ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

MẠNG MÁY TÍNH THỰC HÀNH - CO3094

Báo cáo:

Lab 7

Giảng viên hướng dẫn: Vũ Thành Tài

Sinh viên: Lê Đức Cường

MSSV: 2210423

Thành phố Hồ Chí Minh, tháng 4 năm 2025

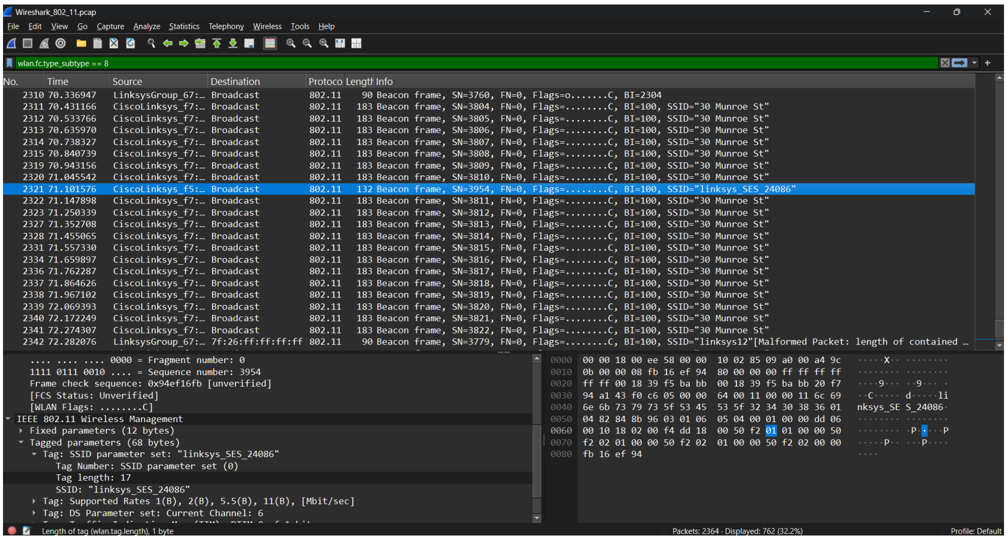
Mục lục

1 Question 1

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

ANS:

The two SSIDs are: 30 Munroe St, linksys_ses_24086. These are seen most frequently in the Beacon frames using the filter wlan.fc.type_subtype == 8.



Wireshark_802_11.pcap

wlan.fc.type_subtype == 8

```
No.  Time       Source               Destination          Protoco Lengtł Info
2310 70.336947  LinksysGroup_67:…    Broadcast            802.11    90 Beacon frame, SN=3760, FN=0, Flags=o.......C, BI=2304
2311 70.431166  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3804, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2312 70.533766  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3805, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2313 70.635970  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3806, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2314 70.738327  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3807, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2315 70.840739  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3808, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2319 70.943156  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3809, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2320 71.045542  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3810, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2321 71.101576  CiscoLinksys_f5:…    Broadcast            802.11   132 Beacon frame, SN=3954, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
2322 71.147898  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3811, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2323 71.250339  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3812, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2327 71.352708  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3813, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2328 71.455065  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3814, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2331 71.557330  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3815, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2334 71.659897  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3816, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2336 71.762287  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3817, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2337 71.864626  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3818, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2338 71.967102  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3819, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2339 72.069393  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3820, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2340 72.172249  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3821, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2341 72.274307  CiscoLinksys_f7:…    Broadcast            802.11   183 Beacon frame, SN=3822, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2342 72.282076  LinksysGroup_67:…    7f:26:ff:ff:ff:ff    802.11    90 Beacon frame, SN=3779, FN=0, Flags=........C, BI=100, SSID="linksys12"[Malformed Packet: length of contained …
```

```
  .... .... .... 0000 = Fragment number: 0
  1111 0111 0010 .... = Sequence number: 3954
  Frame check sequence: 0x94ef16fb [unverified]
  [FCS Status: Unverified]
  [WLAN Flags: ........C]
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
  Tagged parameters (68 bytes)
    Tag: SSID parameter set: "linksys_SES_24086"
      Tag Number: SSID parameter set (0)
      Tag length: 17
      SSID: "linksys_SES_24086"
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 6
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 a4 9c   ·····X·· ········
0010  0b 00 00 08 fb 16 ef 94  80 00 00 00 ff ff ff ff   ········ ········
0020  ff ff 00 18 39 f5 ba bb  00 18 39 f5 ba bb 20 f7   ····9··· ··9··· ·
0030  94 a1 43 f0 c6 05 00 00  64 00 11 00 00 11 6c 69   ··C····· d·····li
0040  6e 6b 73 79 73 5f 53 45  53 5f 32 34 30 38 36 01   nksys_SE S_24086·
0050  04 82 84 8b 96 03 01 06  05 04 00 01 00 00 dd 06   ········ ········
0060  00 10 18 02 00 f4 dd 18  00 50 f2 01 01 00 00 50   ········ ·P····P
0070  f2 02 01 00 00 50 f2 02  01 00 00 50 f2 02 00 00   ·····P·· ···P····
0080  fb 16 ef 94                                        ····
```

Length of tag (wlan.tag.length), 1 byte

Packets: 2364 · Displayed: 762 (32.2%)

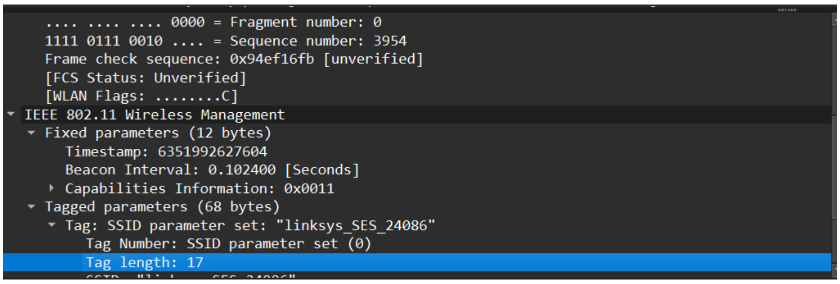
Profile: Default

2 Question 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?

ANS:

The beacon interval is typically 0.1024 seconds for both access points.



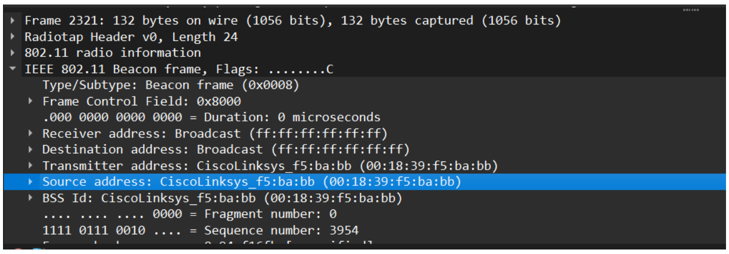
```
  .... .... .... 0000 = Fragment number: 0
  1111 0111 0010 .... = Sequence number: 3954
  Frame check sequence: 0x94ef16fb [unverified]
  [FCS Status: Unverified]
  [WLAN Flags: ........C]
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
    Timestamp: 6351992627604
    Beacon Interval: 0.102400 [Seconds]
    Capabilities Information: 0x0011
  Tagged parameters (68 bytes)
    Tag: SSID parameter set: "linksys_SES_24086"
      Tag Number: SSID parameter set (0)
      Tag length: 17
```

3 Quesiton 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).

ANS:

The source MAC address on the beacon is 00:18:39:f5:ba:bb

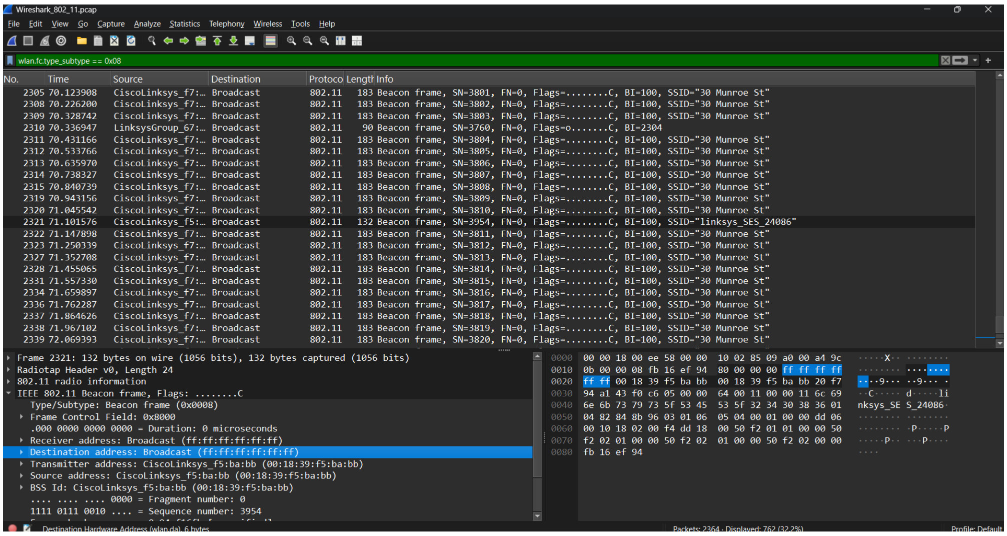


```
Frame 2321: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
   Type/Subtype: Beacon frame (0x0008)
   Frame Control Field: 0x8000
   .000 0000 0000 0000 = Duration: 0 microseconds
   Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
   Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
   Transmitter address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
   Source address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
   BSS Id: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
   .... .... .... 0000 = Fragment number: 0
   1111 0111 0010 .... = Sequence number: 3954
```

4 Question 4

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

ANS: The destination MAC is for broadcast. The destination MAC is ff:ff:ff:ff:ff:ff.



Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type_subtype == 0x08

```
No.   Time      Source              Destination  Protoco Lengtl Info
 2305 70.123908 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3801, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2308 70.226200 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3802, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2309 70.328742 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3803, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2310 70.336947 LinksysGroup_67:... Broadcast    802.11    90 Beacon frame, SN=3760, FN=0, Flags=o.......C, BI=2304
 2311 70.431166 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3804, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2312 70.533766 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3805, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2313 70.635970 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3806, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2314 70.738327 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3807, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2315 70.840739 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3808, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2319 70.943156 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3809, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2320 71.045542 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3810, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2321 71.101576 CiscoLinksys_f5:... Broadcast    802.11   132 Beacon frame, SN=3954, FN=0, Flags=........C, BI=100, SSID="linksys_SES_24086"
 2322 71.147898 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3811, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2323 71.250339 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3812, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2327 71.352708 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3813, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2328 71.455065 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3814, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2331 71.557330 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3815, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2334 71.659897 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3816, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2336 71.762287 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3817, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2337 71.864626 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3818, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2338 71.967102 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3819, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
 2339 72.069393 CiscoLinksys_f7:... Broadcast    802.11   183 Beacon frame, SN=3820, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
```

```
Frame 2321: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
Radiotap Header v0, Length 24
802.11 radio information
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: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
   Source address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
   BSS Id: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
   .... .... .... 0000 = Fragment number: 0
   1111 0111 0010 .... = Sequence number: 3954
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 a4 9c   ·····X·· ········
0010  0b 00 00 08 fb 16 ef 94  80 00 00 00 ff ff ff ff   ········ ········
0020  ff ff 00 18 39 f5 ba bb  00 18 39 f5 ba bb 20 f7   ····9··· ··9··· ·
0030  94 a1 43 f0 c6 05 00 00  64 00 11 00 00 11 6c 69   ··C····· d·····li
0040  6e 6b 73 79 73 5f 53 45  53 5f 32 34 30 38 36 01   nksys_SE S_24086·
0050  04 82 84 8b 96 03 01 06  05 04 00 01 00 00 dd 06   ········ ········
0060  00 10 18 02 00 f4 dd 18  00 50 f2 01 01 00 00 50   ········ ·P·····P
0070  f2 02 01 00 00 50 f2 02  01 00 00 50 f2 02 00 00   ·····P·· ···P····
0080  fb 16 ef 94                                         ····
```

Destination Hardware Address (wlan.da), 6 bytes

Packets: 2364 · Displayed: 762 (32.2%)

Profile: Default

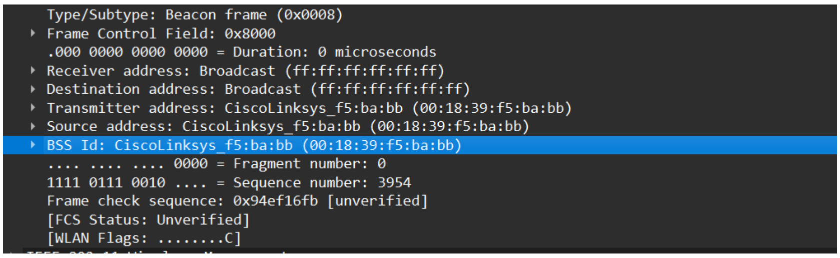
5 Question 5

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

ANS:

`00:18:39:f5:ba:bb`

I found this by filtering beacon frames (wlan.fc.type_subtype == 0x08) and checking the BSS Id field in a frame with SSID "30 Munroe St".



```
    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: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
  ▸ Source address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
  ▸ BSS Id: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    .... .... .... 0000 = Fragment number: 0
    1111 0111 0010 .... = Sequence number: 3954
    Frame check sequence: 0x94ef16fb [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ........C]
```

6 Question 6

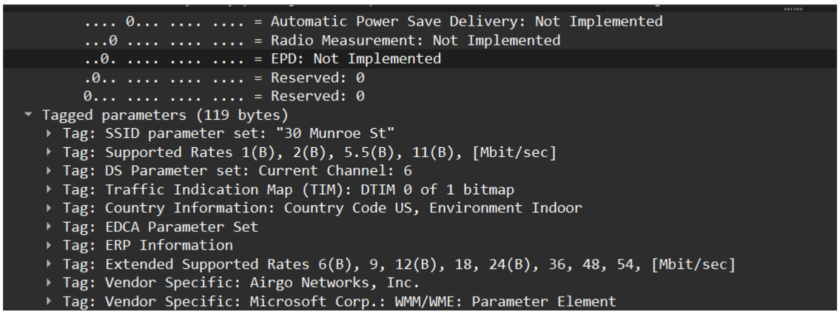
The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?

ANS:

In the beacon frame from 30 Munroe St, the access point advertises the following rates:

Supported Rates: 1, 2, 5.5, 11 Mbps

Extended Supported Rates: 6, 9, 12, 18, 24, 36, 48, 54 Mbps



```
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = EPD: Not Implemented
        .0.. .... .... .... = Reserved: 0
        0... .... .... .... = Reserved: 0
  ▾ 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
```

7 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.

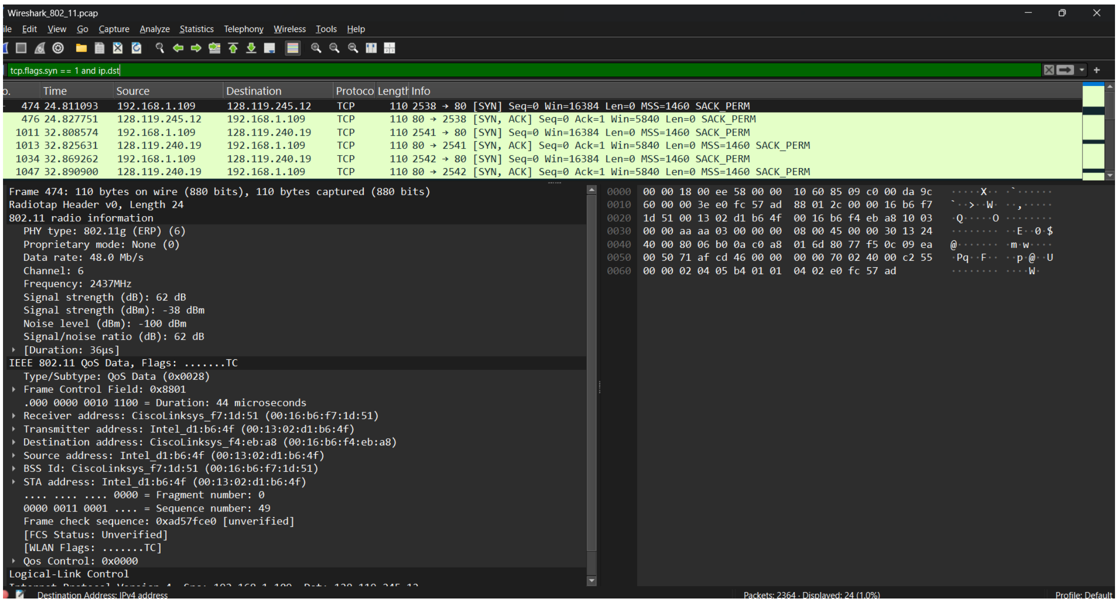
ANS:

The MAC address for the host sending the TCP SYN is 00:13:02:d1:b6:4f.

The MAC address for the destination, which the first hop router to which the host is connected, is 00:16:b6:f4:eb:a8.

The MAC address for the BSS is 00:16:b6:f7:1d:51.

The IP address of the host sending the TCP SYN is 192.168.1.109.


Wireshark_802_11.pcap
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packets: 2364 · Displayed: 24 (1.0%)
Profile: Default
Destination Address: IPv4 address

tcp.flags.syn == 1 and ip.dst

```
o.    Time       Source          Destination     Protoco Length Info
  474 24.811093  192.168.1.109   128.119.245.12  TCP     110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
  476 24.827751  128.119.245.12  192.168.1.109   TCP     110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
 1011 32.808574  192.168.1.109   128.119.240.19  TCP     110 2541 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
 1013 32.825631  128.119.240.19  192.168.1.109   TCP     110 80 → 2541 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
 1034 32.869262  192.168.1.109   128.119.240.19  TCP     110 2542 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
 1047 32.890900  128.119.240.19  192.168.1.109   TCP     110 80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
```

```
Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Radiotap Header v0, Length 24
802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Proprietary mode: None (0)
  Data rate: 48.0 Mb/s
  Channel: 6
  Frequency: 2437MHz
  Signal strength (dB): 62 dB
  Signal strength (dBm): -38 dBm
  Noise level (dBm): -100 dBm
  Signal/noise ratio (dB): 62 dB
› [Duration: 36µs]
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: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
› Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
› Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
› Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
› BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
› STA address: Intel_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]
  [WLAN Flags: .......TC]
› Qos Control: 0x0000
Logical-Link Control
```

```
0000  00 00 18 00 ee 58 00 00  10 60 85 09 c0 00 da 9c   ·····X·· ·`······
0010  60 00 00 3e e0 fc 57 ad  88 01 2c 00 00 16 b6 f7   `··>··W· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 10 03   ·Q·····O ········
0030  00 00 aa aa 03 00 00 00  08 00 45 00 00 30 13 24   ········ ··E··0·$
0040  40 00 80 06 b0 0a c0 a8  01 6d 80 77 f5 0c 09 ea   @······· ·m·w····
0050  00 50 71 af cd 46 00 00  00 00 70 02 40 00 c2 55   ·Pq··F·· ··p·@··U
0060  00 00 02 04 05 b4 01 01  04 02 e0 fc 57 ad         ········ ····W·
```

8 Question 8

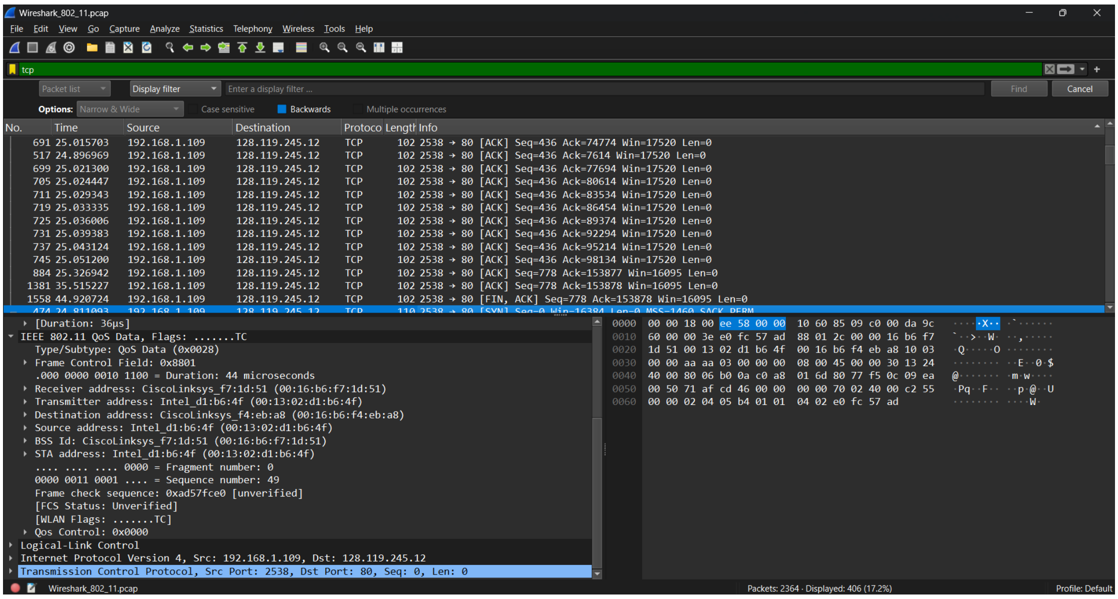
Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address 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).

ANS: The following MAC addresses were noted:

- Source MAC Address (Access Point): 00:13:02:d1:b6:4f
- Destination MAC Address (Host): 00:16:b6:f4:eb:a8
- BSS ID (Network): 00:16:b6:f7:1d:51

I expanded the Internet Protocol Version 4 (IPv4) section to find the IP addresses associated with the frame.

- Source IP Address (Host): 192.168.1.109
- Destination IP Address: 128.199.245.12



Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Display filter
Enter a display filter ...
Find
Cancel
Options: Narrow & Wide
Case sensitive
Backwards
Multiple occurrences
Packets: 2364 · Displayed: 406 (17.2%)
Profile: Default

Display filter: tcp

```
No.  Time      Source         Destination     Protoco Lengtl Info
 691 25.015703 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=74774 Win=17520 Len=0
 517 24.896969 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=7614 Win=17520 Len=0
 699 25.021300 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=77694 Win=17520 Len=0
 705 25.024447 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=80614 Win=17520 Len=0
 711 25.029343 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=83534 Win=17520 Len=0
 719 25.033335 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=86454 Win=17520 Len=0
 725 25.036006 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=89374 Win=17520 Len=0
 731 25.039383 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=92294 Win=17520 Len=0
 737 25.043124 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=95214 Win=17520 Len=0
 745 25.051200 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=436 Ack=98134 Win=17520 Len=0
 884 25.326942 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=778 Ack=153877 Win=16095 Len=0
1381 35.515227 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [ACK] Seq=778 Ack=153878 Win=16095 Len=0
1558 44.920724 192.168.1.109  128.119.245.12  TCP     102 2538 → 80 [FIN, ACK] Seq=778 Ack=153878 Win=16095 Len=0
 474 24.811093 192.168.1.109  128.119.245.12  TCP     110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
```

```
  [Duration: 36µs]
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: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
  Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
  Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
  BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  STA address: Intel_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]
  [WLAN Flags: .......TC]
  Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 00 18 00 ee 58 00 00  10 60 85 09 c0 00 da 9c   ····X·· ·`······
0010  60 00 00 3e e0 fc 57 ad  88 01 2c 00 00 16 b6 f7   `··>··W· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 10 03   ·Q·····O ········
0030  00 00 aa aa 03 00 00 00  08 00 45 00 00 30 13 24   ········ ··E··0·$
0040  40 00 80 06 b0 0a c0 a8  01 6d 80 77 f5 0c 09 ea   @······· ·m·w····
0050  00 50 71 af cd 46 00 00  00 00 70 02 40 00 c2 55   ·Pq··F·· ··p·@··U
0060  00 00 02 04 05 b4 01 01  04 02 e0 fc 57 ad         ········ ····W·
```

Wireshark_802_11.pcap

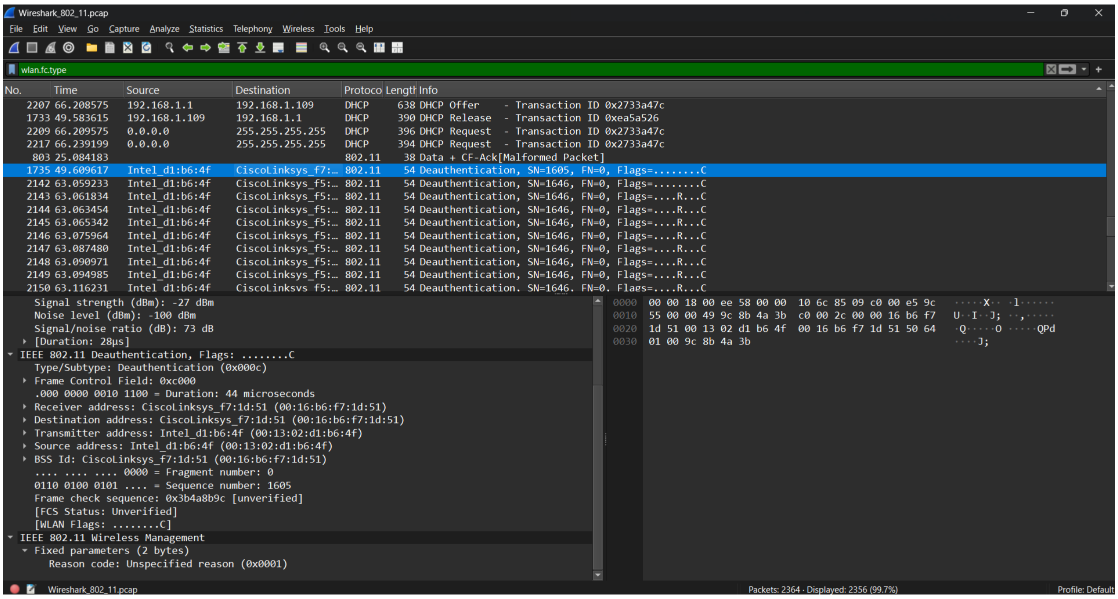
9 Question 9

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?

ANS:

A DHCP is sent to 192.168.1.1

The host sends a DEAUTHENTICATION frame after 0.02s


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan.fc.type

```
No.   Time       Source         Destination        Protoco Length Info
 2207 66.208575  192.168.1.1    192.168.1.109      DHCP    638 DHCP Offer    - Transaction ID 0x2733a47c
 1733 49.583615  192.168.1.109  192.168.1.1        DHCP    390 DHCP Release  - Transaction ID 0xea5a526
 2209 66.209575  0.0.0.0        255.255.255.255    DHCP    396 DHCP Request  - Transaction ID 0x2733a47c
 2217 66.239199  0.0.0.0        255.255.255.255    DHCP    394 DHCP Request  - Transaction ID 0x2733a47c
  803 25.084183                                    802.11   38 Data + CF-Ack[Malformed Packet]
 1735 49.609617  Intel_d1:b6:4f CiscoLinksys_f7:… 802.11   54 Deauthentication, SN=1605, FN=0, Flags=........C
 2142 63.059233  Intel_d1:b6:4f CiscoLinksys_f5:… 802.11   54 Deauthentication, SN=1646, FN=0, Flags=........C
 2143 63.061834  Intel_d1:b6:4f CiscoLinksys_f5:… 802.11   54 Deauthentication, SN=1646, FN=0, Flags=....R...C
 2144 63.063454  Intel_d1:b6:4f CiscoLinksys_f5:… 802.11   54 Deauthentication, SN=1646, FN=0, Flags=....R...C
 2145 63.065342  Intel_d1:b6:4f CiscoLinksys_f5:… 802.11   54 Deauthentication, SN=1646, FN=0, Flags=....R...C
 2146 63.075964  Intel_d1:b6:4f CiscoLinksys_f5:… 802.11   54 Deauthentication, SN=1646, FN=0, Flags=....R...C
 2147 63.087480  Intel_d1:b6:4f CiscoLinksys_f5:… 802.11   54 Deauthentication, SN=1646, FN=0, Flags=....R...C
 2148 63.090971  Intel_d1:b6:4f CiscoLinksys_f5:… 802.11   54 Deauthentication, SN=1646, FN=0, Flags=....R...C
 2149 63.094985  Intel_d1:b6:4f CiscoLinksys_f5:… 802.11   54 Deauthentication, SN=1646, FN=0, Flags=....R...C
 2150 63.116231  Intel_d1:b6:4f CiscoLinksys_f5:… 802.11   54 Deauthentication, SN=1646, FN=0, Flags=....R...C
```

```
    Signal strength (dBm): -27 dBm
    Noise level (dBm): -100 dBm
    Signal/noise ratio (dB): 73 dB
  › [Duration: 28µs]
˅ IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  › Frame Control Field: 0xc000
    .000 0000 0010 1100 = Duration: 44 microseconds
  › Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  › Destination address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  › Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
  › Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
  › BSS Id: CiscoLinksys_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]
    [WLAN Flags: ........C]
˅ IEEE 802.11 Wireless Management
  ˅ Fixed parameters (2 bytes)
      Reason code: Unspecified reason (0x0001)
```

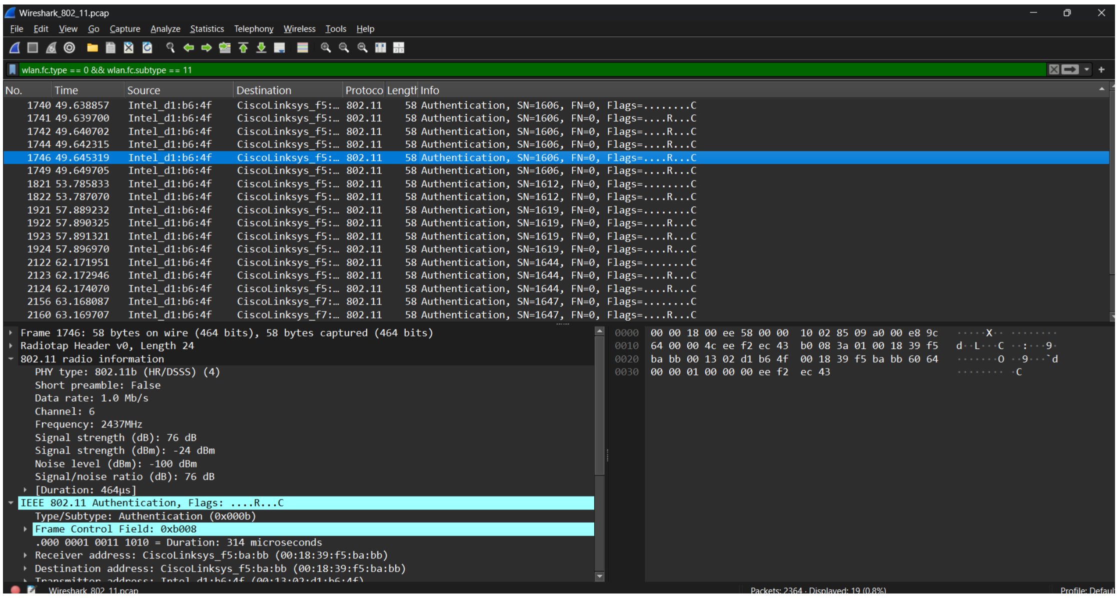
```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e5 9c   ·····X·· ·l······
0010  55 00 00 49 9c 8b 4a 3b  c0 00 2c 00 00 16 b6 f7   U··I··J; ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f7 1d 51 50 64   ·Q·····O ·····QPd
0030  01 00 9c 8b 4a 3b                                  ····J;
```

10 Question 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? .

ANS:

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



```
wlan.fc.type == 0 && wlan.fc.subtype == 11

No.  Time       Source           Destination        Protoco Lengtł Info
1740 49.638857  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1606, FN=0, Flags=........C
1741 49.639700  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1742 49.640702  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1744 49.642315  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1746 49.645319  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1749 49.649705  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1821 53.785833  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1612, FN=0, Flags=........C
1822 53.787070  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1612, FN=0, Flags=....R...C
1921 57.889232  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1619, FN=0, Flags=........C
1922 57.890325  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1619, FN=0, Flags=....R...C
1923 57.891321  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1619, FN=0, Flags=....R...C
1924 57.896970  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1619, FN=0, Flags=....R...C
2122 62.171951  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1644, FN=0, Flags=........C
2123 62.172946  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1644, FN=0, Flags=....R...C
2124 62.174070  Intel_d1:b6:4f   CiscoLinksys_f5:…  802.11   58 Authentication, SN=1644, FN=0, Flags=....R...C
2156 63.168087  Intel_d1:b6:4f   CiscoLinksys_f7:…  802.11   58 Authentication, SN=1647, FN=0, Flags=........C
2160 63.169707  Intel_d1:b6:4f   CiscoLinksys_f7:…  802.11   58 Authentication, SN=1647, FN=0, Flags=....R...C

› Frame 1746: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
› Radiotap Header v0, Length 24
⌄ 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): 76 dB
    Signal strength (dBm): -24 dBm
    Noise level (dBm): -100 dBm
    Signal/noise ratio (dB): 76 dB
  › [Duration: 464µs]
⌄ IEEE 802.11 Authentication, Flags: ....R...C
    Type/Subtype: Authentication (0x000b)
  › Frame Control Field: 0xb008
    .000 0001 0011 1010 = Duration: 314 microseconds
  › Receiver address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
  › Destination address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
  › Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)

0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e8 9c   ·····X·· ········
0010  64 00 00 4c ee f2 ec 43  b0 08 3a 01 00 18 39 f5   d··L···C ··:···9·
0020  ba bb 00 13 02 d1 b6 4f  00 18 39 f5 ba bb 60 64   ·······O ··9···`d
0030  00 00 01 00 00 00 ee f2  ec 43                     ········ ·C

Wireshark_802_11.pcap          Packets: 2364 · Displayed: 19 (0.8%)          Profile: Default
```

11 Quesion 11

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

ANS: In the analysis of the AUTHENTICATION frames sent from the wireless host to the linksys_ses_24086 access point, it was determined that the host is requesting. This indicates that no key is required for the authentication process. The Authentication Algorithm field in the AUTHENTICATION frame confirmed this, as it specified that the host does not need to provide a shared key for authentication. Therefore, the host is attempting to connect to the access point without requiring any encryption key, allowing for an open connection.

12 Quesion 12

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

ANS:

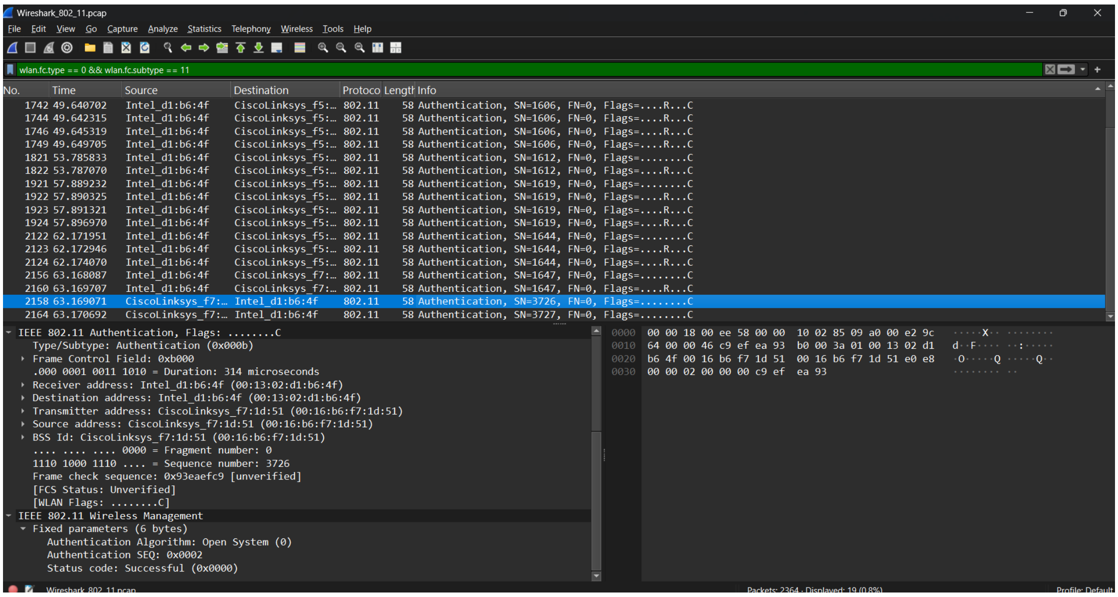
In the examination of the trace for AUTHENTICATION frames, it was found that there is indeed a reply AUTHENTICATION frame sent from the linksys_ses_24086 access point back to the wireless host. This reply is crucial as it indicates the access point's response to the host's authentication request. The AUTHENTICATION frame from the access point confirms whether the host's request was accepted or rejected. In this case, the reply frame shows that the access point did respond, but it is important to analyze the details of this frame to determine the outcome of the authentication process. Specifically, the Status Code field within the AUTHENTICATION frame will indicate whether the authentication was successful or if there was an error.

13 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 AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

ANS:

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

wlan.fc.type == 0 && wlan.fc.subtype == 11

```
No.  Time      Source             Destination        Protoco Lengtl Info
1742 49.640702 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1606, FN=0, Flags=....R...C
1744 49.642315 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1606, FN=0, Flags=....R...C
1746 49.645319 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1606, FN=0, Flags=....R...C
1749 49.649705 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1606, FN=0, Flags=....R...C
1821 53.785833 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1612, FN=0, Flags=........C
1822 53.787070 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1612, FN=0, Flags=....R...C
1921 57.889232 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1619, FN=0, Flags=........C
1922 57.890325 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1619, FN=0, Flags=....R...C
1923 57.891321 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1619, FN=0, Flags=....R...C
1924 57.896970 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1619, FN=0, Flags=....R...C
2122 62.171951 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1644, FN=0, Flags=........C
2123 62.172946 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1644, FN=0, Flags=....R...C
2124 62.174070 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  58 Authentication, SN=1644, FN=0, Flags=....R...C
2156 63.168087 Intel_d1:b6:4f     CiscoLinksys_f7:… 802.11  58 Authentication, SN=1647, FN=0, Flags=........C
2160 63.169707 Intel_d1:b6:4f     CiscoLinksys_f7:… 802.11  58 Authentication, SN=1647, FN=0, Flags=....R...C
2158 63.169071 CiscoLinksys_f7:… Intel_d1:b6:4f     802.11  58 Authentication, SN=3726, FN=0, Flags=........C
2164 63.170692 CiscoLinksys_f7:… Intel_d1:b6:4f     802.11  58 Authentication, SN=3727, FN=0, Flags=........C
```

```
IEEE 802.11 Authentication, Flags: ........C
   Type/Subtype: Authentication (0x000b)
 › Frame Control Field: 0xb000
   .000 0001 0011 1010 = Duration: 314 microseconds
 › Receiver address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
 › Destination address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
 › Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
 › Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
 › BSS Id: CiscoLinksys_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]
   [WLAN Flags: ........C]
IEEE 802.11 Wireless Management
 ⌄ Fixed parameters (6 bytes)
     Authentication Algorithm: Open System (0)
     Authentication SEQ: 0x0002
     Status code: Successful (0x0000)
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e2 9c   ·····X·· ········
0010  64 00 00 46 c9 ef ea 93  b0 00 3a 01 00 13 02 d1   d··F···· ··:·····
0020  b6 4f 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 e0 e8   ·O·····Q ·····Q··
0030  00 00 02 00 00 00 c9 ef  ea 93                     ········ ··
```

Wireshark_802_11.pcap   Packets: 2364 · Displayed: 19 (0.8%)   Profile: Default

14 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.)

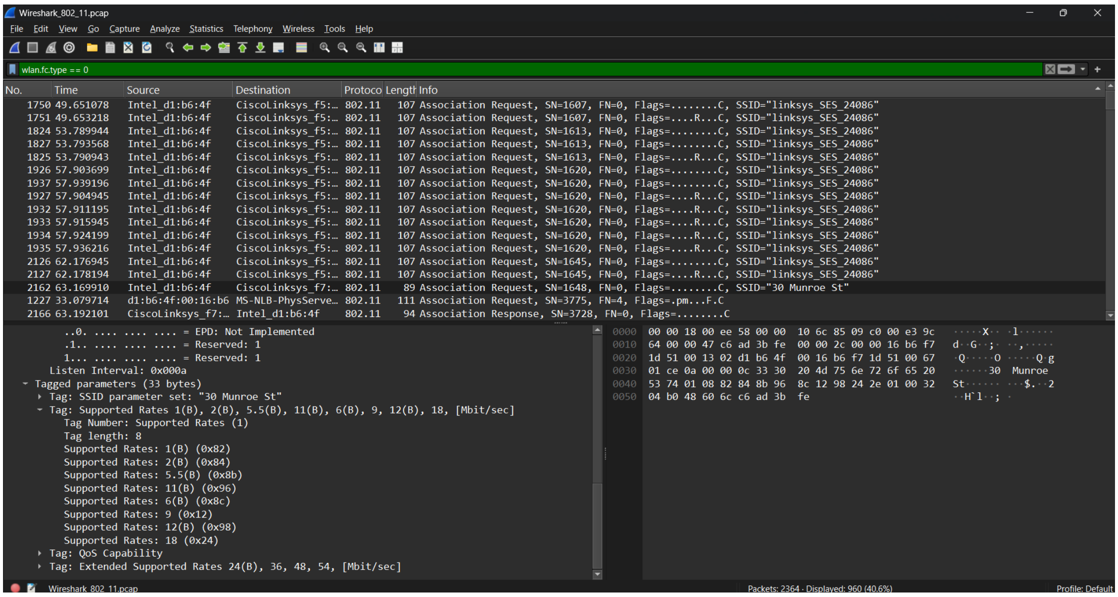
ANS:

ASSOCIATE REQUEST from host to the 30 Munroe St AP at t = 63.169910 and replied at t = 63.192101.

15 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.

ANS: The possible rates are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, 54 Mbps.


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type == 0
```

```
No.  Time      Source             Destination         Protoco Lengtł Info
1750 49.651078 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1607, FN=0, Flags=........C, SSID="linksys_SES_24086"
1751 49.653218 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1607, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1824 53.789944 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1613, FN=0, Flags=........C, SSID="linksys_SES_24086"
1827 53.793568 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1613, FN=0, Flags=........C, SSID="linksys_SES_24086"
1825 53.790943 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1613, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1926 57.903699 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
1937 57.939196 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
1927 57.904945 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1932 57.911195 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1933 57.915945 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1934 57.924199 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1935 57.936216 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
2126 62.176945 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24086"
2127 62.178194 Intel_d1:b6:4f     CiscoLinksys_f5:… 802.11  107 Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
2162 63.169910 Intel_d1:b6:4f     CiscoLinksys_f7:… 802.11   89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
1227 33.079714 d1:b6:4f:00:16:b6 MS-NLB-PhysServe… 802.11  111 Association Request, SN=3775, FN=4, Flags=.pm...F.C
2166 63.192101 CiscoLinksys_f7:… Intel_d1:b6:4f     802.11   94 Association Response, SN=3728, FN=0, Flags=........C
```

```
        ..0. .... .... .... = EPD: Not Implemented
        .1.. .... .... .... = Reserved: 1
        1... .... .... .... = Reserved: 1
     Listen Interval: 0x000a
  ⌄ 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 Number: Supported Rates (1)
          Tag length: 8
          Supported Rates: 1(B) (0x82)
          Supported Rates: 2(B) (0x84)
          Supported Rates: 5.5(B) (0x8b)
          Supported Rates: 11(B) (0x96)
          Supported Rates: 6(B) (0x8c)
          Supported Rates: 9 (0x12)
          Supported Rates: 12(B) (0x98)
          Supported Rates: 18 (0x24)
     › Tag: QoS Capability
     › Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e3 9c   ·····X·· ·l······
0010  64 00 00 47 c6 ad 3b fe  00 00 2c 00 00 16 b6 f7   d··G··;· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f7 1d 51 00 67   ·Q·····O ·····Q·g
0030  01 ce 0a 00 00 0c 33 30  20 4d 75 6e 72 6f 65 20   ······30  Munroe
0040  53 74 01 08 82 84 8b 96  8c 12 98 24 2e 01 00 32   St······ ···$.··2
0050  04 b0 48 60 6c c6 ad 3b  fe                        ··H`l··; ·
```

16 Question 16

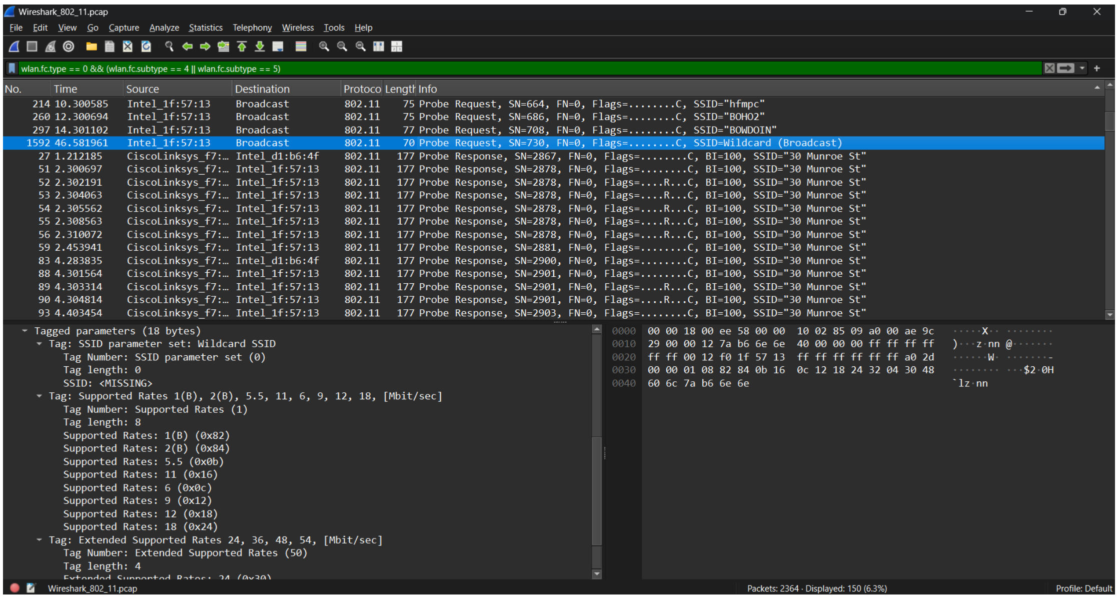
What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).

ANS:

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

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.


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type == 0 && (wlan.fc.subtype == 4 || wlan.fc.subtype == 5)

```
No.   Time       Source              Destination      Protoco Lengtl Info
  214 10.300585  Intel_1f:57:13      Broadcast        802.11   75 Probe Request, SN=664, FN=0, Flags=........C, SSID="hfmpc"
  260 12.300694  Intel_1f:57:13      Broadcast        802.11   75 Probe Request, SN=686, FN=0, Flags=........C, SSID="BOHO2"
  297 14.301102  Intel_1f:57:13      Broadcast        802.11   77 Probe Request, SN=708, FN=0, Flags=........C, SSID="BOWDOIN"
 1592 46.581961  Intel_1f:57:13      Broadcast        802.11   70 Probe Request, SN=730, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
   27 1.212185   CiscoLinksys_f7:…   Intel_d1:b6:4f   802.11  177 Probe Response, SN=2867, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   51 2.300697   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2878, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   52 2.302191   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID="30 Munroe St"
   53 2.304063   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID="30 Munroe St"
   54 2.305562   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID="30 Munroe St"
   55 2.308563   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID="30 Munroe St"
   56 2.310072   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID="30 Munroe St"
   59 2.453941   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2881, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   83 4.283835   CiscoLinksys_f7:…   Intel_d1:b6:4f   802.11  177 Probe Response, SN=2900, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   88 4.301564   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2901, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   89 4.303314   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2901, FN=0, Flags=....R...C, BI=100, SSID="30 Munroe St"
   90 4.304814   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2901, FN=0, Flags=....R...C, BI=100, SSID="30 Munroe St"
   93 4.403454   CiscoLinksys_f7:…   Intel_1f:57:13   802.11  177 Probe Response, SN=2903, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
```

```
▾ Tagged parameters (18 bytes)
  ▾ Tag: SSID parameter set: Wildcard SSID
      Tag Number: SSID parameter set (0)
      Tag length: 0
      SSID: <MISSING>
  ▾ Tag: Supported Rates 1(B), 2(B), 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
      Tag Number: Supported Rates (1)
      Tag length: 8
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5 (0x0b)
      Supported Rates: 11 (0x16)
      Supported Rates: 6 (0x0c)
      Supported Rates: 9 (0x12)
      Supported Rates: 12 (0x18)
      Supported Rates: 18 (0x24)
  ▾ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 4
      Extended Supported Rates: 24 (0x30)
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 ae 9c   ·····X·· ········
0010  29 00 00 12 7a b6 6e 6e  40 00 00 00 ff ff ff ff   )···z·nn @·······
0020  ff ff 00 12 f0 1f 57 13  ff ff ff ff ff ff a0 2d   ······W· ·······-
0030  00 00 01 08 82 84 0b 16  0c 12 18 24 32 04 30 48   ········ ···$2·0H
0040  60 6c 7a b6 6e 6e                                  `lz·nn
```

Wireshark_802_11.pcap   Packets: 2364 · Displayed: 150 (6.3%)   Profile: Default