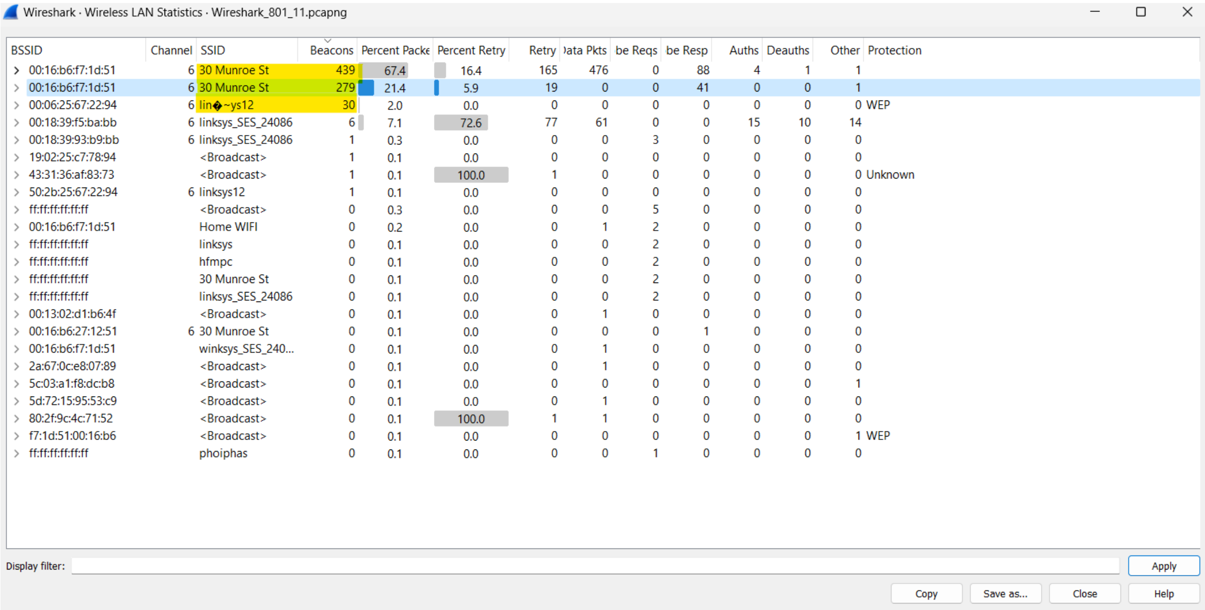
Lab 07_802.11 WiFi

I. Beacon Frames

1. **What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace? [Hint: look at the *Info* field. To display only beacon frames, neter wlan.fc.type_subtype == 8 into the Wireshark display filter].**

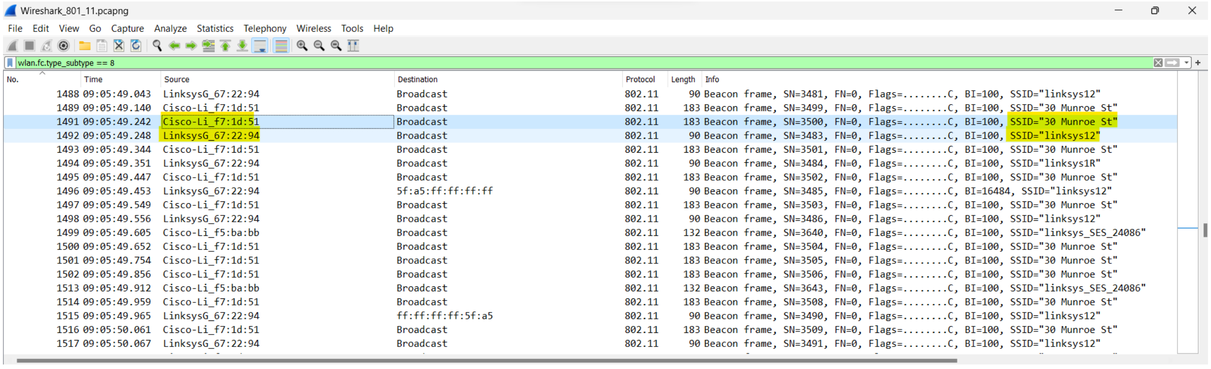


Wireshark · Wireless LAN Statistics · Wireshark_801_11.pcapng

BSSID	Channel	SSID	Beacons	Percent Packe	Percent Retry	Retry	)ata Pkts	be Reqs	be Resp	Auths	Deauths	Other	Protection
00:16:b6:f7:1d:51	6	30 Munroe St	439	67.4	16.4	165	476	0	88	4	1	1	
00:16:b6:f7:1d:51	6	30 Munroe St	279	21.4	5.9	19	0	0	41	0	0	1	
00:06:25:67:22:94	6	lin�~ys12	30	2.0	0.0	0	0	0	0	0	0	0	WEP
00:18:39:f5:ba:bb	6	linksys_SES_24086	6	7.1	72.6	77	61	0	0	15	10	14	
00:18:39:93:b9:bb	6	linksys_SES_24086	1	0.3	0.0	0	0	3	0	0	0	0	
19:02:25:c7:78:94		<Broadcast>	1	0.1	0.0	0	0	0	0	0	0	0	
43:31:36:af:83:73		<Broadcast>	1	0.1	100.0	1	0	0	0	0	0	0	Unknown
50:2b:25:67:22:94	6	linksys12	1	0.1	0.0	0	0	0	0	0	0	0	
ff:ff:ff:ff:ff:ff		<Broadcast>	0	0.3	0.0	0	0	5	0	0	0	0	
00:16:b6:f7:1d:51		Home WIFI	0	0.2	0.0	0	1	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		linksys	0	0.1	0.0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		hfmpc	0	0.1	0.0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		30 Munroe St	0	0.1	0.0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		linksys_SES_24086	0	0.1	0.0	0	0	2	0	0	0	0	
00:13:02:d1:b6:4f		<Broadcast>	0	0.1	0.0	0	1	0	0	0	0	0	
00:16:b6:27:12:51	6	30 Munroe St	0	0.1	0.0	0	0	0	1	0	0	0	
00:16:b6:f7:1d:51		winksys_SES_240...	0	0.1	0.0	0	1	0	0	0	0	0	
2a:67:0c:e8:07:89		<Broadcast>	0	0.1	0.0	0	1	0	0	0	0	0	
5c:03:a1:f8:dc:b8		<Broadcast>	0	0.1	0.0	0	0	0	0	0	0	1	
5d:72:15:95:53:c9		<Broadcast>	0	0.1	0.0	0	1	0	0	0	0	0	
80:2f:9c:4c:71:52		<Broadcast>	0	0.1	100.0	1	1	0	0	0	0	0	
f7:1d:51:00:16:b6		<Broadcast>	0	0.1	0.0	0	0	0	0	0	0	1	WEP
ff:ff:ff:ff:ff:ff		phoiphas	0	0.1	0.0	0	0	1	0	0	0	0	

Display filter:

SSIDs are “30 Munroe St” and “linksys12”



Wireshark_801_11.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type_subtype == 8

No.	Time	Source	Destination	Protocol	Length	Info
1488	09:05:49.043	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3481, FN=0, Flags=........C, BI=100, SSID="linksys12"
1489	09:05:49.140	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3499, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1491	09:05:49.242	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1492	09:05:49.248	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID="linksys12"
1493	09:05:49.344	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3501, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1494	09:05:49.351	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID="linksys1R"
1495	09:05:49.447	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3502, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1496	09:05:49.453	LinksysG_67:22:94	5f:a5:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3485, FN=0, Flags=........C, BI=16484, SSID="linksys12"
1497	09:05:49.549	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3503, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1498	09:05:49.556	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3486, FN=0, Flags=........C, BI=100, SSID="linksys12"
1499	09:05:49.605	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
1500	09:05:49.652	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3504, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1501	09:05:49.754	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3505, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1502	09:05:49.856	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3506, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1513	09:05:49.912	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3643, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
1514	09:05:49.959	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3508, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1515	09:05:49.965	LinksysG_67:22:94	ff:ff:ff:ff:5f:a5	802.11	90	Beacon frame, SN=3490, FN=0, Flags=........C, BI=100, SSID="linksys12"
1516	09:05:50.061	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3509, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1517	09:05:50.067	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3491, FN=0, Flags=........C, BI=100, SSID="linksys12"

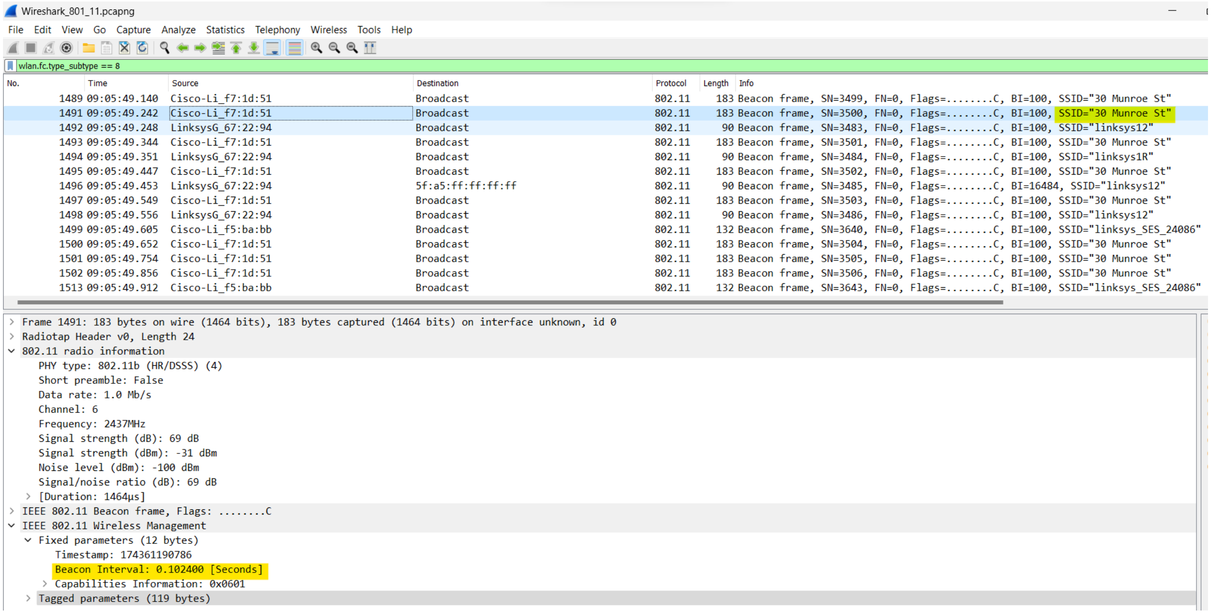
2. **What 802.11 channel is being used by both of these access points [Hint: you’ll need to dig into the radio information in an 802.11 beacon frame]**

Channel: 6

3. **What is the interval of time between the transmissions of beacon frames from this access point (AP)? (Hint: this interval of time is contained in a field within the beacon frame itself).**

It is 0.1024 seconds for both the linksys12 access point and the 30 Munroe St. access point.

- The 30 Munroe St. access point:



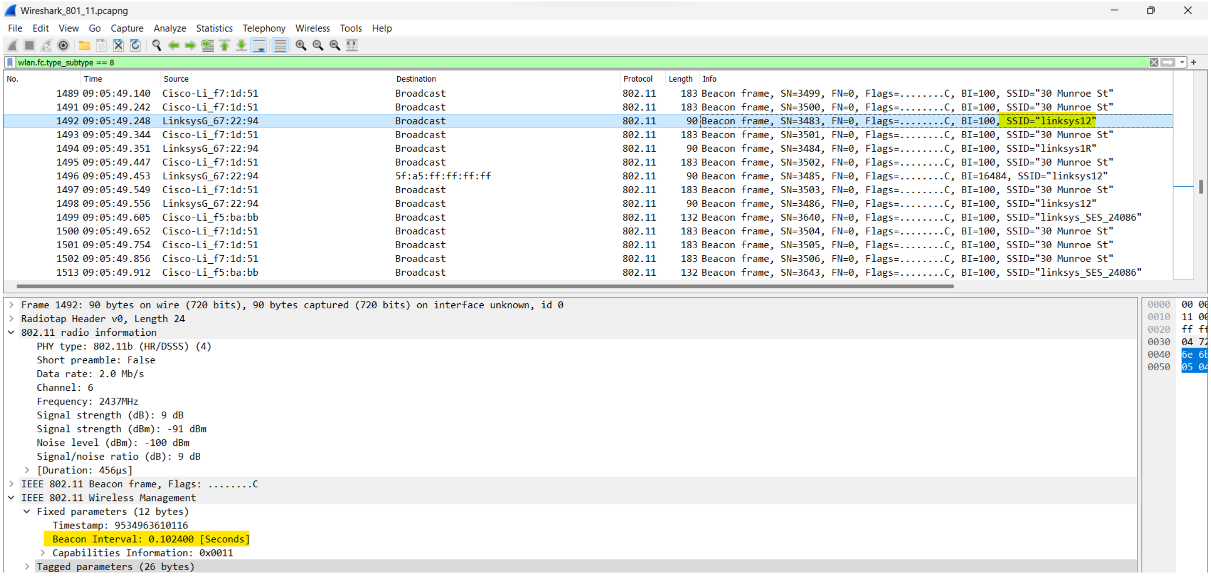
Wireshark_801_11.pcapng

wlan.fc.type_subtype == 8

```
No.   Time          Source             Destination         Protocol Length Info
 1489 09:05:49.140  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3499, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1491 09:05:49.242  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1492 09:05:49.248  LinksysG_67:22:94  Broadcast           802.11    90 Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID="linksys12"
 1493 09:05:49.344  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3501, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1494 09:05:49.351  LinksysG_67:22:94  Broadcast           802.11    90 Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID="linksys1R"
 1495 09:05:49.447  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3502, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1496 09:05:49.453  LinksysG_67:22:94  5f:a5:ff:ff:ff:ff   802.11    90 Beacon frame, SN=3485, FN=0, Flags=........C, BI=16484, SSID="linksys12"
 1497 09:05:49.549  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3503, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1498 09:05:49.556  LinksysG_67:22:94  Broadcast           802.11    90 Beacon frame, SN=3486, FN=0, Flags=........C, BI=100, SSID="linksys12"
 1499 09:05:49.605  Cisco-Li_f5:ba:bb  Broadcast           802.11   132 Beacon frame, SN=3640, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
 1500 09:05:49.652  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3504, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1501 09:05:49.754  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3505, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1502 09:05:49.856  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3506, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1513 09:05:49.912  Cisco-Li_f5:ba:bb  Broadcast           802.11   132 Beacon frame, SN=3643, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
```

```
> Frame 1491: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
v 802.11 radio information
    PHY type: 802.11b (HR/DSSS) (4)
    Short preamble: False
    Data rate: 1.0 Mb/s
    Channel: 6
    Frequency: 2437MHz
    Signal strength (dB): 69 dB
    Signal strength (dBm): -31 dBm
    Noise level (dBm): -100 dBm
    Signal/noise ratio (dB): 69 dB
  > [Duration: 1464µs]
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
        Timestamp: 174361190786
        Beacon Interval: 0.102400 [Seconds]
      > Capabilities Information: 0x0601
  > Tagged parameters (119 bytes)
```

- The linksys12 access point:



Wireshark_801_11.pcapng

wlan.fc.type_subtype == 8

```
No.   Time          Source             Destination         Protocol Length Info
 1489 09:05:49.140  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3499, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1491 09:05:49.242  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1492 09:05:49.248  LinksysG_67:22:94  Broadcast           802.11    90 Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID="linksys12"
 1493 09:05:49.344  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3501, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1494 09:05:49.351  LinksysG_67:22:94  Broadcast           802.11    90 Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID="linksys1R"
 1495 09:05:49.447  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3502, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1496 09:05:49.453  LinksysG_67:22:94  5f:a5:ff:ff:ff:ff   802.11    90 Beacon frame, SN=3485, FN=0, Flags=........C, BI=16484, SSID="linksys12"
 1497 09:05:49.549  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3503, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1498 09:05:49.556  LinksysG_67:22:94  Broadcast           802.11    90 Beacon frame, SN=3486, FN=0, Flags=........C, BI=100, SSID="linksys12"
 1499 09:05:49.605  Cisco-Li_f5:ba:bb  Broadcast           802.11   132 Beacon frame, SN=3640, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
 1500 09:05:49.652  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3504, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1501 09:05:49.754  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3505, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1502 09:05:49.856  Cisco-Li_f7:1d:51  Broadcast           802.11   183 Beacon frame, SN=3506, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 1513 09:05:49.912  Cisco-Li_f5:ba:bb  Broadcast           802.11   132 Beacon frame, SN=3643, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
```

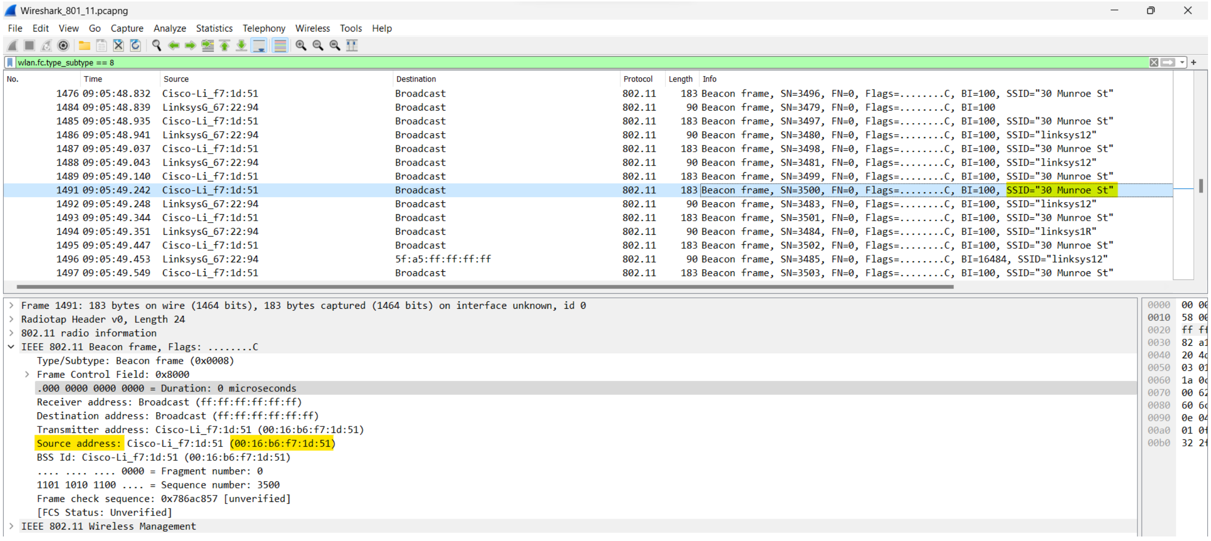
```
> Frame 1492: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
v 802.11 radio information
    PHY type: 802.11b (HR/DSSS) (4)
    Short preamble: False
    Data rate: 2.0 Mb/s
    Channel: 6
    Frequency: 2437MHz
    Signal strength (dB): 9 dB
    Signal strength (dBm): -91 dBm
    Noise level (dBm): -100 dBm
    Signal/noise ratio (dB): 9 dB
  > [Duration: 456µs]
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
        Timestamp: 9534963610116
        Beacon Interval: 0.102400 [Seconds]
      > Capabilities Information: 0x0011
  > Tagged parameters (26 bytes)
```

```
0000  00 00
0010  11 00
0020  ff ff
0030  04 72
0040  6e 6b
0050  05 04
```

4. **What (in hexadecimal notation) is the source MAC address on the beacon frame from this access point? 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**

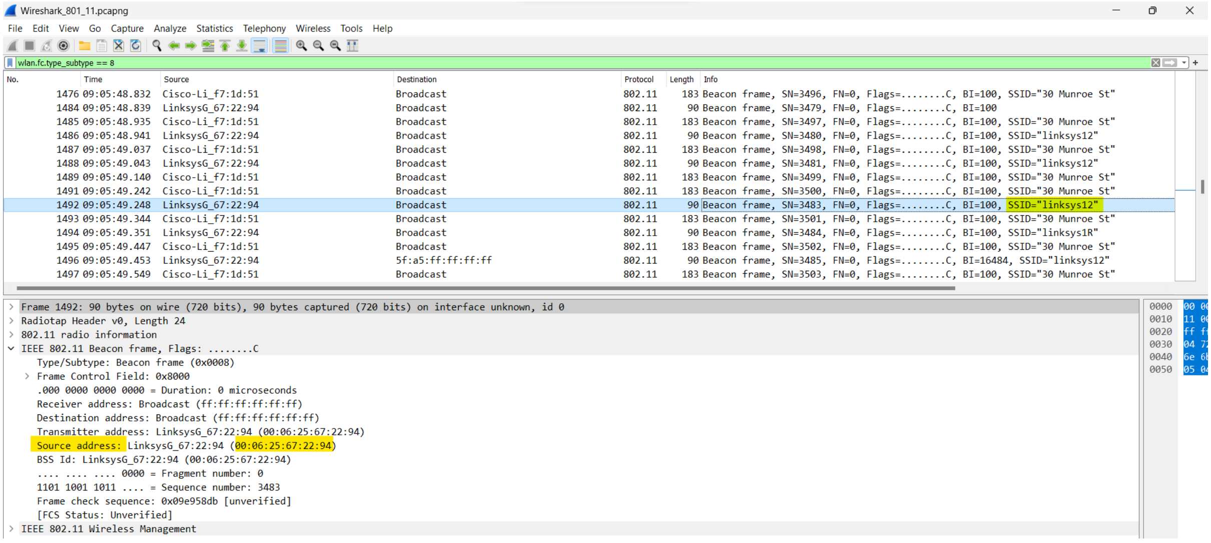
discussion of the 802.11 frame structure, see section 9.2.3-9.2.4.1in the IEEE 802.11 standards document, excerpted here.

The source MAC address on the beacon frame from 30 Munroe St is 00:16:b6:f7:1d:51


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type_subtype == 8

No.    Time          Source             Destination         Protocol  Length Info
  1476 09:05:48.832  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3496, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1484 09:05:48.839  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3479, FN=0, Flags=........C, BI=100
  1485 09:05:48.935  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3497, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1486 09:05:48.941  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3480, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1487 09:05:49.037  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3498, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1488 09:05:49.043  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3481, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1489 09:05:49.140  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3499, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1491 09:05:49.242  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1492 09:05:49.248  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1493 09:05:49.344  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3501, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1494 09:05:49.351  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID="linksys1R"
  1495 09:05:49.447  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3502, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1496 09:05:49.453  LinksysG_67:22:94  5f:a5:ff:ff:ff:ff   802.11     90 Beacon frame, SN=3485, FN=0, Flags=........C, BI=16484, SSID="linksys12"
  1497 09:05:49.549  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3503, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"

> Frame 1491: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 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
    1101 1010 1100 .... = Sequence number: 3500
    Frame check sequence: 0x786ac857 [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 Wireless Management

0000  00
0010  58
0020  ff
0030  82
0040  20
0050  03
0060  1a
0070  00
0080  60
0090  0e
00a0  01
00b0  32
```

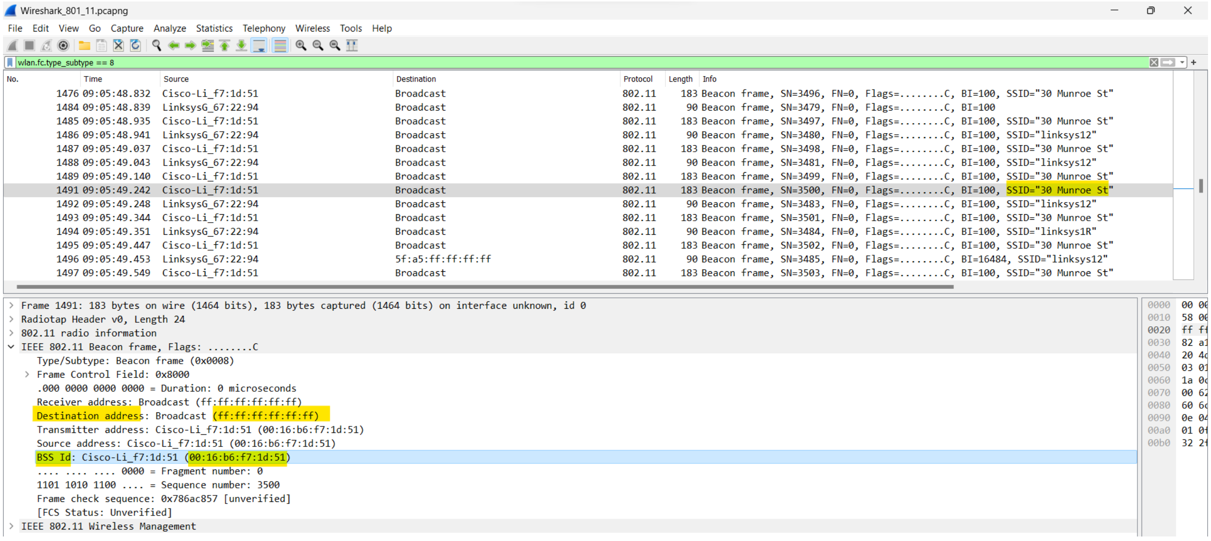
The source MAC address on the beacon frame from linksys12 is 00:06:25:67:22:94


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type_subtype == 8

No.    Time          Source             Destination         Protocol  Length Info
  1476 09:05:48.832  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3496, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1484 09:05:48.839  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3479, FN=0, Flags=........C, BI=100
  1485 09:05:48.935  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3497, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1486 09:05:48.941  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3480, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1487 09:05:49.037  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3498, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1488 09:05:49.043  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3481, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1489 09:05:49.140  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3499, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1491 09:05:49.242  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1492 09:05:49.248  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1493 09:05:49.344  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3501, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1494 09:05:49.351  LinksysG_67:22:94  Broadcast           802.11     90 Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID="linksys1R"
  1495 09:05:49.447  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3502, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1496 09:05:49.453  LinksysG_67:22:94  5f:a5:ff:ff:ff:ff   802.11     90 Beacon frame, SN=3485, FN=0, Flags=........C, BI=16484, SSID="linksys12"
  1497 09:05:49.549  Cisco-Li_f7:1d:51  Broadcast           802.11    183 Beacon frame, SN=3503, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"

> Frame 1492: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 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: LinksysG_67:22:94 (00:06:25:67:22:94)
    Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
    BSS Id: LinksysG_67:22:94 (00:06:25:67:22:94)
    .... .... .... 0000 = Fragment number: 0
    1101 1001 1011 .... = Sequence number: 3483
    Frame check sequence: 0x09e958db [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 Wireless Management

0000  00
0010  11
0020  ff
0030  04
0040  6e
0050  05
```

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

The destination MAC address on the beacon frame from *30 Munroe St* is ff:ff:ff:ff:ff:ff



wlan.fc.type_subtype == 8

```
No.    Time            Source              Destination          Protocol  Length Info
  1476 09:05:48.832   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3496, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1484 09:05:48.839   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3479, FN=0, Flags=........C, BI=100
  1485 09:05:48.935   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3497, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1486 09:05:48.941   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3480, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1487 09:05:49.037   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3498, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1488 09:05:49.043   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3481, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1489 09:05:49.140   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3499, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1491 09:05:49.242   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1492 09:05:49.248   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1493 09:05:49.344   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3501, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1494 09:05:49.351   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID="linksys1R"
  1495 09:05:49.447   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3502, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1496 09:05:49.453   LinksysG_67:22:94   5f:a5:ff:ff:ff:ff    802.11     90 Beacon frame, SN=3485, FN=0, Flags=........C, BI=16484, SSID="linksys12"
  1497 09:05:49.549   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3503, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
```

```
> Frame 1491: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 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
    1101 1010 1100 .... = Sequence number: 3500
    Frame check sequence: 0x786ac857 [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
```

```
0000  00
0010  58
0020  ff
0030  82
0040  20
0050  03
0060  1a
0070  00
0080  60
0090  0e
00a0  01
00b0  32
```

6. **What (in hexadecimal notation) is the MAC BSS ID on the beacon frame from *30 Munroe St*?**

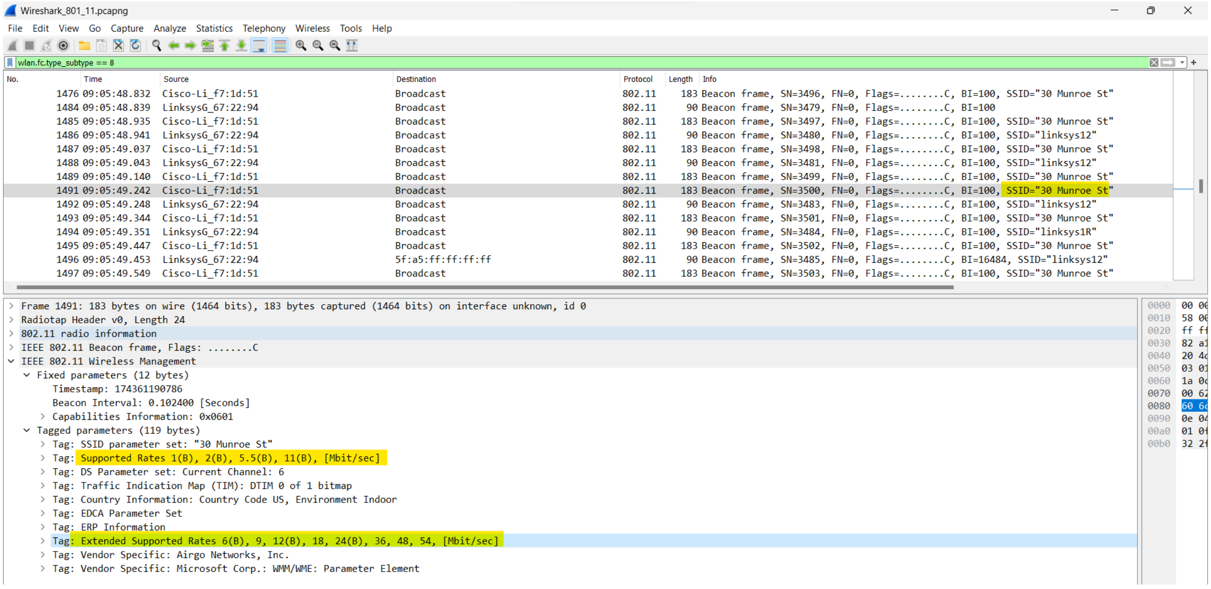
   The MAC BSS ID on the beacon frame from *30 Munroe St* is 00:16:b6:f7:1d:51

   This is the same as the source address because this is a beacon frame.

7. **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? [Note: the traces were taken on a rather old AP].**

   Four supported data rates: 1, 2, 5.5, 11 (Mbit/sec)

   Eight extended supported rates: 6, 9, 12, 18, 24, 36, 48, 54 (Mbit/sec)



wlan.fc.type_subtype == 8

```
No.    Time            Source              Destination          Protocol  Length Info
  1476 09:05:48.832   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3496, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1484 09:05:48.839   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3479, FN=0, Flags=........C, BI=100
  1485 09:05:48.935   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3497, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1486 09:05:48.941   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3480, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1487 09:05:49.037   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3498, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1488 09:05:49.043   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3481, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1489 09:05:49.140   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3499, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1491 09:05:49.242   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1492 09:05:49.248   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID="linksys12"
  1493 09:05:49.344   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3501, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1494 09:05:49.351   LinksysG_67:22:94   Broadcast            802.11     90 Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID="linksys1R"
  1495 09:05:49.447   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3502, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  1496 09:05:49.453   LinksysG_67:22:94   5f:a5:ff:ff:ff:ff    802.11     90 Beacon frame, SN=3485, FN=0, Flags=........C, BI=16484, SSID="linksys12"
  1497 09:05:49.549   Cisco-Li_f7:1d:51   Broadcast            802.11    183 Beacon frame, SN=3503, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
```

```
> Frame 1491: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
> 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: 174361190786
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  v 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, [Mbit/sec]
    > Tag: Vendor Specific: Airgo Networks, Inc.
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

```
0000  00
0010  58
0020  ff
0030  82
0040  20
0050  03
0060  1a
0070  00
0080  60
0090  0e
00a0  01
00b0  32
```

II. Data Transfer

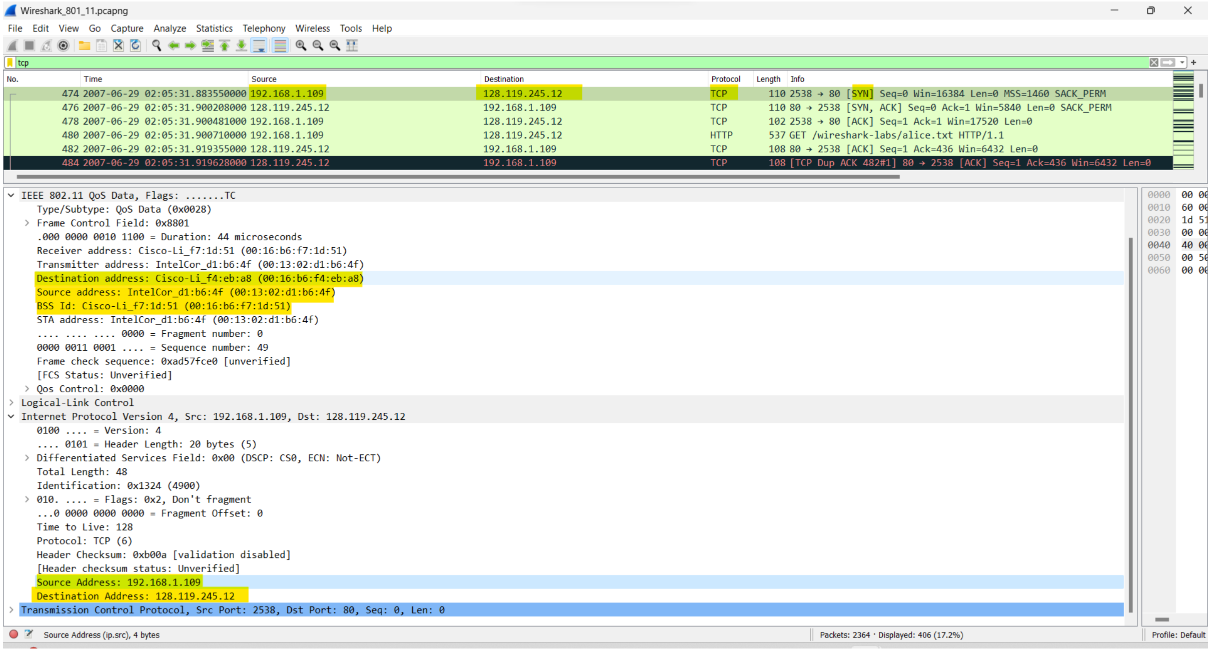
8. **Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt) at t=24.8110. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address 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 for the TCP syn segment?**
    - Three MAC address fields in the 802.11 frame are

Destination: 00:16:b6:f4:eb:a8

Source address: 00:13:02:d1:b6:4f

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

- The MAC address corresponds to the **wireless host** is: 00:13:02:d1:b6:4f **(Source)**
- The MAC address corresponds to the **access point** is: 00:16:b6:f7:1d:51 **(BSS Id)**
- The MAC address corresponds to the **first-hop router** is: 00:16:b6:f4:eb:a8
- **(Destination).**
- The IP address of the wireless host sending this TCP segment is: Source Address: 192.168.1.109
- The destination IP address for the TCP syn segment is: 128.119.245.12



Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time                          Source          Destination      Protocol Length Info
  474 2007-06-29 02:05:31.883550000 192.168.1.109   128.119.245.12   TCP      110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
  476 2007-06-29 02:05:31.900208000 128.119.245.12  192.168.1.109    TCP      110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
  478 2007-06-29 02:05:31.900481000 192.168.1.109   128.119.245.12   TCP      102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
  480 2007-06-29 02:05:31.900710000 192.168.1.109   128.119.245.12   HTTP     537 GET /wireshark-labs/alice.txt HTTP/1.1
  482 2007-06-29 02:05:31.919355000 128.119.245.12  192.168.1.109    TCP      108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  484 2007-06-29 02:05:31.919628000 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
```

```
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    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)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    0000 0011 0001 .... = Sequence number: 49
    Frame check sequence: 0xad57fce0 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
> Logical-Link Control
v Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x1324 (4900)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xb00a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.109
    Destination Address: 128.119.245.12
> Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 0
0010  60 0
0020  1d 5
0030  00 0
0040  40 0
0050  00 5
0060  00 0
```

```
Source Address (ip.src), 4 bytes    Packets: 2364 · Displayed: 406 (17.2%)    Profile: Default
```

9. **Does the destination IP address of this TCP SYN correspond to the host, access point, first-hop router, or the destination web server?**

This corresponds to the server gaia.cs.umass.edu (*The IP address of gaia.cs.umass.edu is 128.119.245.12*). It is important to understand that the **destination MAC address of the frame** containing the SYN, is **different from** the **destination IP address of the IP packet** contained within this frame

10. **Find the 802.11 frame containing the SYNACK segment for this TCP session received at t=24.8277. 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).**

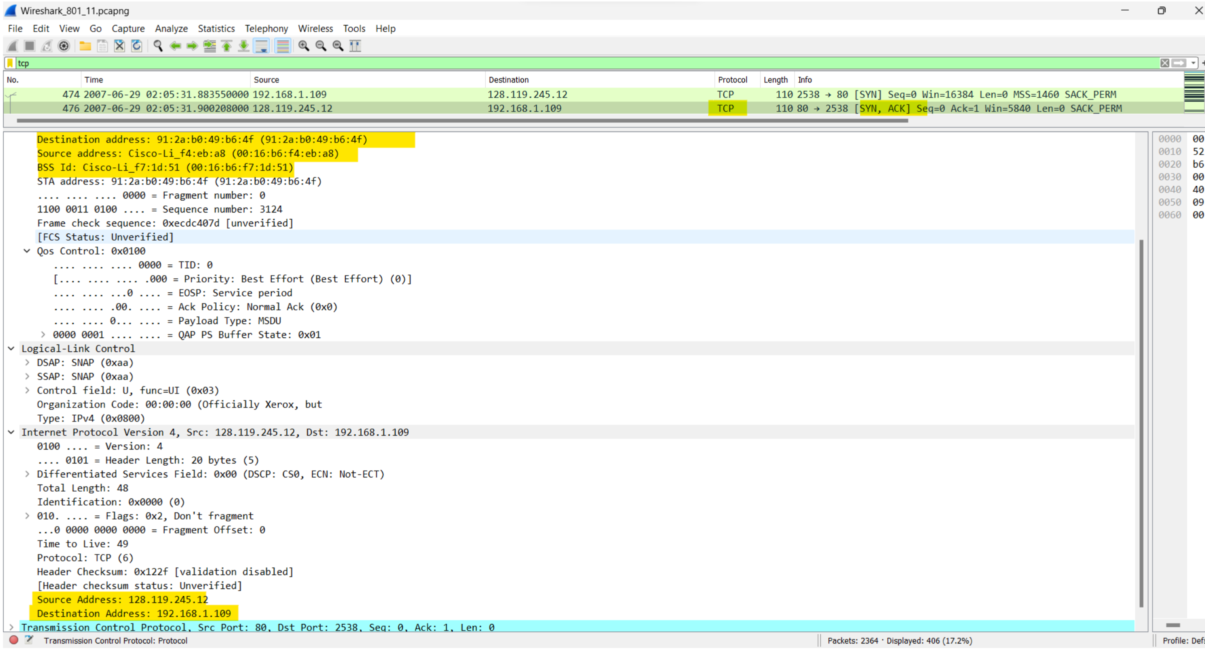
- Three MAC address fields in the 802.11 frame are

Destination: 91:2a:b0:49:b6:4f

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

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

- The **MAC address in this frame corresponds to the host is:** 91:2a:b0:49:b6:4f (Destination).
- The **MAC address in this frame corresponds to the access point is:** 00:16:b6:f7:1d:51 (BSS Id)**.**
- The **MAC address in this frame corresponds to the first-hop router is:** 00:16:b6:f4:eb:a8 (Source)
- This is different from the MAC address of the host used in the frame that sends the TCP SYN. The host wireless interface is behaving as if it has two interface addresses.



Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.     Time                           Source           Destination      Protocol  Length  Info
    474 2007-06-29 02:05:31.883550000 192.168.1.109    128.119.245.12   TCP       110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
    476 2007-06-29 02:05:31.900208000 128.119.245.12   192.168.1.109    TCP       110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
```

```
    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]
  ˅ Qos Control: 0x0100
      .... .... .... 0000 = TID: 0
      [.... .... .... .000 = Priority: Best Effort (Best Effort) (0)]
      .... .... ...0 .... = EOSP: Service period
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... .... 0... .... = Payload Type: MSDU
    › 0000 0001 .... .... = QAP PS Buffer State: 0x01
˅ Logical-Link Control
  › DSAP: SNAP (0xaa)
  › SSAP: SNAP (0xaa)
  › Control field: U, func=UI (0x03)
    Organization Code: 00:00:00 (Officially Xerox, but
    Type: IPv4 (0x0800)
˅ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x0000 (0)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 49
    Protocol: TCP (6)
    Header Checksum: 0x122f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.1.109
› Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 0, Ack: 1, Len: 0
```

```
0000  00
0010  52
0020  b6
0030  00
0040  40
0050  09
0060  00
```

```
Transmission Control Protocol: Protocol        Packets: 2364 · Displayed: 406 (17.2%)        Profile: Def
```

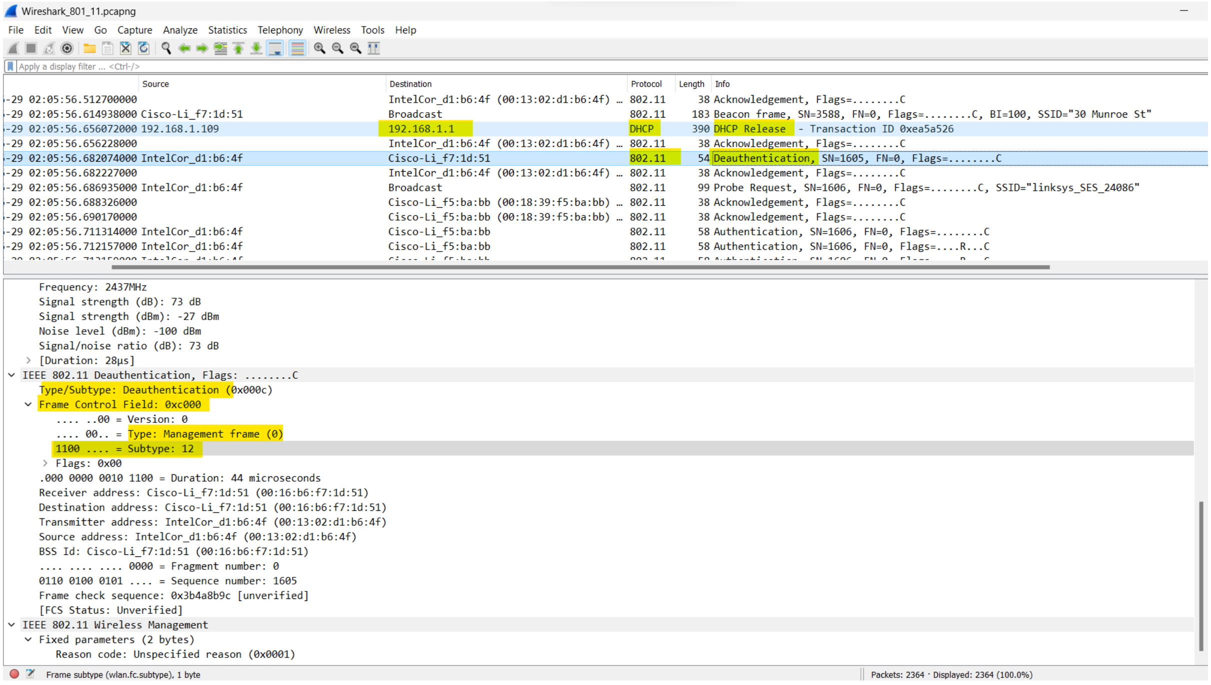
III. Disassociation/Authentication/Association

11. **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).**

    - Two actions taken by the host:

    + The host sends the **DHCP release** to return the IP Address to the DHCP server (IP address is192.168.1.1) (packet number 1733)

    + The host sends the **Deauthentication frame** to end the association with 30 Munroe St (packet number 1735)


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
                             Source                 Destination                          Protocol  Length Info
-29 02:05:56.512700000                              IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) … 802.11    38 Acknowledgement, Flags=........C
-29 02:05:56.614938000 Cisco-Li_f7:1d:51            Broadcast                               802.11   183 Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
-29 02:05:56.656072000 192.168.1.109                192.168.1.1                             DHCP     390 DHCP Release  - Transaction ID 0xea5a526
-29 02:05:56.656228000                              IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) … 802.11    38 Acknowledgement, Flags=........C
-29 02:05:56.682074000 IntelCor_d1:b6:4f            Cisco-Li_f7:1d:51                       802.11    54 Deauthentication, SN=1605, FN=0, Flags=........C
-29 02:05:56.682227000                              IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) … 802.11    38 Acknowledgement, Flags=........C
-29 02:05:56.686935000 IntelCor_d1:b6:4f            Broadcast                               802.11    99 Probe Request, SN=1606, FN=0, Flags=........C, SSID="linksys_SES_24086"
-29 02:05:56.688326000                              Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb) … 802.11    38 Acknowledgement, Flags=........C
-29 02:05:56.690170000                              Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb) … 802.11    38 Acknowledgement, Flags=........C
-29 02:05:56.711314000 IntelCor_d1:b6:4f            Cisco-Li_f5:ba:bb                       802.11    58 Authentication, SN=1606, FN=0, Flags=........C
-29 02:05:56.712157000 IntelCor_d1:b6:4f            Cisco-Li_f5:ba:bb                       802.11    58 Authentication, SN=1606, FN=0, Flags=....R...C
```

```
    Frequency: 2437MHz
    Signal strength (dB): 73 dB
    Signal strength (dBm): -27 dBm
    Noise level (dBm): -100 dBm
    Signal/noise ratio (dB): 73 dB
  > [Duration: 28µs]
v IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  v Frame Control Field: 0xc000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1100 .... = Subtype: 12
    > Flags: 0x00
    .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 0100 0101 .... = Sequence number: 1605
    Frame check sequence: 0x3b4a8b9c [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (2 bytes)
      Reason code: Unspecified reason (0x0001)
```

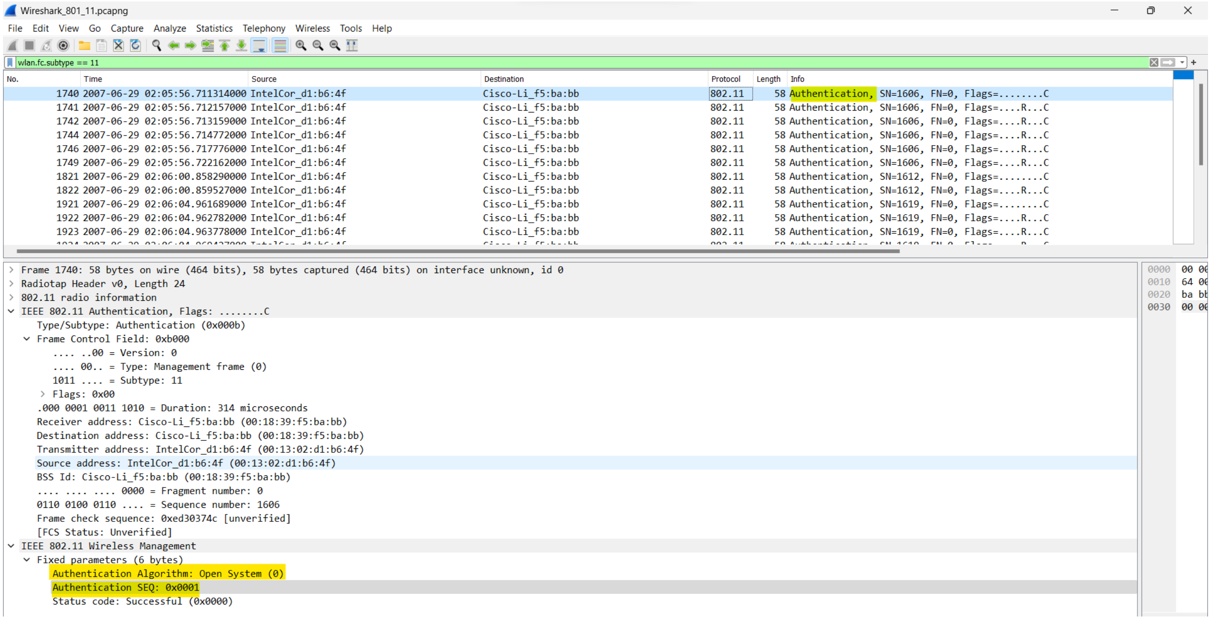
```
Frame subtype (wlan.fc.subtype), 1 byte                    Packets: 2364 · Displayed: 2364 (100.0%)
```

12. **Let's look first at AUTHENTICATION frames. At *t = 63.1680,* our host tries to associate with the *30 Munroe St* AP. Use the Wireshark display filter `wlan.fc.subtype == 11` to show AUTHENICATION frames sent from the host to and AP and vice versa. What form of authentication is the host requesting?**

    The host is requesting that the association be open (by specifying Authentication Algorithm: Open System).

13. **What is the `Authentication SEQ` value (authentication sequence number) of this authentication frame from host to AP?**

    Authentication SEQ: 0x0001



Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

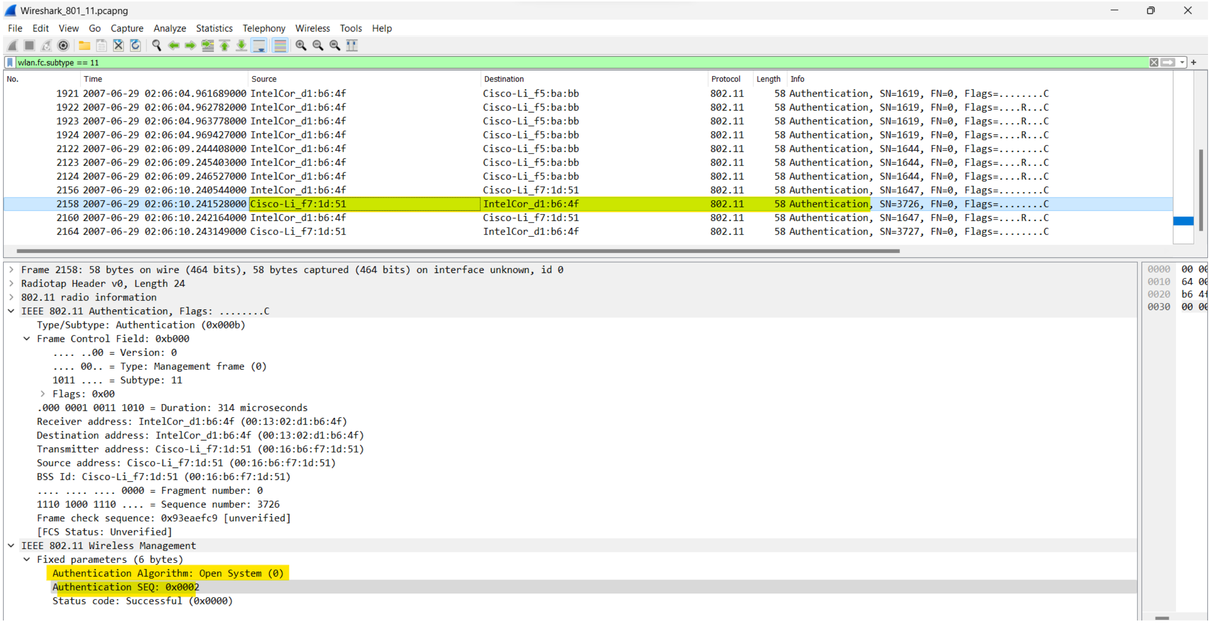
```
wlan.fc.subtype == 11

No.   Time                          Source                 Destination            Protocol  Length  Info
 1740 2007-06-29 02:05:56.711314000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1606, FN=0, Flags=........C
 1741 2007-06-29 02:05:56.712157000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1606, FN=0, Flags=....R...C
 1742 2007-06-29 02:05:56.713159000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1606, FN=0, Flags=....R...C
 1744 2007-06-29 02:05:56.714772000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1606, FN=0, Flags=....R...C
 1746 2007-06-29 02:05:56.717776000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1606, FN=0, Flags=....R...C
 1749 2007-06-29 02:05:56.722162000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1606, FN=0, Flags=....R...C
 1821 2007-06-29 02:06:00.858290000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1612, FN=0, Flags=........C
 1822 2007-06-29 02:06:00.859527000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1612, FN=0, Flags=....R...C
 1921 2007-06-29 02:06:04.961689000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1619, FN=0, Flags=........C
 1922 2007-06-29 02:06:04.962782000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1619, FN=0, Flags=....R...C
 1923 2007-06-29 02:06:04.963778000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1619, FN=0, Flags=....R...C
```

```
> Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  v Frame Control Field: 0xb000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1011 .... = Subtype: 11
    > Flags: 0x00
    .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
    0110 0100 0110 .... = Sequence number: 1606
    Frame check sequence: 0xed30374c [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)
```

```
0000  00 00
0010  64 00
0020  ba bb
0030  00 00
```

14. The AP response to the authentication request is received at *t = 63.1690.* Has the AP accepted the form of authentication requested by the host?

Yes



Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.subtype == 11

No.   Time                          Source                 Destination            Protocol  Length  Info
 1921 2007-06-29 02:06:04.961689000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1619, FN=0, Flags=........C
 1922 2007-06-29 02:06:04.962782000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1619, FN=0, Flags=....R...C
 1923 2007-06-29 02:06:04.963778000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1619, FN=0, Flags=....R...C
 1924 2007-06-29 02:06:04.969427000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1619, FN=0, Flags=....R...C
 2122 2007-06-29 02:06:09.244408000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1644, FN=0, Flags=........C
 2123 2007-06-29 02:06:09.245403000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1644, FN=0, Flags=....R...C
 2124 2007-06-29 02:06:09.246527000 IntelCor_d1:b6:4f      Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1644, FN=0, Flags=....R...C
 2156 2007-06-29 02:06:10.240544000 IntelCor_d1:b6:4f      Cisco-Li_f7:1d:51      802.11        58 Authentication, SN=1647, FN=0, Flags=........C
 2158 2007-06-29 02:06:10.241528000 Cisco-Li_f7:1d:51      IntelCor_d1:b6:4f      802.11        58 Authentication, SN=3726, FN=0, Flags=........C
 2160 2007-06-29 02:06:10.242164000 IntelCor_d1:b6:4f      Cisco-Li_f7:1d:51      802.11        58 Authentication, SN=1647, FN=0, Flags=....R...C
 2164 2007-06-29 02:06:10.243149000 Cisco-Li_f7:1d:51      IntelCor_d1:b6:4f      802.11        58 Authentication, SN=3727, FN=0, Flags=........C
```

```
> Frame 2158: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  v Frame Control Field: 0xb000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1011 .... = Subtype: 11
    > Flags: 0x00
    .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]
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
```

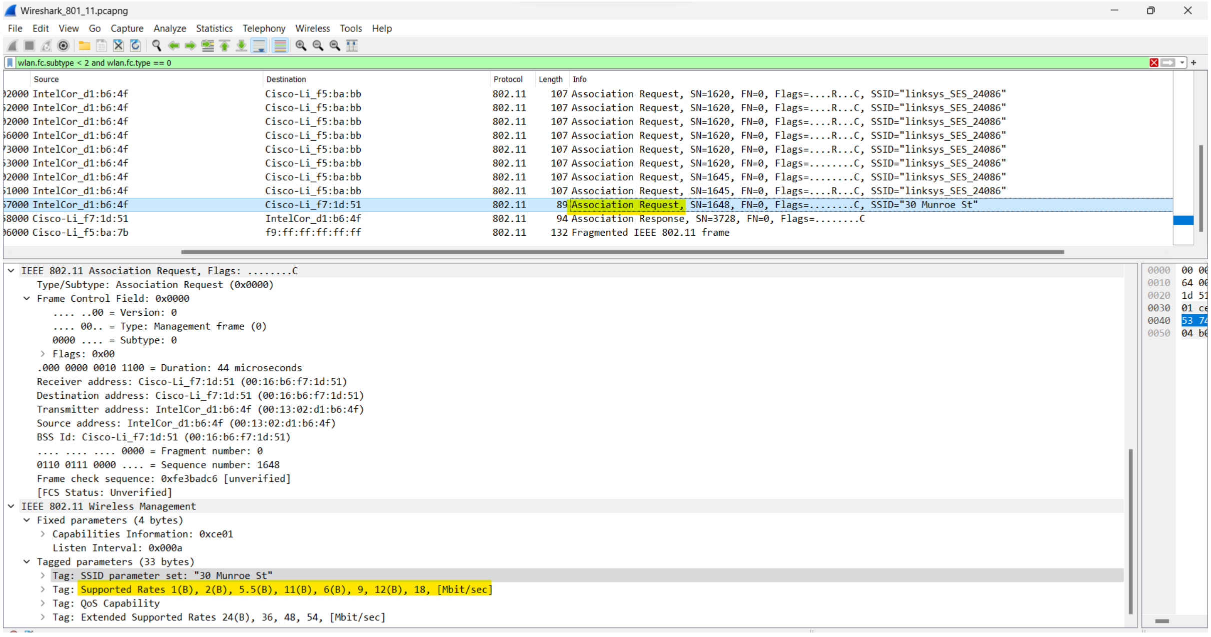
```
0000  00 00
0010  64 00
0020  b6 4f
0030  00 00
```

15. What is the `Authentication SEQ` value of this authentication frame from AP to Host?

Authentication SEQ: 0x0002

16. What rates are indicated in the frame as SUPPORTED RATES. Do *not* include in your answers below any rates that are indicates as EXTENDED SUPPORTE RATES.

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



Wireshark_801_11.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

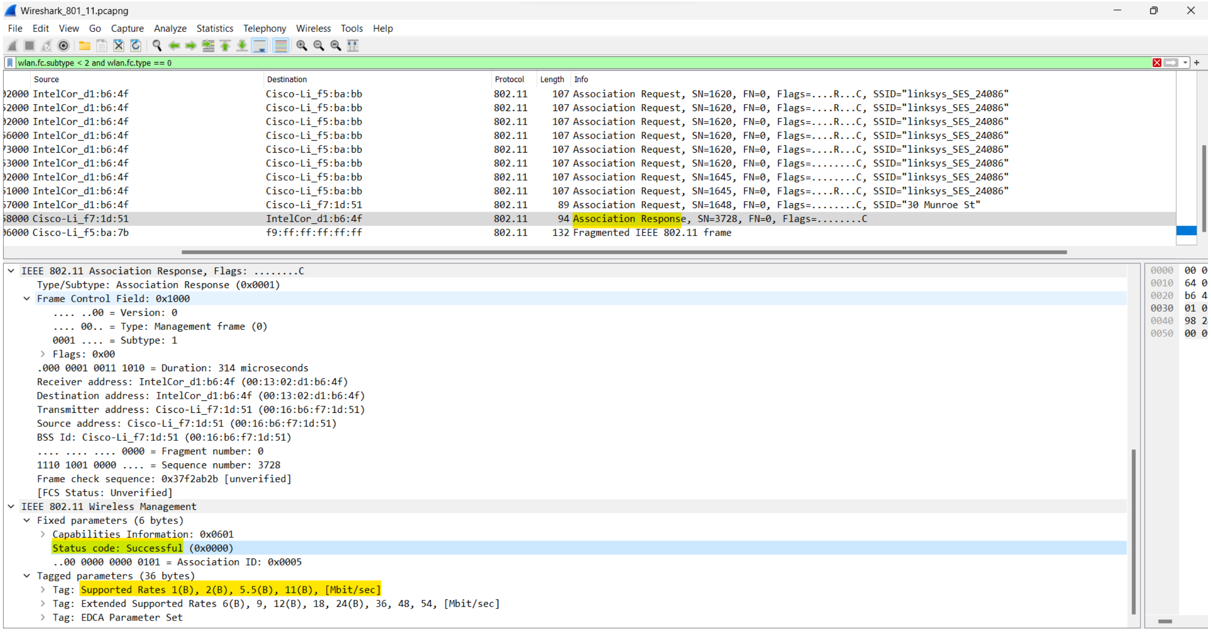
wlan.fc.subtype < 2 and wlan.fc.type == 0

```
      Source                  Destination          Protocol Length Info
)2000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
52000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
)2000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
56000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
73000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
53000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
)2000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24086"
51000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
57000 IntelCor_d1:b6:4f       Cisco-Li_f7:1d:51    802.11    89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
58000 Cisco-Li_f7:1d:51       IntelCor_d1:b6:4f    802.11    94 Association Response, SN=3728, FN=0, Flags=........C
)6000 Cisco-Li_f5:ba:7b       f9:ff:ff:ff:ff:ff    802.11   132 Fragmented IEEE 802.11 frame
```

```
v IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  v Frame Control Field: 0x0000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0000 .... = Subtype: 0
    > Flags: 0x00
    .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 0111 0000 .... = Sequence number: 1648
    Frame check sequence: 0xfe3badc6 [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (4 bytes)
    > Capabilities Information: 0xce01
      Listen Interval: 0x000a
  v 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]
```

```
0000  00 00
0010  64 00
0020  1d 51
0030  01 ce
0040  53 74
0050  04 b6
```

Association Request: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]



Wireshark_801_11.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.subtype < 2 and wlan.fc.type == 0

```
      Source                  Destination          Protocol Length Info
)2000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
52000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
)2000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
56000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
73000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
53000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
)2000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24086"
51000 IntelCor_d1:b6:4f       Cisco-Li_f5:ba:bb    802.11   107 Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
57000 IntelCor_d1:b6:4f       Cisco-Li_f7:1d:51    802.11    89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
58000 Cisco-Li_f7:1d:51       IntelCor_d1:b6:4f    802.11    94 Association Response, SN=3728, FN=0, Flags=........C
)6000 Cisco-Li_f5:ba:7b       f9:ff:ff:ff:ff:ff    802.11   132 Fragmented IEEE 802.11 frame
```

```
v IEEE 802.11 Association Response, Flags: ........C
    Type/Subtype: Association Response (0x0001)
  v Frame Control Field: 0x1000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0001 .... = Subtype: 1
    > Flags: 0x00
    .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 1001 0000 .... = Sequence number: 3728
    Frame check sequence: 0x37f2ab2b [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
    > Capabilities Information: 0x0601
      Status code: Successful (0x0000)
      ..00 0000 0000 0101 = Association ID: 0x0005
  v 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
```

```
0000  00 0
0010  64 0
0020  b6 4
0030  01 0
0040  98 2
0050  00 0
```

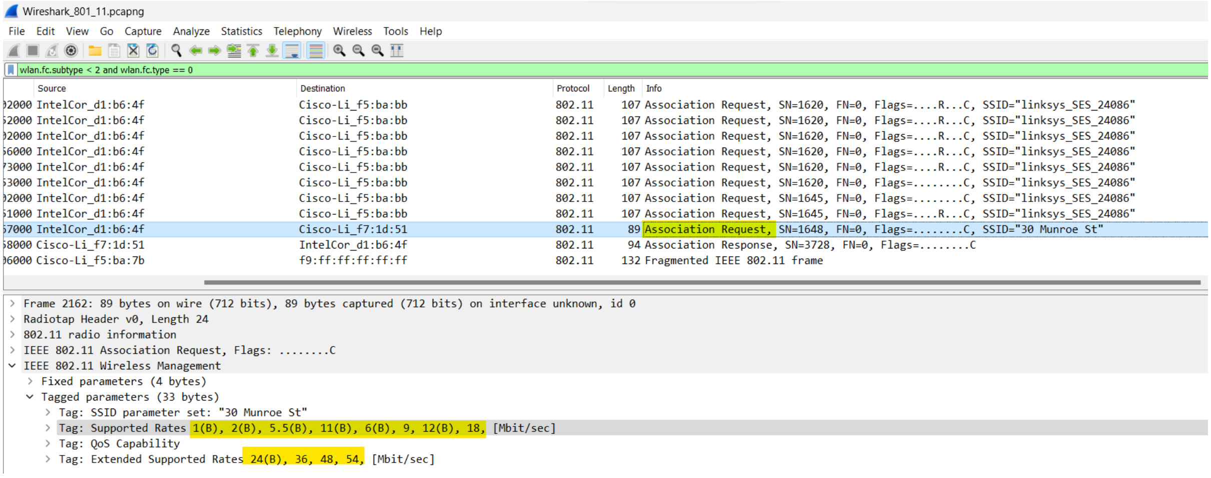
17. Does the ASSOCIATION RESPONSE indicate a Successful or Unsuccessful association response?

Successful

18. Does the fastest (largest) Extended Supported Rate the host has offered match the fastest (largest) Extended Supported Rate the AP is able to provide?

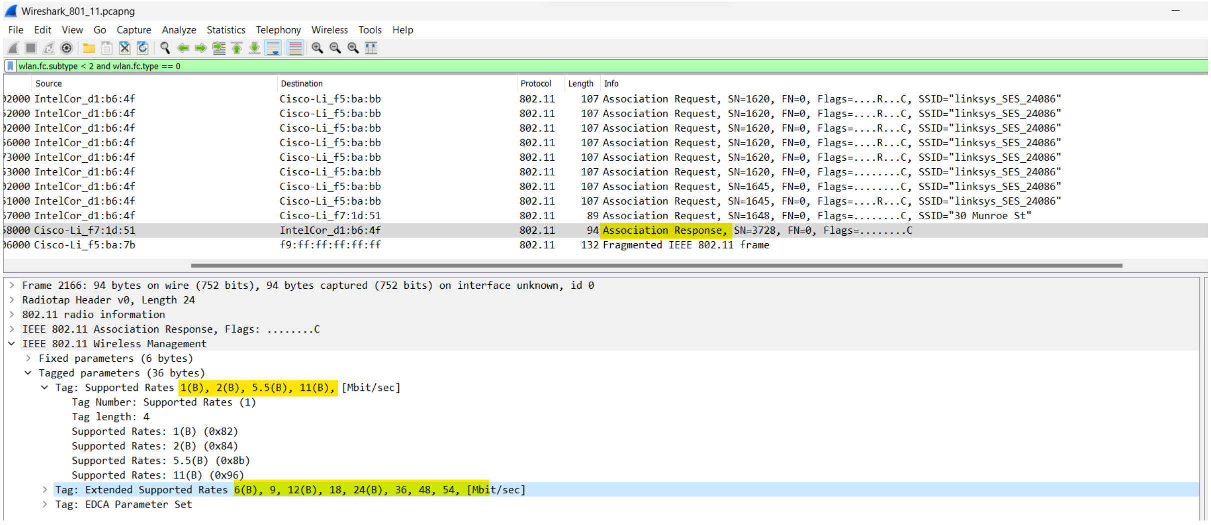
Same.

Transmission rates that the AP (ASSOCIATION REQUEST) willing to use are 1, 2, 5.5, 11, 6, 9,12, 18, 24, 36, 48, 54 (Mbit/sec)


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.subtype < 2 and wlan.fc.type == 0

     Source                    Destination                Protocol  Length Info
2000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
2000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
2000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
6000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
3000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
3000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
2000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24086"
1000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
7000 IntelCor_d1:b6:4f         Cisco-Li_f7:1d:51          802.11     89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
8000 Cisco-Li_f7:1d:51         IntelCor_d1:b6:4f          802.11     94 Association Response, SN=3728, FN=0, Flags=........C
6000 Cisco-Li_f5:ba:7b         f9:ff:ff:ff:ff:ff          802.11    132 Fragmented IEEE 802.11 frame

> Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  v 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]
```

Transmission rates that the AP (ASSOCIATION RESPONSE) willing to use are 1, 2, 5.5, 11, 6, 9,12, 18, 24, 36, 48, 54 (Mbit/sec)


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.subtype < 2 and wlan.fc.type == 0

     Source                    Destination                Protocol  Length Info
2000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
2000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
2000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
6000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
3000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
3000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
2000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24086"
1000 IntelCor_d1:b6:4f         Cisco-Li_f5:ba:bb          802.11    107 Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
7000 IntelCor_d1:b6:4f         Cisco-Li_f7:1d:51          802.11     89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
8000 Cisco-Li_f7:1d:51         IntelCor_d1:b6:4f          802.11     94 Association Response, SN=3728, FN=0, Flags=........C
6000 Cisco-Li_f5:ba:7b         f9:ff:ff:ff:ff:ff          802.11    132 Fragmented IEEE 802.11 frame

> Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface unknown, id 0
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (6 bytes)
  v Tagged parameters (36 bytes)
    v Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
        Tag Number: Supported Rates (1)
        Tag length: 4
        Supported Rates: 1(B) (0x82)
        Supported Rates: 2(B) (0x84)
        Supported Rates: 5.5(B) (0x8b)
        Supported Rates: 11(B) (0x96)
    > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: EDCA Parameter Set
```