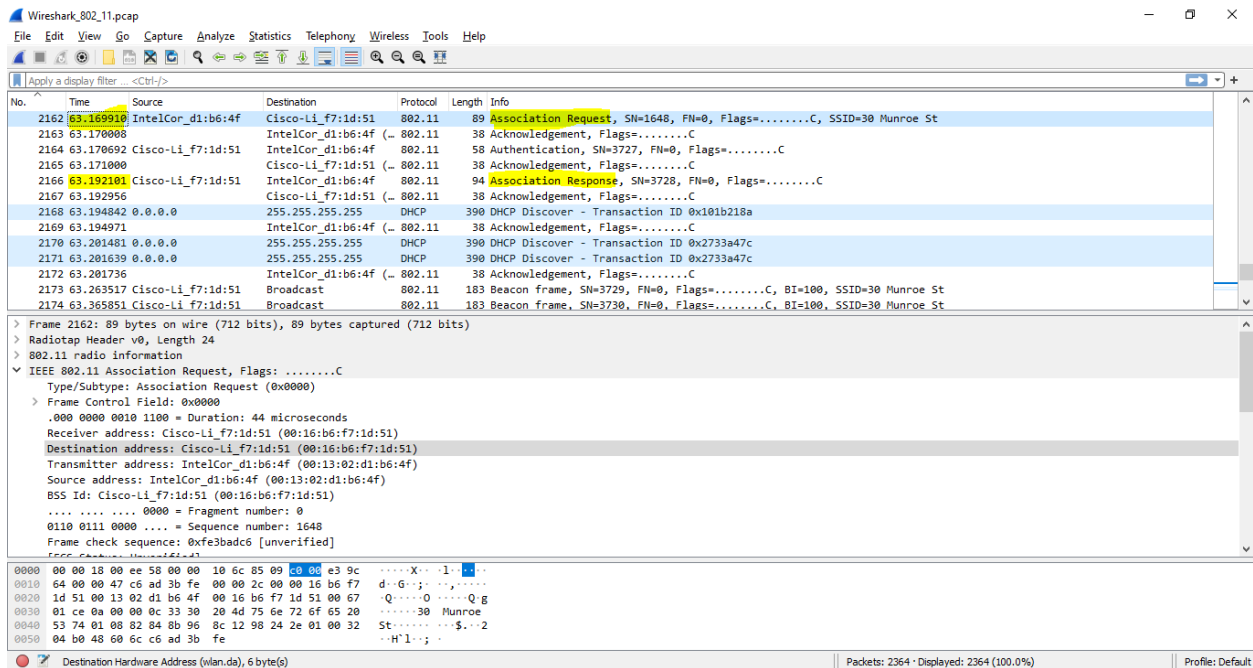
Packets: 2364 · Displayed: 2364 (100.0%)

Profile: Default

Question 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.)

ANSWER:

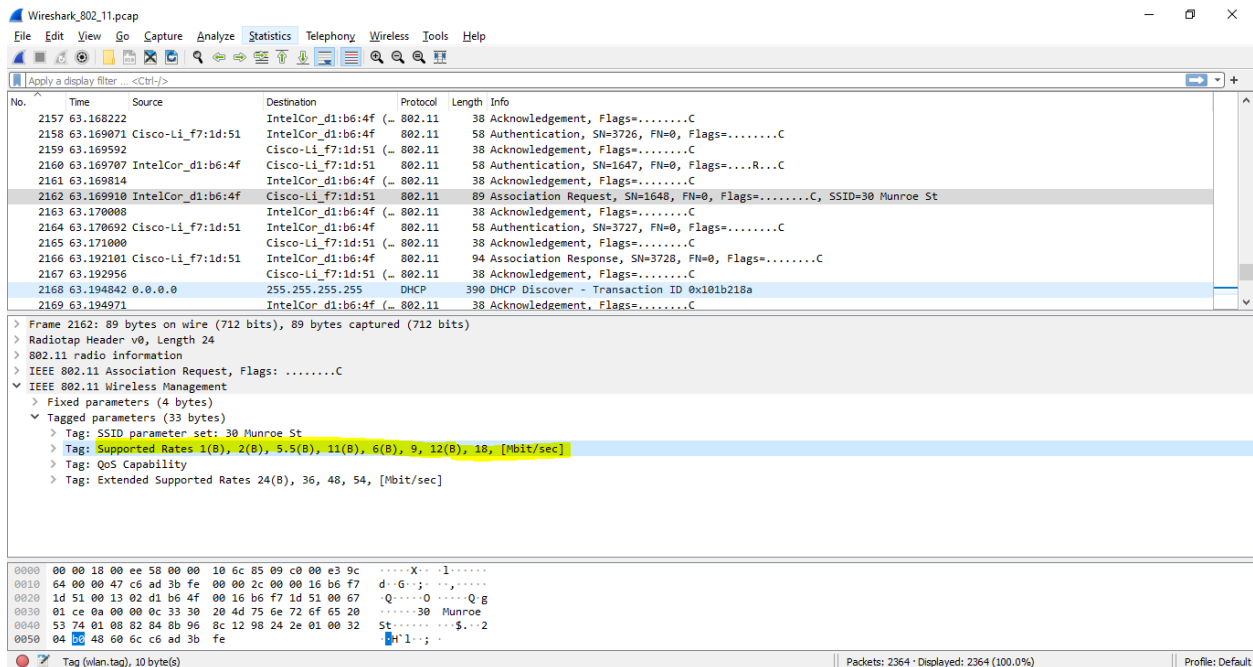
ASSOCIATE REQUEST from host to the *30 Munroe St* AP at **t = 63.169910**
Corresponding reply sent at **t = 63.192101**



Question 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 possible rates are 1, 2, 5.5, 11, 6, 9, 12, 18 Mbps



4. Other Frame types

Question 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).

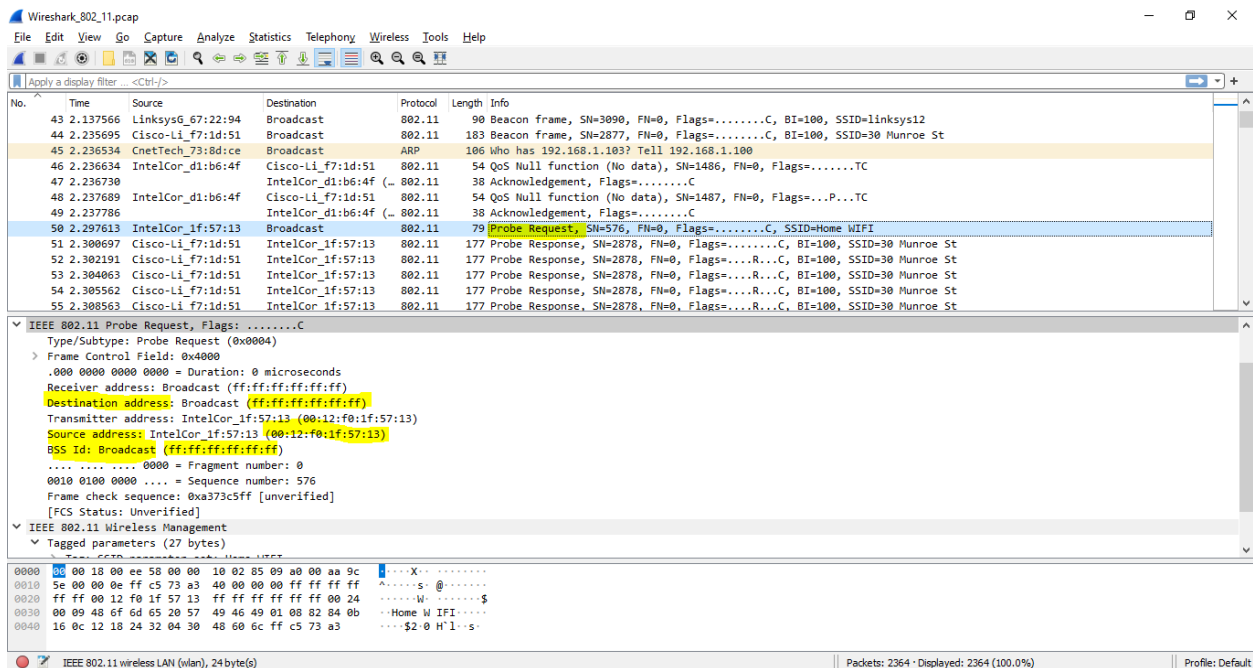
ANSWER:

Probe request:

+ Source: 00:12:f0:1f:57:13

+ Destination: ff:ff:ff:ff:ff:ff

+ BSSID: ff:ff:ff:ff:ff:ff



Probe response:

+ Source: 00:16:b6:f7:1d:51

+ Destination: 00:12:f0:1f:57:13

+ BSSID: 00:16:b6:f7:1d:51

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
46	2.236634	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1486, FN=0, Flags=.....TC
47	2.236730	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
48	2.237689	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1487, FN=0, Flags=...P...TC
49	2.237786	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
53	2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
54	2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
55	2.308563	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
56	2.310072	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
57	2.338148	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2879, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
58	2.440572	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2880, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

IEEE 802.11 Probe Response, Flags:C

Type/Subtype: Probe Response (0x0005)

Frame Control Field: 0x5000

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)

Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)

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 Ids: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

.... 0000 = Fragment number: 0

1011 0011 1110 = Sequence number: 2878

Frame check sequence: 0x6ed851bb [unverified]

[FCS Status: Unverified]

IEEE 802.11 Wireless Management

Fixed parameters (12 bytes)

0010 64 00 00 46 bb 51 d8 6e 50 00 3a 01 00 12 f0 1f d...F Q n P:.....

0020 57 13 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 e0 b3 M.....QQ.....

0030 d9 3f 5c 95 28 00 00 00 64 00 01 06 00 0c 33 30 ?\{... d...30

0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St.....

0050 03 01 06 07 06 55 53 01 0b 1a 0c 12 0f 00 03US.....

0060 a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f 00 2aB C^b2/*

IEEE 802.11 wireless LAN (vlan), 24 byte(s)

Packets: 2364 · Displayed: 2364 (100.0%)

Profile: Default

The probe request is a broadcast to scan for an access point from the host. The probe response is used to response the host from the access point