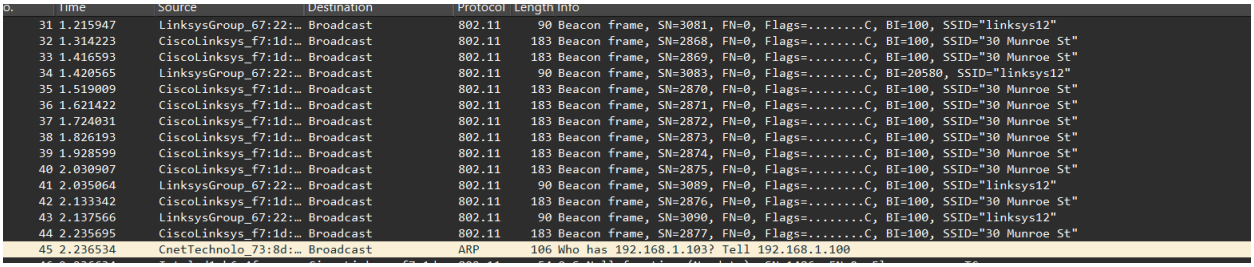
Họ và tên: Nguyễn Huỳnh Thái Bảo

MSSV: 2210238.

Lớp: L09

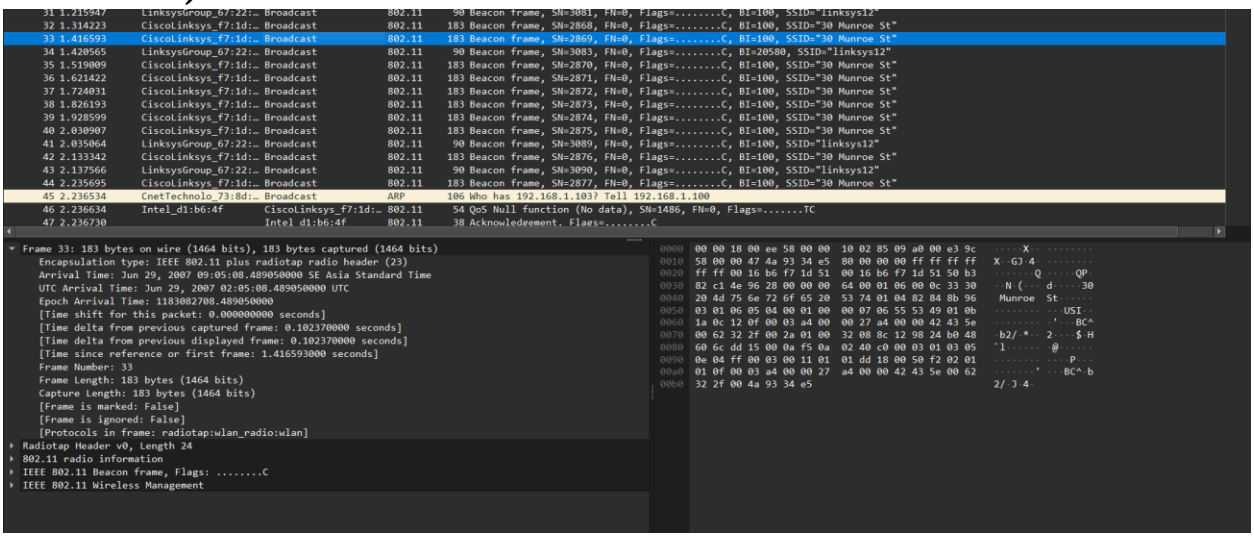
1. **What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?**



No.	Time	Source	Destination	Protocol	Length	Info
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"
33	1.416593	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2869, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
34	1.420565	LinksysGroup_67:22:…	Broadcast	802.11	90	Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, SSID="linksys12"
35	1.519009	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2870, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
36	1.621422	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2871, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
37	1.724031	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2872, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
38	1.826193	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2873, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
39	1.928599	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2874, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
40	2.030907	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2875, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
41	2.035064	LinksysGroup_67:22:…	Broadcast	802.11	90	Beacon frame, SN=3089, FN=0, Flags=........C, BI=100, SSID="linksys12"
42	2.133342	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2876, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
43	2.137566	LinksysGroup_67:22:…	Broadcast	802.11	90	Beacon frame, SN=3090, FN=0, Flags=........C, BI=100, SSID="linksys12"
44	2.235695	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2877, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
45	2.236534	CnetTechnolo_73:8d:…	Broadcast	ARP	106	Who has 192.168.1.103? Tell 192.168.1.100

An SSID is a one or two word identifiers of the access point. In this case, Cisco-Li's SSID is 30 Munroe St, and LinksysG_67:22:94's SSID is linksys12.

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).**



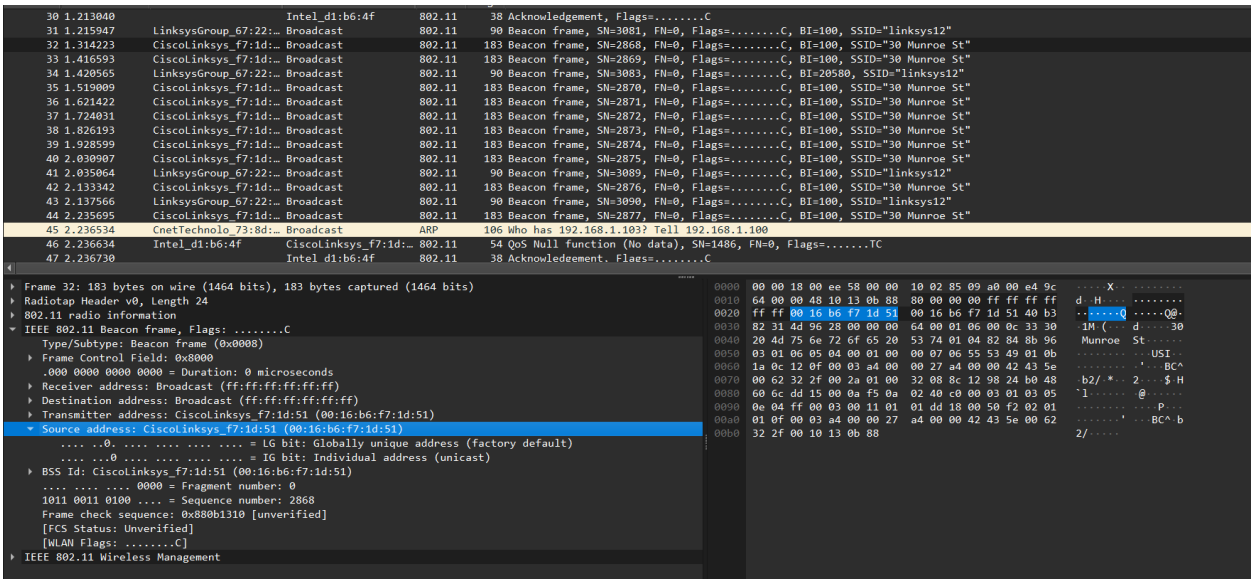
No.	Time	Source	Destination	Protocol	Length	Info
32	1.314223	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2868, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
33	1.416593	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2869, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
34	1.420565	LinksysGroup_67:22:…	Broadcast	802.11	90	Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, SSID="linksys12"
35	1.519009	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2870, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
36	1.621422	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2871, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
37	1.724031	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2872, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
38	1.826193	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2873, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
39	1.928599	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2874, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
40	2.030907	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2875, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
41	2.035064	LinksysGroup_67:22:…	Broadcast	802.11	90	Beacon frame, SN=3089, FN=0, Flags=........C, BI=100, SSID="linksys12"
42	2.133342	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2876, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
43	2.137566	LinksysGroup_67:22:…	Broadcast	802.11	90	Beacon frame, SN=3090, FN=0, Flags=........C, BI=100, SSID="linksys12"
44	2.235695	CiscoLinksys_f7:1d:…	Broadcast	802.11	183	Beacon frame, SN=2877, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
45	2.236534	CnetTechnolo_73:8d:…	Broadcast	ARP	106	Who has 192.168.1.103? Tell 192.168.1.100
46	2.236634	Intel_d1:b6:4f	CiscoLinksys_f7:1d:…	802.11	54	QoS Null function (No data), SN=1486, FN=0, Flags=.......TC
47	2.236730		Intel_d1:b6:4f	802.11	38	Acknowledgement, Flags=.......C

```
Frame 33: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 29, 2007 09:05:08.489050000 SE Asia Standard Time
    UTC Arrival Time: Jun 29, 2007 02:05:08.489050000 UTC
    Epoch Arrival Time: 1183082708.489050000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.102370000 seconds]
    [Time delta from previous displayed frame: 0.102370000 seconds]
    [Time since reference or first frame: 1.416593000 seconds]
    Frame Number: 33
    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 Management
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e3 9c   .....X..  ........
0010  58 00 00 47 4a 93 34 e5  80 00 00 00 ff ff ff ff   X..GJ.4.  ........
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 50 b3   .......Q  .....QP.
0030  82 c1 4e 96 28 00 00 00  64 00 01 06 00 0c 33 30   ..N.(...  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 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
0080  60 6c dd 15 00 0a f5 0a  02 40 c0 00 03 01 03 05   `l.....@  ........
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01   ........  ....P...
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   .......'  ...BC^.b
00b0  32 2f 00 4a 93 34 e5                              2/.J.4.
```

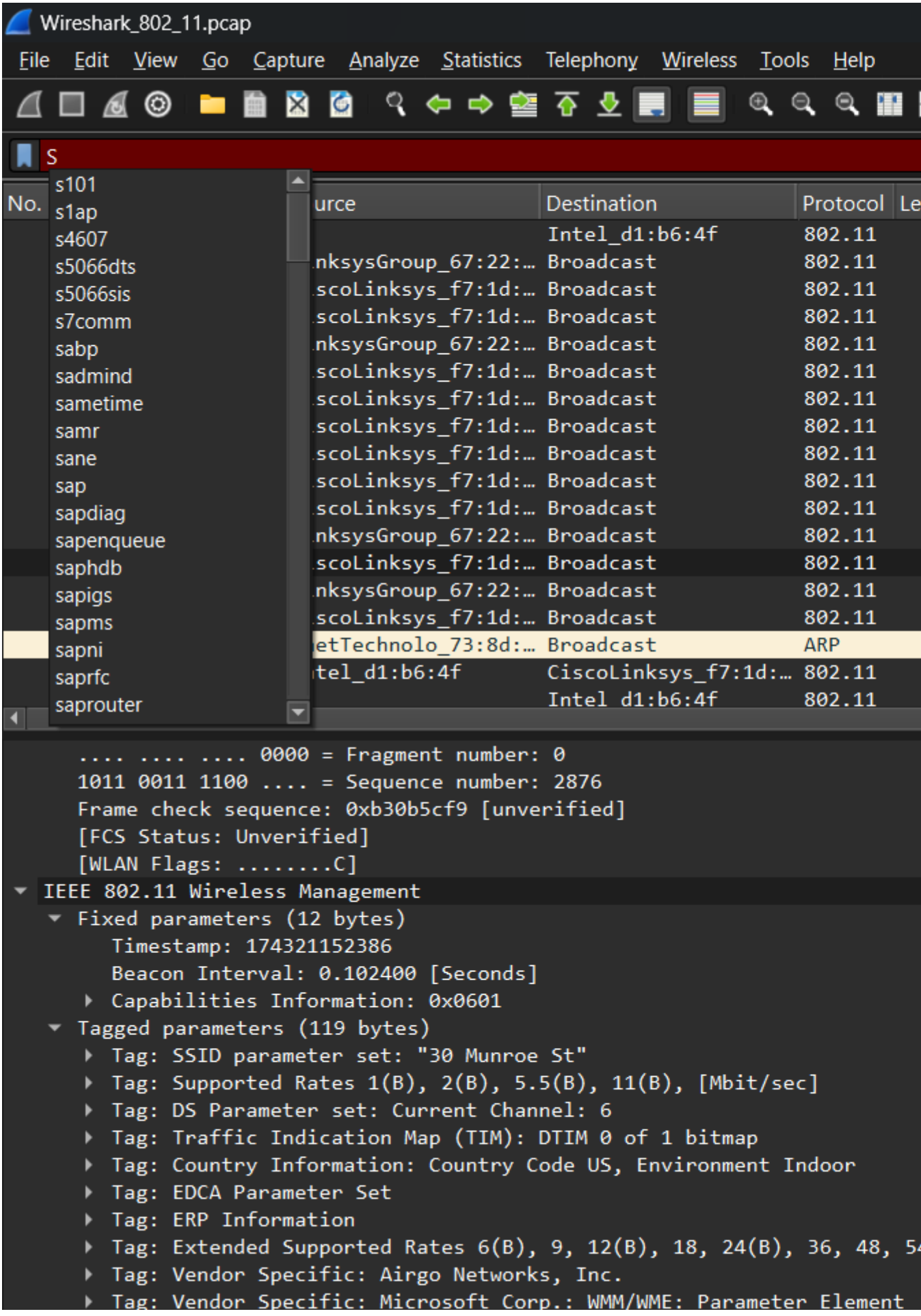
[Time delta from previous displayed frame: 0.102370000 seconds]

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).**



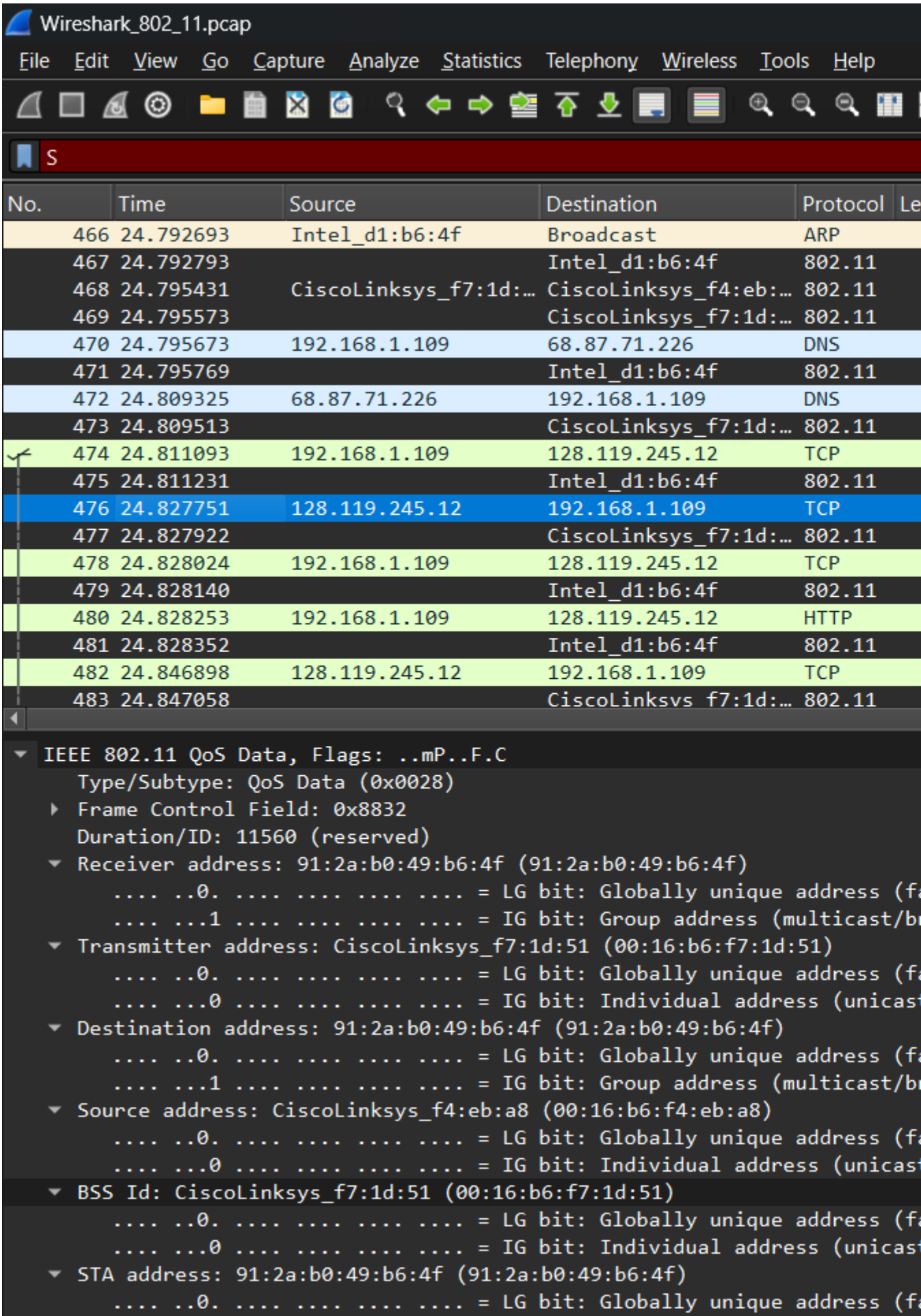
Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)

4. **What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??**
   Destination 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?**
   BSS Id: CiscoLinksys_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?**


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
S
s101
s1ap
s4607
s5066dts
s5066sis
s7comm
sabp
sadmind
sametime
samr
sane
sap
sapdiag
sapenqueue
saphdb
sapigs
sapms
sapni
saprfc
saprouter
No.
urce
Destination
Protocol
Intel_d1:b6:4f 802.11
nksysGroup_67:22:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
nksysGroup_67:22:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
nksysGroup_67:22:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
nksysGroup_67:22:… Broadcast 802.11
scoLinksys_f7:1d:… Broadcast 802.11
etTechnolo_73:8d:… Broadcast ARP
tel_d1:b6:4f CiscoLinksys_f7:1d:… 802.11
Intel_d1:b6:4f 802.11
.... 0000 = Fragment number: 0
1011 0011 1100 .... = Sequence number: 2876
Frame check sequence: 0xb30b5cf9 [unverified]
[FCS Status: Unverified]
[WLAN Flags: ....C]
IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Timestamp: 174321152386
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 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
Tag: Vendor Specific: Airgo Networks, Inc.
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

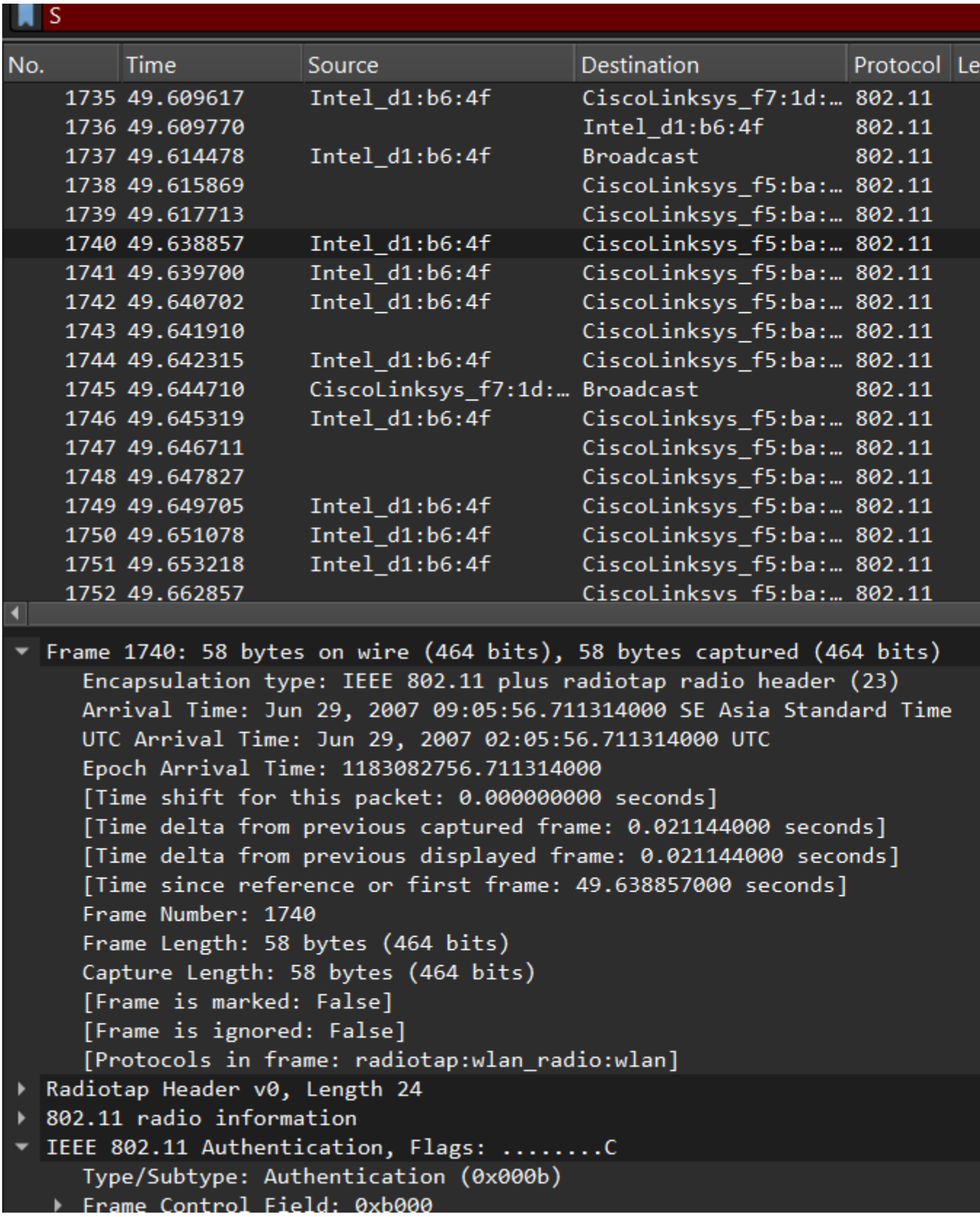
This data is found within the IEEE 802.11 wireless LAN management frame, within the Tagged parameters subfield. The four supported rates are 1(B), 2(B), 5.5(B) AND 11(B). The 8 Extended Unsupported Rates are 6(B), 9, 12(B), 18, 24(B), 36, 48 and 54. All these rates are measured in Mbit/sec.

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.**


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
S
No. Time Source Destination Protocol Le
466 24.792693 Intel_d1:b6:4f Broadcast ARP
467 24.792793 Intel_d1:b6:4f 802.11
468 24.795431 CiscoLinksys_f7:1d:… CiscoLinksys_f4:eb:… 802.11
469 24.795573 CiscoLinksys_f7:1d:… 802.11
470 24.795673 192.168.1.109 68.87.71.226 DNS
471 24.795769 Intel_d1:b6:4f 802.11
472 24.809325 68.87.71.226 192.168.1.109 DNS
473 24.809513 CiscoLinksys_f7:1d:… 802.11
474 24.811093 192.168.1.109 128.119.245.12 TCP
475 24.811231 Intel_d1:b6:4f 802.11
476 24.827751 128.119.245.12 192.168.1.109 TCP
477 24.827922 CiscoLinksys_f7:1d:… 802.11
478 24.828024 192.168.1.109 128.119.245.12 TCP
479 24.828140 Intel_d1:b6:4f 802.11
480 24.828253 192.168.1.109 128.119.245.12 HTTP
481 24.828352 Intel_d1:b6:4f 802.11
482 24.846898 128.119.245.12 192.168.1.109 TCP
483 24.847058 CiscoLinksys_f7:1d:… 802.11
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)
.... ..0. .... = LG bit: Globally unique address (f
....1 .... = IG bit: Group address (multicast/b
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.... ..0. .... = LG bit: Globally unique address (f
....0 .... = IG bit: Individual address (unicas
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
.... ..0. .... = LG bit: Globally unique address (f
....1 .... = IG bit: Group address (multicast/b
Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
.... ..0. .... = LG bit: Globally unique address (f
....0 .... = IG bit: Individual address (unicas
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.... ..0. .... = LG bit: Globally unique address (f
....0 .... = IG bit: Individual address (unicas
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
.... ..0. .... = LG bit: Globally unique address (f

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).**
   Three MAC address fields in the 802.11 frame are BSS id: 00:16:b6:f7:1d:5 1, Destination: 00:13:02:d1:b6:4f and source address: 00:16:b6:f4:eb:a8. Th e MAC corresponds to the host is 00:13:02:d1:b6:4f (destination). The MA C corresponds to the first hop is 00:16:b6:f4:eb:a8 (Source). The sender M AC 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 T CP SYNACK's IP address is 128:199:245:12 but the destination IP address is 192.168.1.109
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?**



1. A DHCP is sent to 192.168.1.1

2. The host sends a DEAUTHENTICATION frame after 0.02s

10. **Examine the trace file and look for AUTHENICATION 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? .**
    There are 17 AUTHENTICATION messages from the wireless host to the li nksys_ses_24086 AP.
11. **Does the host want the authentication to require a key or be open?**

To determine if a system is open or uses a key, one must look for the value on the Authentication Algorithm Number field, per Section 7.3.1.1. Composed of 2 octets, it is either 0 for open system, and 1 for shared key authentication. This is contained in the 1740th packet instance, a t = 49.638857, and further located in the IEEE 802.11 wireless LAN management frame. It indicates an Authentication Algorithm field of "Open System (0)", and Authentication SEQ of 0x0001, as well as a Status Code of Successful, or 0x0000. This is a shared key system.

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 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.)**
    AUTHENTICATION from Host to 30 Munroe (AP): t = 63.168087

    Reply AUTHENTICATION from AP to Host: t = 63.169071
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.)

Associate Request: t = 63.169910

Associate Reply: t = 63.192191

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.**
    Host transmission rates in Mbit/sec: 1(B), 2(B), 5.5(B), 11(B), 6(B), 9(B), 12(B), & 18(B). Extended rates are also offered at 24(B), 36, 48 and 54.
    AP transmission rates (30 Munroe or f7:1d:51) in Mbit/sec: 1(B), 2(B), 5.5(B), 11(B). Extended rates are also offered at 6(B), 9, 12(B), 18, 24(B), 36, 48 and 54.
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).**
    Probe Request: Sender = InterCor_d1:b6:4f, Receiver = Broadcast (ff:ff:ff:ff:ff:ff) & BSS Id = Broadcast (ff:ff:ff:ff:ff:ff)

    Probe Response: Sender = Cisco-Li_f7:1d:51, Receiver =InterCor_d1:b6:4f & BSS Id = Cisco-Li_f7:1d:51.

    Probe requests & responses are generated for active scanning. Unlike passive scanning, where an STA listens to each channel for a set duration, once a probe response is received and processed, authorization can be commenced as directly after ACK'ing a probe request.