Name - Khushi Nitinkumar Patel
PRN - 2020BTECS00037
Batch - S3

ASSIGNMENT 6 - Wireshark Lab: 802.11

In this lab, we'll investigate the 802.11 wireless network protocol.

In all of the Wireshark labs thus far, we've captured frames on a wired Ethernet connection. Here, since 802.11 is a wireless link-layer protocol, we'll be capturing frames "in the air." Unfortunately, most of the device drivers for wireless 802.11 NICs (particularly for Windows operating systems) don't provide the hooks to capture/copy received 802.11 frames for use in Wireshark .Thus, in this lab, we'll provide a trace of captured 802.11 frames for you to analyze and assume in the questions below that you are using this trace. If you're able to capture 802.11 frames using your version of Wireshark, you're welcome to do so. Additionally, if you're really into frame capture, you can buy a small USB device, AirPcap, http://www.cacetech.com, that captures 802.11 frames and provides integrated support for Wireshark under Windows.

1. Getting Started

Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file Wireshark_802_11.pcap. This trace was collected using AirPcap and Wireshark running on a computer in the home network , consisting of a Linksys 802.11g combined access point/router, with two wired PCs and one wireless host PC attached to the access point/router. In this trace file, we'll see frames captured on channel 6. Since the host and AP that we are interested in are not the only devices using channel 6, we'll see a lot of frames that we're not interested in for this lab, such as beacon frames advertised by a neighbor's AP also operating on channel 6. The wireless host activities taken in the trace file are:

- The host is already associated with the *30 Munroe St* AP when the trace begins.

- At *t = 24.82*, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12.

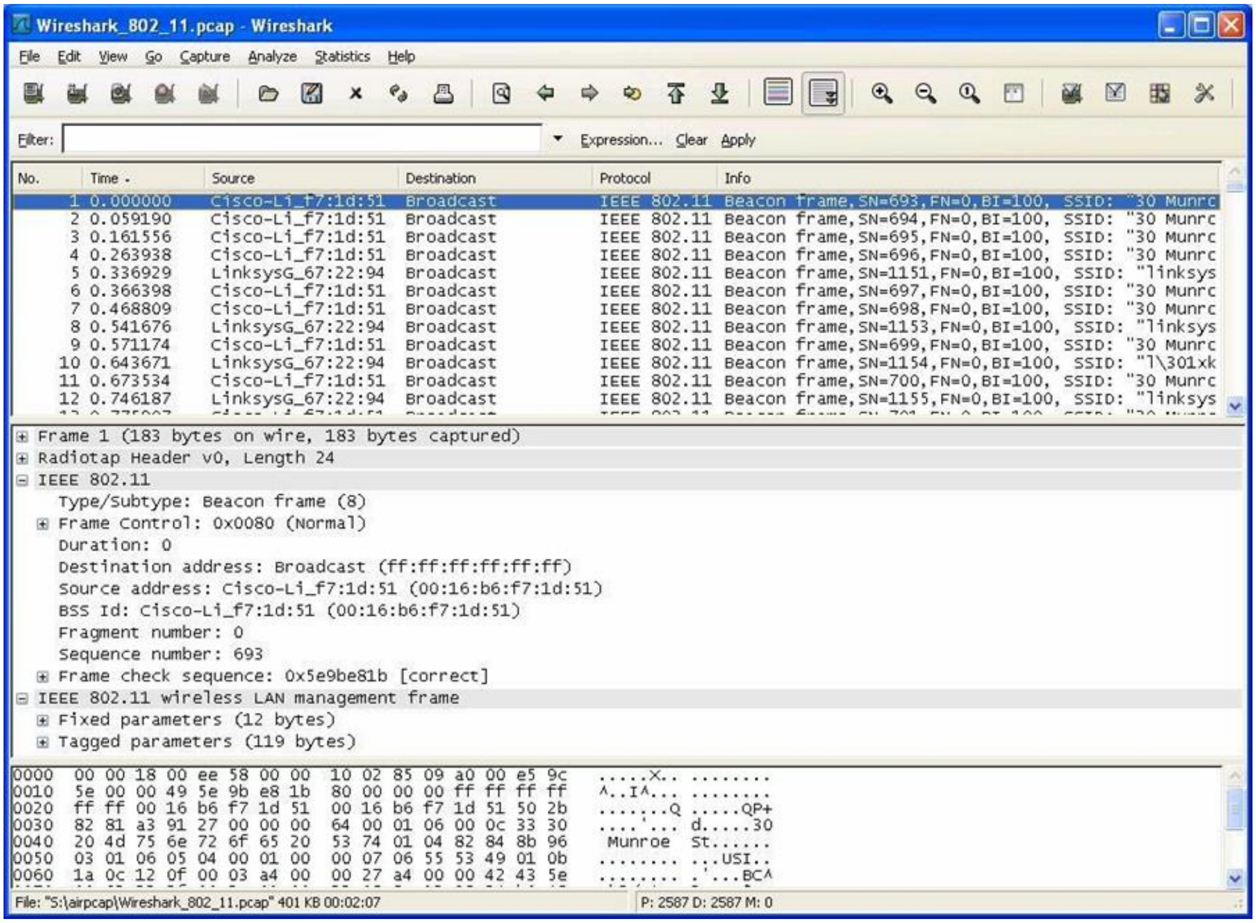
- At *t=32.82, t*he host makes an HTTP request to http://www.cs.umass.edu, whose IP address is 128.119.240.19.

- At *t = 49.58,* the host disconnects from the *30 Munroe St* AP and attempts to connect to the *linksys_ses_24086* AP. This is not an open access point, and so the host is eventually unable to connect to this AP.

- At *t=63.0* the host gives up trying to associate with the *linksys_ses_24086* AP, and associates again with the *30 Munroe St* access point.

Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the

Wireshark_802_11.pcap trace file. The resulting display should look just like Figure 1.


Wireshark_802_11.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No.  Time       Source              Destination  Protocol     Info
  1 0.000000   Cisco-Li_f7:1d:51   Broadcast    IEEE 802.11  Beacon frame,SN=693,FN=0,BI=100, SSID: "30 Munrc
  2 0.059190   Cisco-Li_f7:1d:51   Broadcast    IEEE 802.11  Beacon frame,SN=694,FN=0,BI=100, SSID: "30 Munrc
  3 0.161556   Cisco-Li_f7:1d:51   Broadcast    IEEE 802.11  Beacon frame,SN=695,FN=0,BI=100, SSID: "30 Munrc
  4 0.263938   Cisco-Li_f7:1d:51   Broadcast    IEEE 802.11  Beacon frame,SN=696,FN=0,BI=100, SSID: "30 Munrc
  5 0.336929   LinksysG_67:22:94   Broadcast    IEEE 802.11  Beacon frame,SN=1151,FN=0,BI=100, SSID: "linksys
  6 0.366398   Cisco-Li_f7:1d:51   Broadcast    IEEE 802.11  Beacon frame,SN=697,FN=0,BI=100, SSID: "30 Munrc
  7 0.468809   Cisco-Li_f7:1d:51   Broadcast    IEEE 802.11  Beacon frame,SN=698,FN=0,BI=100, SSID: "30 Munrc
  8 0.541676   LinksysG_67:22:94   Broadcast    IEEE 802.11  Beacon frame,SN=1153,FN=0,BI=100, SSID: "linksys
  9 0.571174   Cisco-Li_f7:1d:51   Broadcast    IEEE 802.11  Beacon frame,SN=699,FN=0,BI=100, SSID: "30 Munrc
 10 0.643671   LinksysG_67:22:94   Broadcast    IEEE 802.11  Beacon frame,SN=1154,FN=0,BI=100, SSID: "l\301xk
 11 0.673534   Cisco-Li_f7:1d:51   Broadcast    IEEE 802.11  Beacon frame,SN=700,FN=0,BI=100, SSID: "30 Munrc
 12 0.746187   LinksysG_67:22:94   Broadcast    IEEE 802.11  Beacon frame,SN=1155,FN=0,BI=100, SSID: "linksys
```

```
⊞ Frame 1 (183 bytes on wire, 183 bytes captured)
⊞ Radiotap Header v0, Length 24
⊟ IEEE 802.11
    Type/Subtype: Beacon frame (8)
  ⊞ Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    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)
    Fragment number: 0
    Sequence number: 693
  ⊞ Frame check sequence: 0x5e9be81b [correct]
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊞ Tagged parameters (119 bytes)
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e5 9c   .....X.. ........
0010  5e 00 00 49 5e 9b e8 1b  80 00 00 00 ff ff ff ff   ^..I^... ........
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 50 2b   .......Q .....QP+
0030  82 81 a3 91 27 00 00 00  64 00 01 06 00 0c 33 30   ....'... d.....30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe  St......
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b   ........ ...USI..
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e   ........ .'...BC^
```

File: "S:\airpcap\Wireshark_802_11.pcap" 401 KB 00:02:07   P: 2587 D: 2587 M: 0

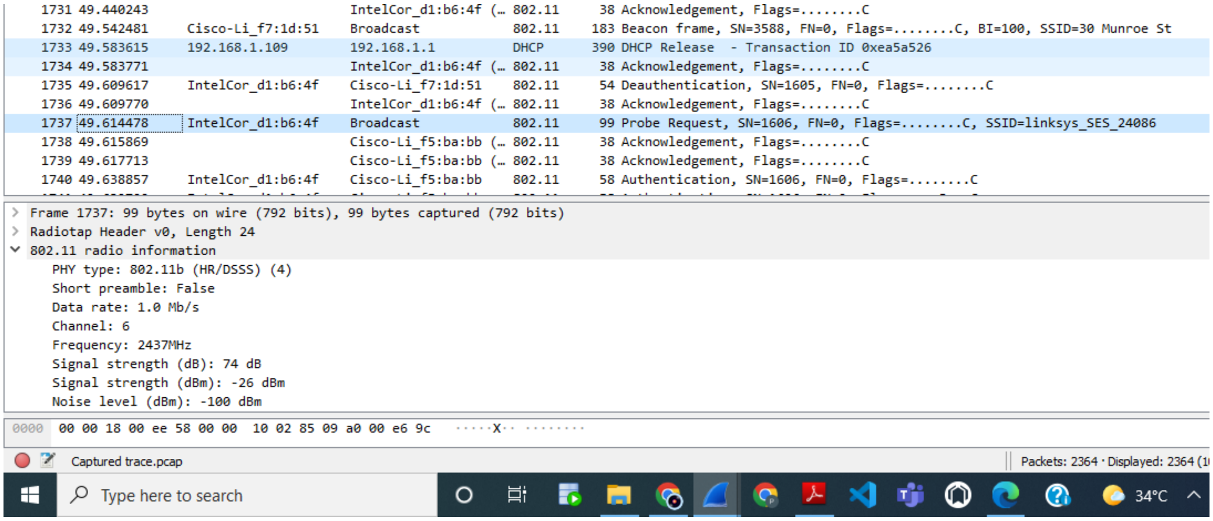
Figure 1: Wireshark window, after opening the Wireshark_802_11.pcap file

2. Beacon Frames

Recall that beacon frames are used by an 802.11 AP to advertise its existence. To answer some of the questions below, you'll want to look at the details of the "IEEE 802.11" frame and subfields in the middle Wireshark window.

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

The two access points that are issuing most of the beacon frames in the trace, have an SSID of 30 Munroe St and linsys_SES_24086.



```
1731 49.440243                     IntelCor_d1:b6:4f (… 802.11     38 Acknowledgement, Flags=........C
1732 49.542481   Cisco-Li_f7:1d:51  Broadcast            802.11    183 Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1733 49.583615   192.168.1.109      192.168.1.1          DHCP      390 DHCP Release  - Transaction ID 0xea5a526
1734 49.583771                     IntelCor_d1:b6:4f (… 802.11     38 Acknowledgement, Flags=........C
1735 49.609617   IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51    802.11     54 Deauthentication, SN=1605, FN=0, Flags=........C
1736 49.609770                     IntelCor_d1:b6:4f (… 802.11     38 Acknowledgement, Flags=........C
1737 49.614478   IntelCor_d1:b6:4f  Broadcast            802.11     99 Probe Request, SN=1606, FN=0, Flags=........C, SSID=linksys_SES_24086
1738 49.615869                     Cisco-Li_f5:ba:bb (… 802.11     38 Acknowledgement, Flags=........C
1739 49.617713                     Cisco-Li_f5:ba:bb (… 802.11     38 Acknowledgement, Flags=........C
1740 49.638857   IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11     58 Authentication, SN=1606, FN=0, Flags=........C
```

```
> Frame 1737: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
> 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): 74 dB
    Signal strength (dBm): -26 dBm
    Noise level (dBm): -100 dBm
```

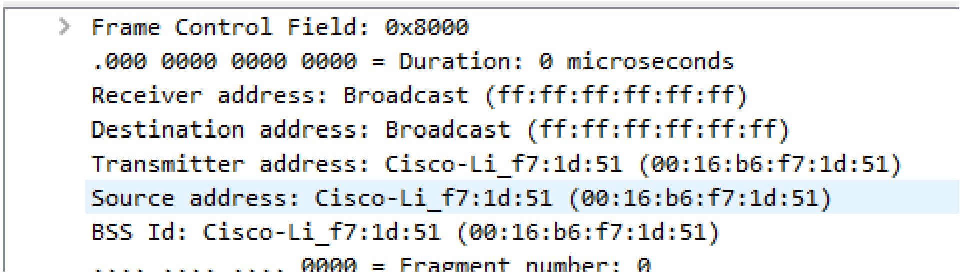
```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e6 9c   ·····X·· ········
```

2. **What are the intervals of time between the transmission of the beacon frames the *linksys_ses_24086* access point? From the *30 Munroe St*. access point? (Hint: this interval of time is contained in the beacon frame itself).**

The beacon interval for both access points in the Beacon Interval of the 802.11 wireless LAN Management frame as 100 milliseconds.

3. **What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 6.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).**

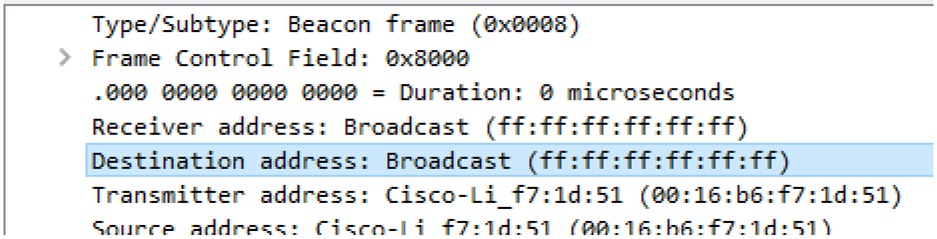
The source MAC address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51 .



```
> 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
```

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

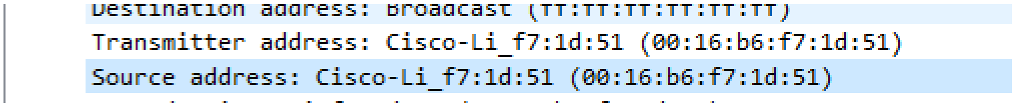
The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff



```
  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)
```

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

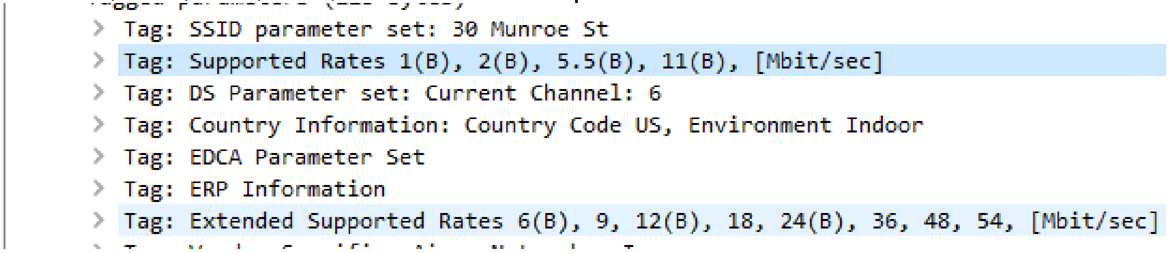
The MAC BSS ID address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51



```
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)
```

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?**

The support rates are 1.0, 2.0, 5.5, 11.0 Mbps. The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 Mbps.



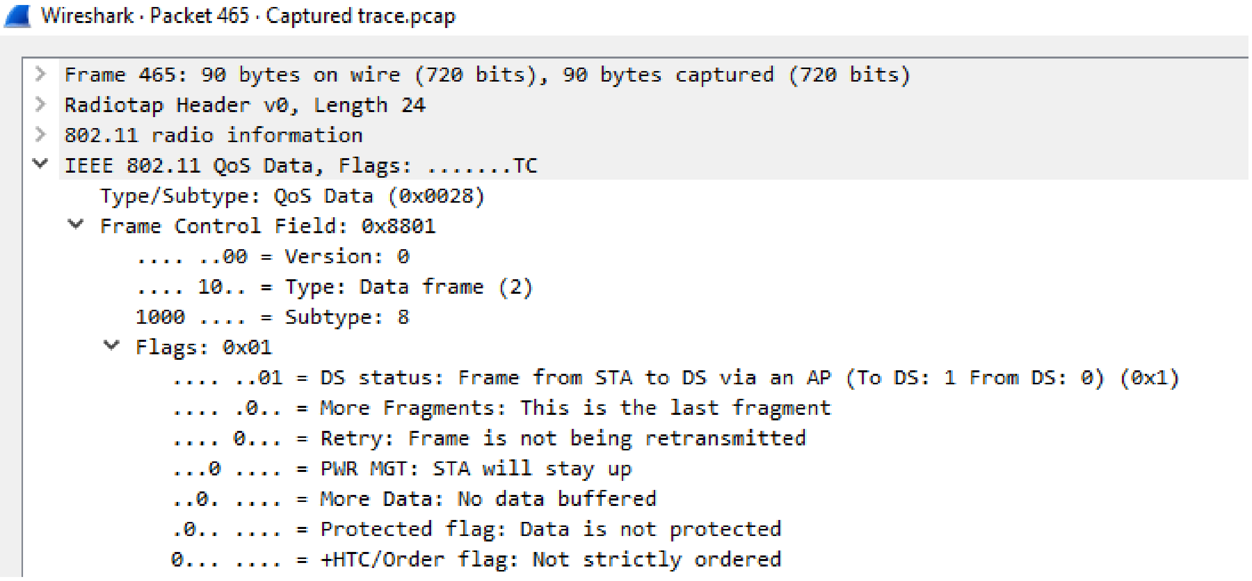
```
> Tag: SSID parameter set: 30 Munroe St
> Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
> Tag: DS Parameter set: Current Channel: 6
> Tag: Country Information: Country Code US, Environment Indoor
> Tag: EDCA Parameter Set
> Tag: ERP Information
> Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
```

3. Data Transfer

Since the trace starts with the host already associated with the AP, let first look at data transfer over an 802.11 association before looking at AP association/disassociation. Recall that in this trace, at *t = 24.82*, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark- labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12. Then, at *t=32.82,* the host makes an HTTP request to http://www.cs.umass.edu.

7. **Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). At what time is the TCP SYN sent? What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain. (Hint: review Figure 5.19 in the text if you are unsure of how to answer this question, or the corresponding part of the next question. It's particularly important that you understand this).**

Those MAC addresses are BSSid, source address and destination.
The MAC address corresponds to the wireless host is 00:13:02:d1:b6:4f.
Corresponding to the first hop router is 00:16:b6:f4:eb:a8.
Corresponding to the wireless host sending this TCP segment is 00:16:b6:f7:1d:51.
The corresponding IP of the wireless host is 192.168.1.109.
The destination IP is 128.199.245.12 and this IP is corresponds to the host.



Wireshark · Packet 465 · Captured trace.pcap

```
> Frame 465: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
     Type/Subtype: QoS Data (0x0028)
   v Frame Control Field: 0x8801
          .... ..00 = Version: 0
          .... 10.. = Type: Data frame (2)
          1000 .... = Subtype: 8
        v Flags: 0x01
               .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
               .... .0.. = More Fragments: This is the last fragment
               .... 0... = Retry: Frame is not being retransmitted
               ...0 .... = PWR MGT: STA will stay up
               ..0. .... = More Data: No data buffered
               .0.. .... = Protected flag: Data is not protected
               0... .... = +HTC/Order flag: Not strictly ordered
```

8. **Find the 802.11 frame containing the SYNACK segment for this TCP session. At what time is the TCP SYNACK received? What are three MAC address fields in the 802.11 frame containing the SYNACK? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram?**

The TCP SYNACK is received at t = 24.827751 sec, into the trace. The MAC address for the sender of the 802.11 frame containing the TCP SYNACK segment is 00:16:b6:f4:eb:a8, which is the 1st hop router to which the host is attached .

The MAC address for the destination, is 91:2a:b0:49:b6:4f.

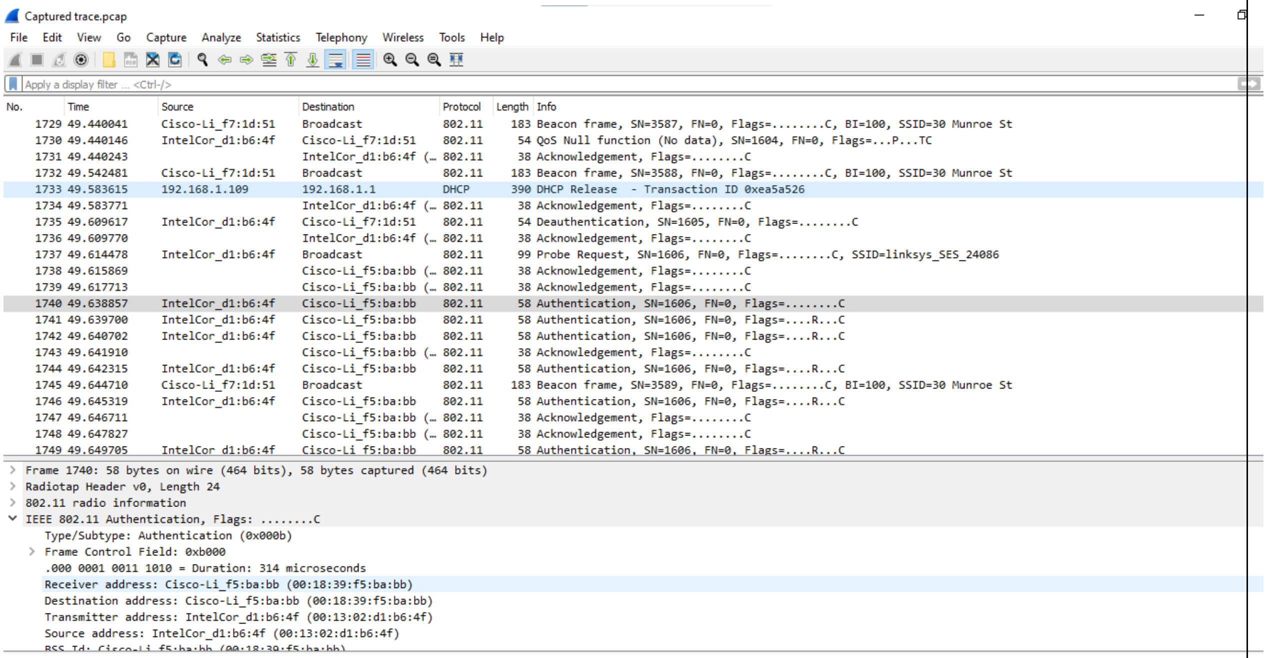
3. Association/Disassociation

A host must first *associate* with an access point before sending data. Association in 802.11 is performed using the ASSOCIATE REQUEST frame (sent from host to AP, with a frame type 0) and the ASSOCIATE RESPONSE frame (sent by the AP to a host with a frame type 0 and subtype of 1, in response to a received ASSOCIAT REQUEST). For a detailed explanation of each field in the 802.11 frame, see page 34 (Section 7) of the 802.11 spec at http://gaia.cs.umass.edu/wireshark-labs/802.111999.pdf.

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, and at what times are these frames sent? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?**

The DHCP is sent to 192.168.1.1

The host sends a DEAUTHENTICATION frame after 0.02s

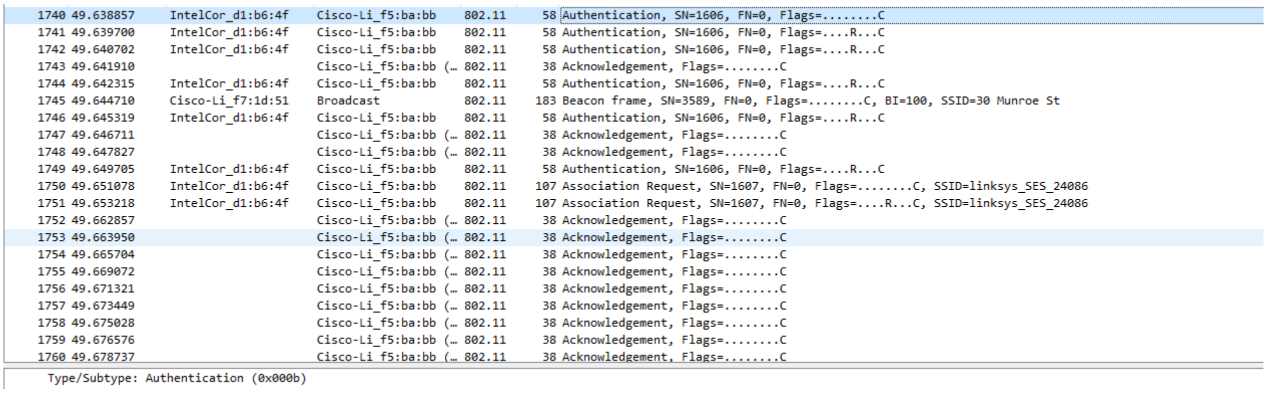

Captured trace.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source             Destination          Protocol Length Info
 1729 49.440041  Cisco-Li_f7:1d:51  Broadcast            802.11   183 Beacon frame, SN=3587, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1730 49.440146  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51    802.11    54 QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
 1731 49.440243                     IntelCor_d1:b6:4f (… 802.11    38 Acknowledgement, Flags=........C
 1732 49.542481  Cisco-Li_f7:1d:51  Broadcast            802.11   183 Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1733 49.583615  192.168.1.109      192.168.1.1          DHCP     390 DHCP Release  - Transaction ID 0xea5a526
 1734 49.583771                     IntelCor_d1:b6:4f (… 802.11    38 Acknowledgement, Flags=........C
 1735 49.609617  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51    802.11    54 Deauthentication, SN=1605, FN=0, Flags=........C
 1736 49.609770                     IntelCor_d1:b6:4f (… 802.11    38 Acknowledgement, Flags=........C
 1737 49.614478  IntelCor_d1:b6:4f  Broadcast            802.11    99 Probe Request, SN=1606, FN=0, Flags=........C, SSID=linksys_SES_24086
 1738 49.615869                     Cisco-Li_f5:ba:bb (… 802.11    38 Acknowledgement, Flags=........C
 1739 49.617713                     Cisco-Li_f5:ba:bb (… 802.11    38 Acknowledgement, Flags=........C
 1740 49.638857  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0, Flags=........C
 1741 49.639700  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0, Flags=....R...C
 1742 49.640702  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0, Flags=....R...C
 1743 49.641910                     Cisco-Li_f5:ba:bb (… 802.11    38 Acknowledgement, Flags=........C
 1744 49.642315  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0, Flags=....R...C
 1745 49.644710  Cisco-Li_f7:1d:51  Broadcast            802.11   183 Beacon frame, SN=3589, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1746 49.645319  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0, Flags=....R...C
 1747 49.646711                     Cisco-Li_f5:ba:bb (… 802.11    38 Acknowledgement, Flags=........C
 1748 49.647827                     Cisco-Li_f5:ba:bb (… 802.11    38 Acknowledgement, Flags=........C
 1749 49.649705  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0, Flags=....R...C
```

```
> Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb000
    .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)
```

10. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. When is the first AUTHENTICATION frame sent from the wireless host to the *linksys_ses_24086* AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around *t=49?* .

The first AUTHENTICATION from the host to the AP is at t = 49.638857.

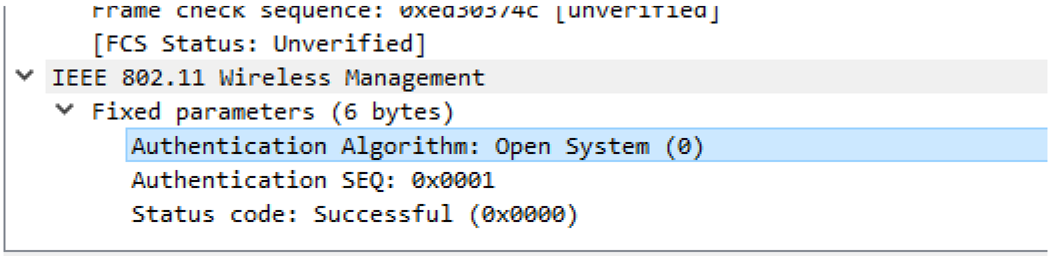


```
1740 49.638857  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11   58 Authentication, SN=1606, FN=0, Flags=........C
1741 49.639700  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1742 49.640702  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1743 49.641910                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1744 49.642315  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1745 49.644710  Cisco-Li_f7:1d:51  Broadcast            802.11  183 Beacon frame, SN=3589, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1746 49.645319  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1747 49.646711                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1748 49.647827                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1749 49.649705  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11   58 Authentication, SN=1606, FN=0, Flags=....R...C
1750 49.651078  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11  107 Association Request, SN=1607, FN=0, Flags=........C, SSID=linksys_SES_24086
1751 49.653218  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11  107 Association Request, SN=1607, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1752 49.662857                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1753 49.663950                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1754 49.665704                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1755 49.669072                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1756 49.671321                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1757 49.673449                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1758 49.675028                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1759 49.676576                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C
1760 49.678737                     Cisco-Li_f5:ba:bb (… 802.11   38 Acknowledgement, Flags=........C

    Type/Subtype: Authentication (0x000b)
```

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

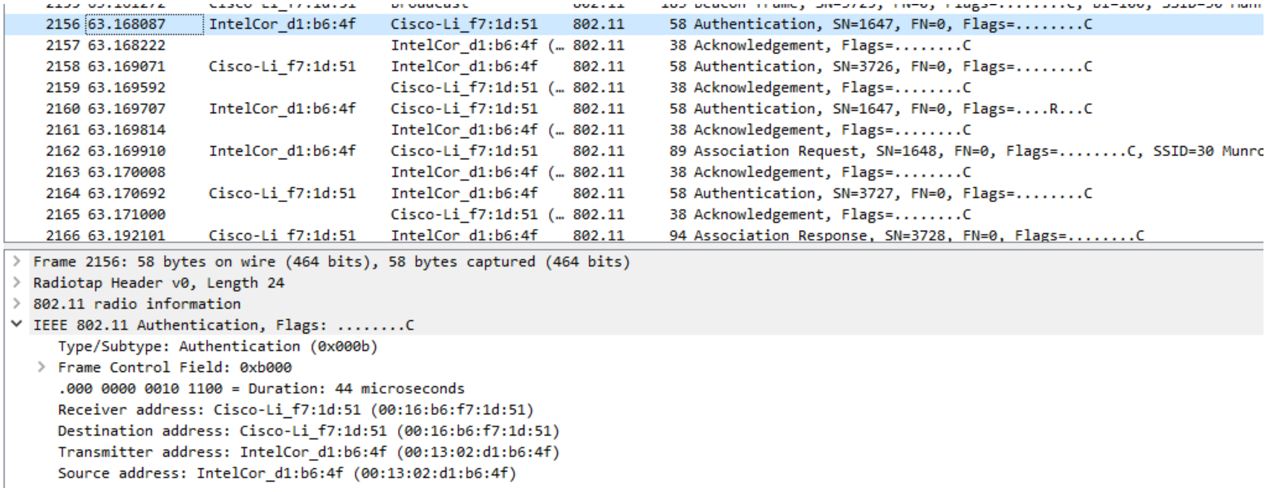
Open



```
        Frame check sequence: 0xed30374c [unverified]
        [FCS Status: Unverified]
  IEEE 802.11 Wireless Management
      Fixed parameters (6 bytes)
          Authentication Algorithm: Open System (0)
          Authentication SEQ: 0x0001
          Status code: Successful (0x0000)
```

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

No



```
2155 63.161272  Cisco-Li_f7:1d:51  Broadcast            802.11  183 Beacon frame, SN=3725, FN=0, Flags=........C, BI=100, SSID=30 Munr
2156 63.168087  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51    802.11   58 Authentication, SN=1647, FN=0, Flags=........C
2157 63.168222                     IntelCor_d1:b6:4f (… 802.11   38 Acknowledgement, Flags=........C
2158 63.169071  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f    802.11   58 Authentication, SN=3726, FN=0, Flags=........C
2159 63.169592                     Cisco-Li_f7:1d:51 (… 802.11   38 Acknowledgement, Flags=........C
2160 63.169707  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51    802.11   58 Authentication, SN=1647, FN=0, Flags=....R...C
2161 63.169814                     IntelCor_d1:b6:4f (… 802.11   38 Acknowledgement, Flags=........C
2162 63.169910  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51    802.11   89 Association Request, SN=1648, FN=0, Flags=........C, SSID=30 Munro
2163 63.170008                     IntelCor_d1:b6:4f (… 802.11   38 Acknowledgement, Flags=........C
2164 63.170692  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f    802.11   58 Authentication, SN=3727, FN=0, Flags=........C
2165 63.171000                     Cisco-Li_f7:1d:51 (… 802.11   38 Acknowledgement, Flags=........C
2166 63.192101  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f    802.11   94 Association Response, SN=3728, FN=0, Flags=........C
```

```
> Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 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)
```

13. Now let's consider what happens as the host gives up (sometime after *t* = 63.0) trying to associate with the *linksys_ses_24086* AP and now tries to associate with the *30 Munroe St* AP. Look for AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the *30 Munroe St.* AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

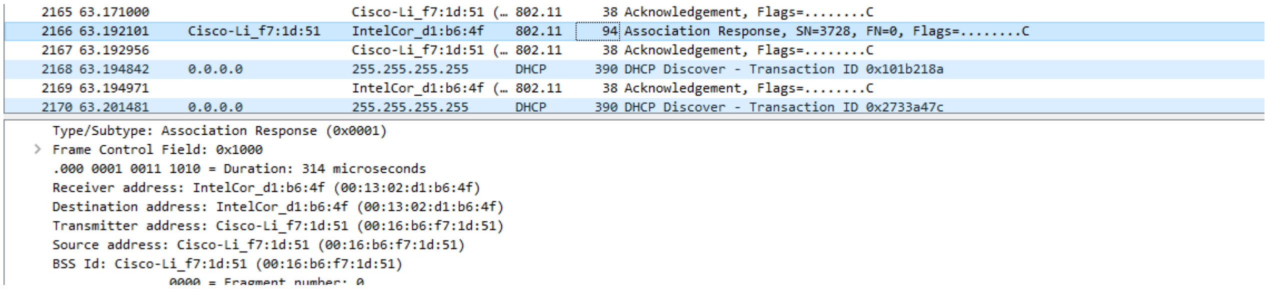
There is an AUTHENTICATION frame from 00:13:02:d1:b6:4f to 00:16:b7:f7:1d:51 when t = 63.168087. The AUTHENTICATION sent back at t = 63.169071.

14. Let’s continue on with the association between the wireless host and the *30 Munroe St* AP that happens after *t* = 63.0. An ASSOCIATE from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the *30 Munroe St* AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression “wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr IntelCor_d1:b6:4f” to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE

frames for this trace.)

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

replied at t = 63.192101.

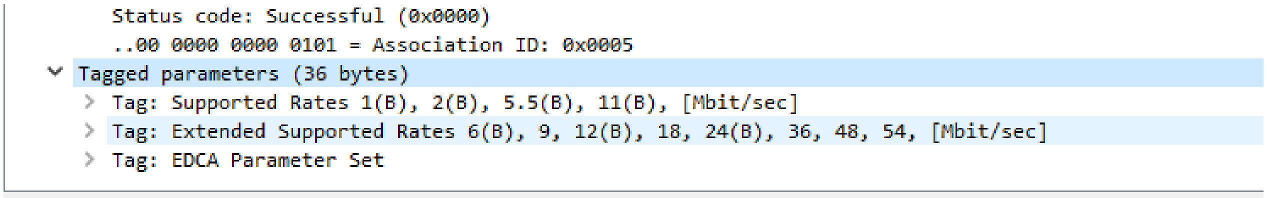


```
   2165 63.171000                      Cisco-Li_f7:1d:51 (… 802.11      38 Acknowledgement, Flags=........C
   2166 63.192101     Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f    802.11      94 Association Response, SN=3728, FN=0, Flags=........C
   2167 63.192956                      Cisco-Li_f7:1d:51 (… 802.11      38 Acknowledgement, Flags=........C
   2168 63.194842     0.0.0.0          255.255.255.255      DHCP       390 DHCP Discover - Transaction ID 0x101b218a
   2169 63.194971                      IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   2170 63.201481     0.0.0.0          255.255.255.255      DHCP       390 DHCP Discover - Transaction ID 0x2733a47c

     Type/Subtype: Association Response (0x0001)
   > Frame Control Field: 0x1000
     .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
```

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.

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



```
      Status code: Successful (0x0000)
      ..00 0000 0000 0101 = Association ID: 0x0005
  ⌄ 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
```

4. Other Frame types

Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.

16. Consider the first PROBE REQUEST and the soonest subsequent PROBE RESPONSE PAIR occurs after *t* = 2.0 seconds in the trace. When are these frames sent and what are the sender, receiver and BSS ID MAC addresses for these frames? What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).

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.