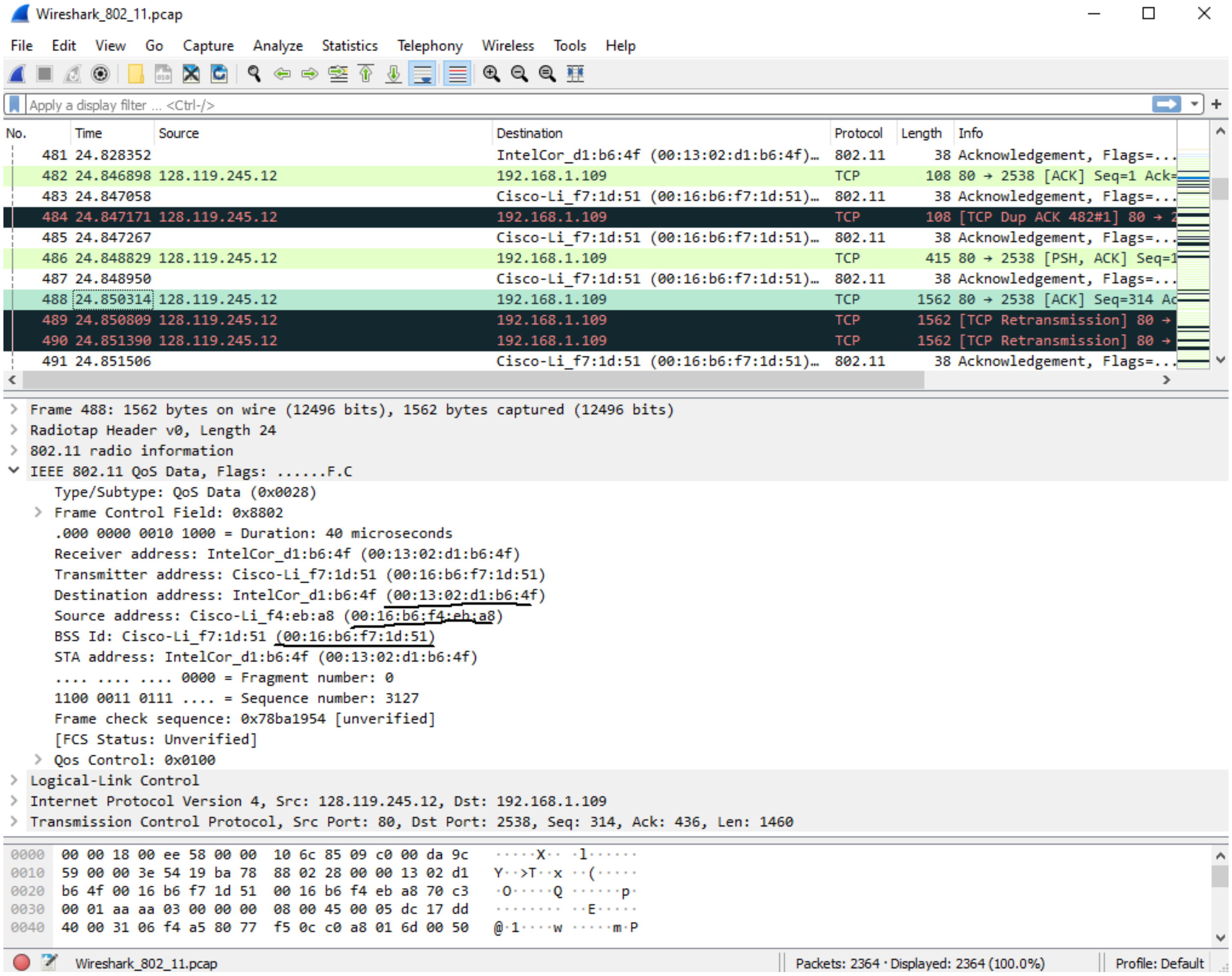
Frank, March 23, 2020

# COMPSCI-4C03 Lab Assignment 6

## Question 1: Understanding 802.11

### #1-A:



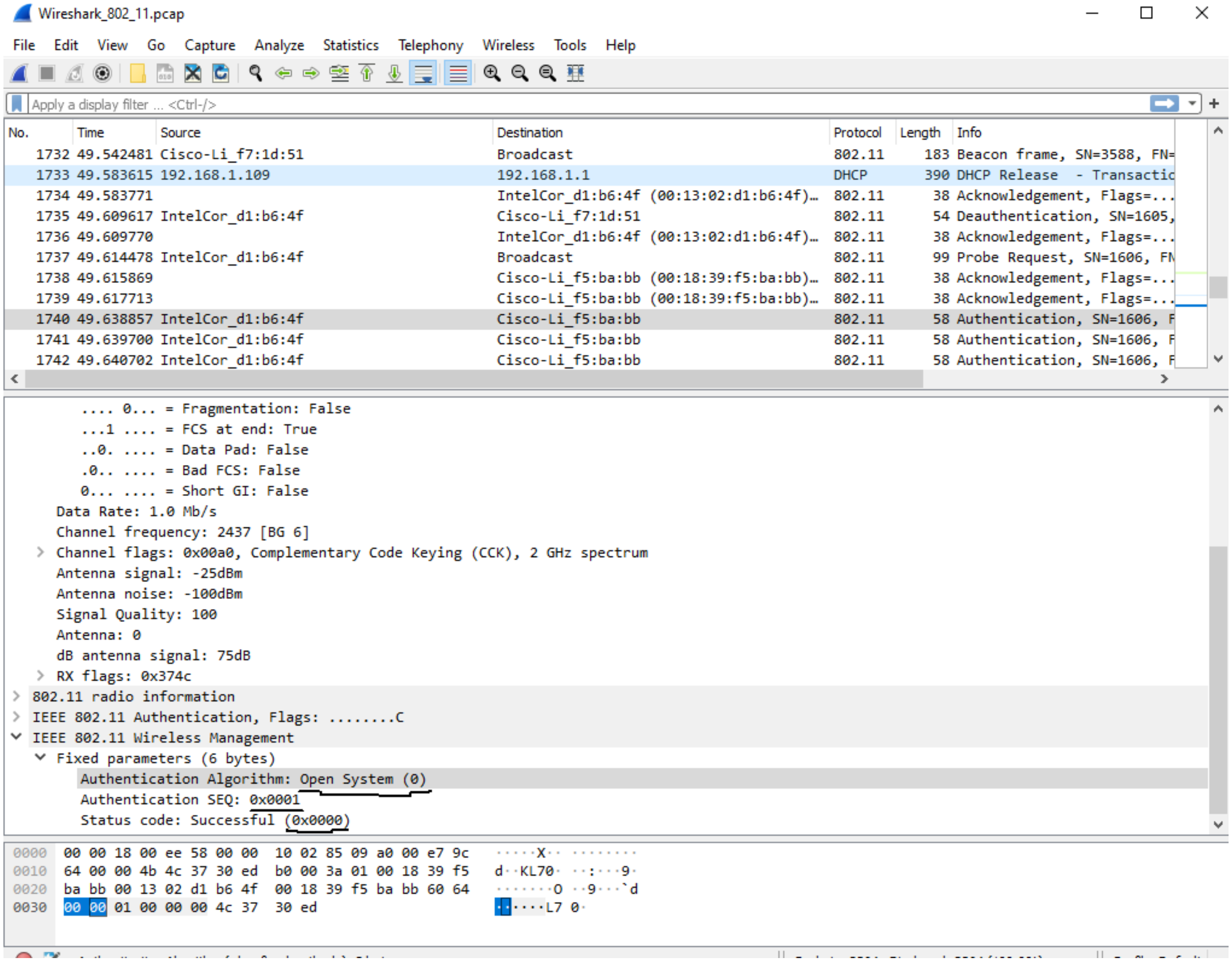
```
No.  Time      Source          Destination                                    Protocol Length Info
 481 24.828352                 IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)…          802.11     38 Acknowledgement, Flags=...
 482 24.846898 128.119.245.12  192.168.1.109                                  TCP       108 80 → 2538 [ACK] Seq=1 Ack=
 483 24.847058                 Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)…          802.11     38 Acknowledgement, Flags=...
 484 24.847171 128.119.245.12  192.168.1.109                                  TCP       108 [TCP Dup ACK 482#1] 80 → 2
 485 24.847267                 Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)…          802.11     38 Acknowledgement, Flags=...
 486 24.848829 128.119.245.12  192.168.1.109                                  TCP       415 80 → 2538 [PSH, ACK] Seq=1
 487 24.848950                 Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)…          802.11     38 Acknowledgement, Flags=...
 488 24.850314 128.119.245.12  192.168.1.109                                  TCP      1562 80 → 2538 [ACK] Seq=314 Ac
 489 24.850809 128.119.245.12  192.168.1.109                                  TCP      1562 [TCP Retransmission] 80 →
 490 24.851390 128.119.245.12  192.168.1.109                                  TCP      1562 [TCP Retransmission] 80 →
 491 24.851506                 Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)…          802.11     38 Acknowledgement, Flags=...
```

```
> Frame 488: 1562 bytes on wire (12496 bits), 1562 bytes captured (12496 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: ......F.C
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8802
    .000 0000 0010 1000 = Duration: 40 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1: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: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0111 .... = Sequence number: 3127
    Frame check sequence: 0x78ba1954 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0100
> Logical-Link Control
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
> Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 314, Ack: 436, Len: 1460
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 da 9c   ·····X·· ·l······
0010  59 00 00 3e 54 19 ba 78  88 02 28 00 00 13 02 d1   Y··>T··x ··(·····
0020  b6 4f 00 16 b6 f7 1d 51  00 16 b6 f4 eb a8 70 c3   ·O·····Q ······p·
0030  00 01 aa aa 03 00 00 00  08 00 45 00 05 dc 17 dd   ········ ··E·····
0040  40 00 31 06 f4 a5 80 77  f5 0c c0 a8 01 6d 00 50   @·1····w ·····m·P
```

As seen in the screenshot above, the 802.11 frame that contains the SYN TCP segment for the first TCP section is frame 488, being sent at t = 24.811093 seconds into the trace. The MAC address for the host is: **00:13:02:d1:b6:4f**. The destination IP address corresponds to the first-hop router, and has a MAC address of: **00:16:b6:f4:eb:a8.** This address also is the address for the gaia.cs.umass.edu servers. The destination MAC address of the frame containing the SYN is different from the destination address of the IP packet contained in this frame. Finally, the MAC address for the BSS is: **00:16:b6:f7:1d:51.**

## #1-B:



Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source              Destination                                Protocol Length Info
1732 49.542481 Cisco-Li_f7:1d:51   Broadcast                                  802.11   183 Beacon frame, SN=3588, FN=
1733 49.583615 192.168.1.109       192.168.1.1                                DHCP     390 DHCP Release  - Transactic
1734 49.583771                     IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)…     802.11    38 Acknowledgement, Flags=...
1735 49.609617 IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51                          802.11    54 Deauthentication, SN=1605,
1736 49.609770                     IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)…     802.11    38 Acknowledgement, Flags=...
1737 49.614478 IntelCor_d1:b6:4f   Broadcast                                  802.11    99 Probe Request, SN=1606, FN
1738 49.615869                     Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)…     802.11    38 Acknowledgement, Flags=...
1739 49.617713                     Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)…     802.11    38 Acknowledgement, Flags=...
1740 49.638857 IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb                          802.11    58 Authentication, SN=1606, F
1741 49.639700 IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb                          802.11    58 Authentication, SN=1606, F
1742 49.640702 IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb                          802.11    58 Authentication, SN=1606, F
```

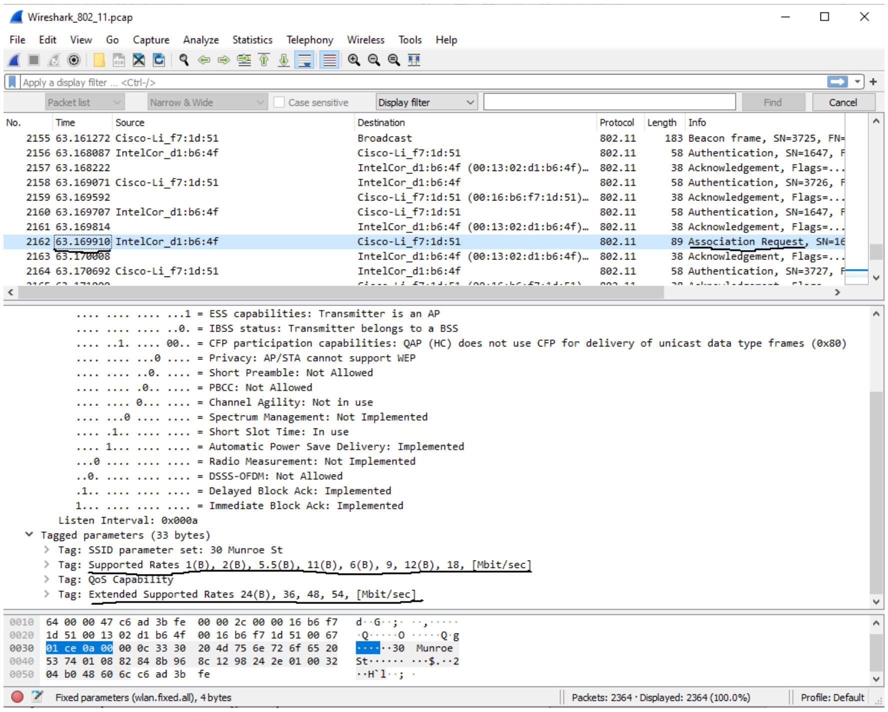
```
        .... 0... = Fragmentation: False
        ...1 .... = FCS at end: True
        ..0. .... = Data Pad: False
        .0.. .... = Bad FCS: False
        0... .... = Short GI: False
      Data Rate: 1.0 Mb/s
      Channel frequency: 2437 [BG 6]
    > Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
      Antenna signal: -25dBm
      Antenna noise: -100dBm
      Signal Quality: 100
      Antenna: 0
      dB antenna signal: 75dB
    > RX flags: 0x374c
  > 802.11 radio information
  > IEEE 802.11 Authentication, Flags: ........C
  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 18 00 ee 58 00 00  10 02 85 09 a0 00 e7 9c   ·····X·· ········
0010  64 00 00 4b 4c 37 30 ed  b0 00 3a 01 00 18 39 f5   d··KL70· ··:···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 4c 37  30 ed                     ······L7 0·
```

We find the answer in the 1733th frame in the trace. Looking at the Authentication Algorithm field, we see that it is 0, standing for open system, with an Authentication SEQ of 0x0001, as well as a Status code of 0x0000, meaning successful. Thus, the host clearly wants the authentication to be open.

## #1-C:

## Association Request Frame:


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

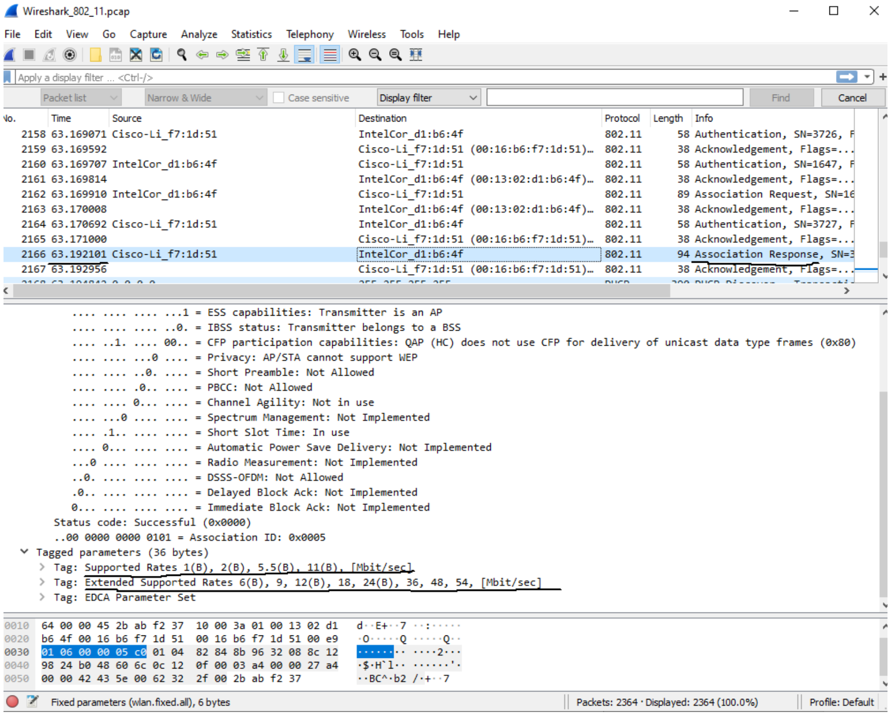
```
No.   Time      Source               Destination                            Protocol  Length  Info
 2155 63.161272 Cisco-Li_f7:1d:51    Broadcast                              802.11      183 Beacon frame, SN=3725, FN=
 2156 63.168087 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51                      802.11       58 Authentication, SN=1647, F
 2157 63.168222                      IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)… 802.11       38 Acknowledgement, Flags=...
 2158 63.169071 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f                      802.11       58 Authentication, SN=3726, F
 2159 63.169592                      Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)… 802.11       38 Acknowledgement, Flags=...
 2160 63.169707 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51                      802.11       58 Authentication, SN=1647, F
 2161 63.169814                      IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)… 802.11       38 Acknowledgement, Flags=...
 2162 63.169910 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51                      802.11       89 Association Request, SN=16
 2163 63.170008                      IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)… 802.11       38 Acknowledgement, Flags=...
 2164 63.170692 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f                      802.11       58 Authentication, SN=3727, F
```

```
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..1. .... 00.. = CFP participation capabilities: QAP (HC) does not use CFP for delivery of unicast data type frames (0x80)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..0. .... = Short Preamble: Not Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 1... .... .... = Automatic Power Save Delivery: Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .1.. .... .... .... = Delayed Block Ack: Implemented
        1... .... .... .... = Immediate Block Ack: Implemented
     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: QoS Capability
     > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

```
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··; ·
```

Fixed parameters (wlan.fixed.all), 4 bytes | Packets: 2364 · Displayed: 2364 (100.0%) | Profile: Default

## Association Response Frame:


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

```
No.   Time      Source               Destination                            Protocol  Length  Info
 2158 63.169071 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f                      802.11       58 Authentication, SN=3726, F
 2159 63.169592                      Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)… 802.11       38 Acknowledgement, Flags=...
 2160 63.169707 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51                      802.11       58 Authentication, SN=1647, F
 2161 63.169814                      IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)… 802.11       38 Acknowledgement, Flags=...
 2162 63.169910 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51                      802.11       89 Association Request, SN=16
 2163 63.170008                      IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)… 802.11       38 Acknowledgement, Flags=...
 2164 63.170692 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f                      802.11       58 Authentication, SN=3727, F
 2165 63.171000                      Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)… 802.11       38 Acknowledgement, Flags=...
 2166 63.192101 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f                      802.11       94 Association Response, SN=3
 2167 63.192956                      Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)… 802.11       38 Acknowledgement, Flags=...
```

```
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..1. .... 00.. = CFP participation capabilities: QAP (HC) does not use CFP for delivery of unicast data type frames (0x80)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..0. .... = Short Preamble: Not Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
     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
```

```
0010  64 00 00 45 2b ab f2 37  10 00 3a 01 00 13 02 d1   d··E+··7 ··:·····
0020  b6 4f 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 00 e9   ·O·····Q ·····Q··
0030  01 06 00 00 05 c0 01 04  82 84 8b 96 32 08 8c 12   ········ ····2···
0040  98 24 b0 48 60 6c 0c 12  0f 00 03 a4 00 00 27 a4   ·$·H`l·· ······'·
0050  00 00 42 43 5e 00 62 32  2f 00 2b ab f2 37         ··BC^·b2 /·+··7
```

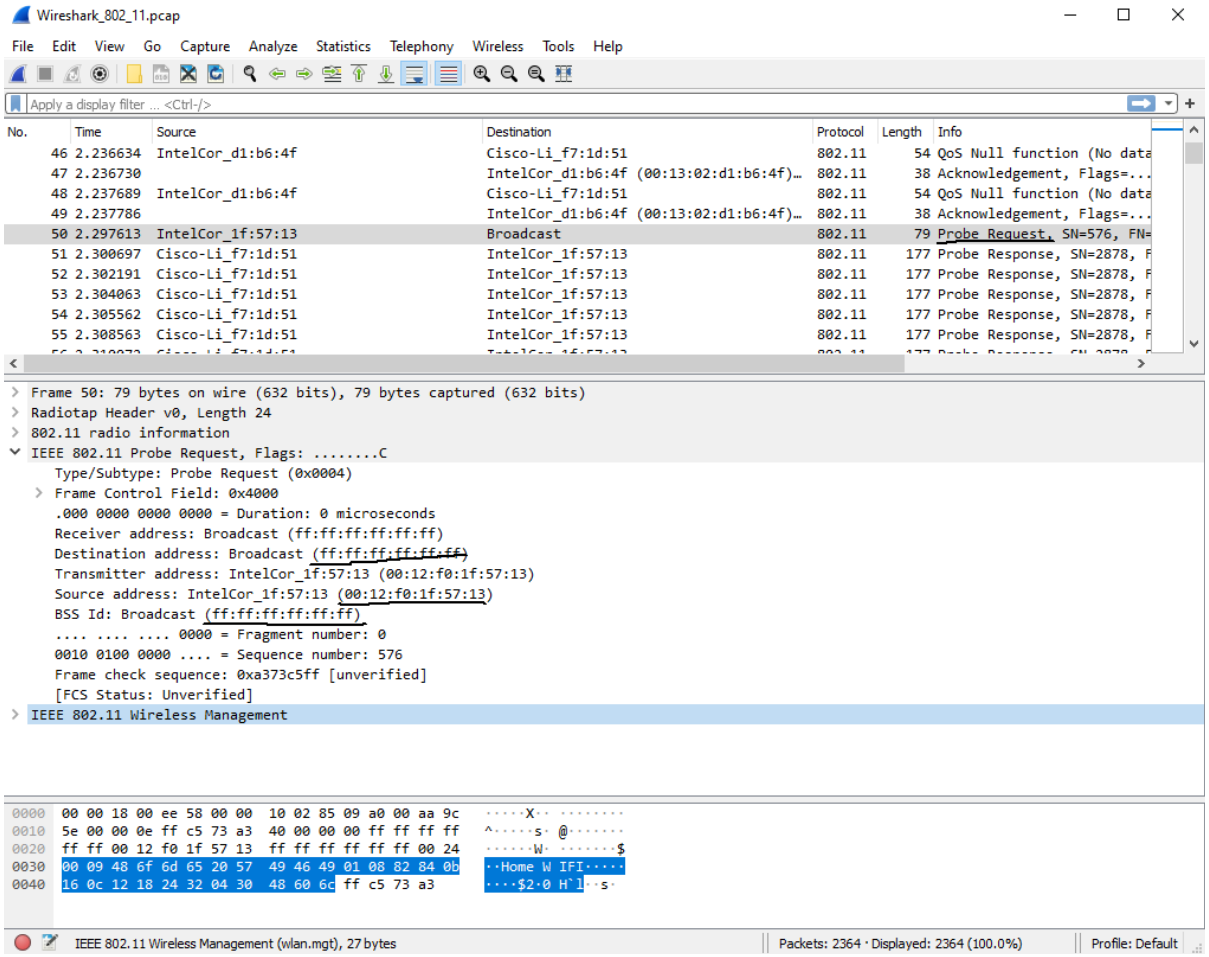
Fixed parameters (wlan.fixed.all), 6 bytes | Packets: 2364 · Displayed: 2364 (100.0%) | Profile: Default

First, we look at the Association request frame representing the transmission from host to AP. We see that the supported rates (in Mbit/sec) are: 1, 2, 5.5, 11, 6, 9, 12, and 18, with extended supported rates (in Mbit/sec) of: 24, 36, 48, and 54.

Next, we look at the Association response frame represnting the transmission from AP to host. We see that the supported rates (in Mbit/sec) are: 1, 2, 5.5, and 11, with extended supported rates (in Mbit/sec) of: 6, 9, 12, 18, 24, 36, 48, and 54.

**#1-D:**

**Probe Request:**


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source               Destination                              Protocol Length Info
   46 2.236634  IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51                        802.11      54 QoS Null function (No data
   47 2.236730                       IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)…   802.11      38 Acknowledgement, Flags=...
   48 2.237689  IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51                        802.11      54 QoS Null function (No data
   49 2.237786                       IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)…   802.11      38 Acknowledgement, Flags=...
   50 2.297613  IntelCor_1f:57:13    Broadcast                                802.11      79 Probe Request, SN=576, FN=
   51 2.300697  Cisco-Li_f7:1d:51    IntelCor_1f:57:13                        802.11     177 Probe Response, SN=2878, F
   52 2.302191  Cisco-Li_f7:1d:51    IntelCor_1f:57:13                        802.11     177 Probe Response, SN=2878, F
   53 2.304063  Cisco-Li_f7:1d:51    IntelCor_1f:57:13                        802.11     177 Probe Response, SN=2878, F
   54 2.305562  Cisco-Li_f7:1d:51    IntelCor_1f:57:13                        802.11     177 Probe Response, SN=2878, F
   55 2.308563  Cisco-Li_f7:1d:51    IntelCor_1f:57:13                        802.11     177 Probe Response, SN=2878, F
```

```
> Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  > Frame Control Field: 0x4000
    .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: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0010 0100 0000 .... = Sequence number: 576
    Frame check sequence: 0xa373c5ff [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
```

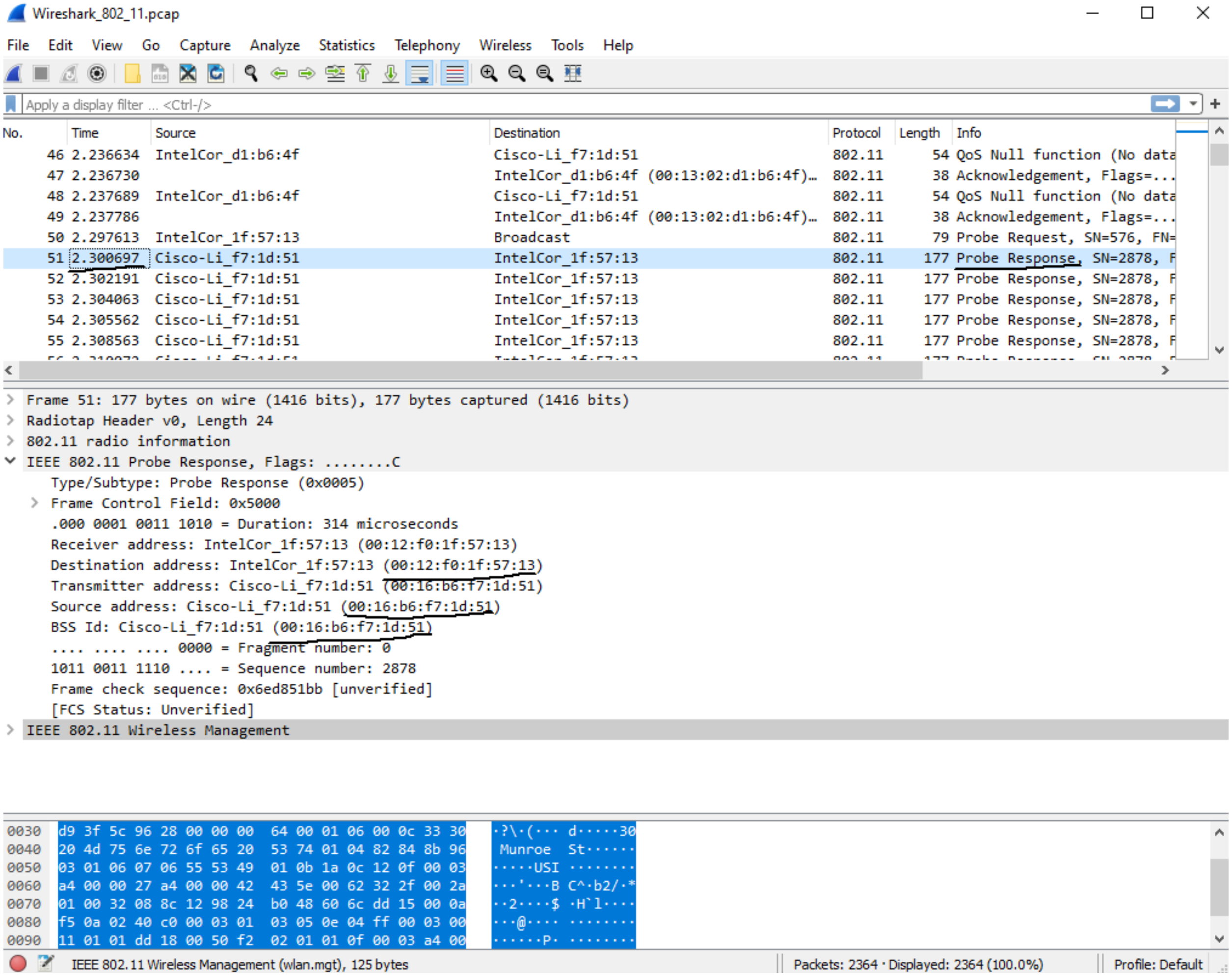
```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 aa 9c   ·····X·· ········
0010  5e 00 00 0e ff c5 73 a3  40 00 00 00 ff ff ff ff   ^·····s· @·······
0020  ff ff 00 12 f0 1f 57 13  ff ff ff ff ff ff 00 24   ······W· ·······$
0030  00 09 48 6f 6d 65 20 57  49 46 49 01 08 82 84 0b   ··Home W IFI·····
0040  16 0c 12 18 24 32 04 30  48 60 6c ff c5 73 a3      ····$2·0 H`l··s·
```

IEEE 802.11 Wireless Management (wlan.mgt), 27 bytes

Packets: 2364 · Displayed: 2364 (100.0%)

Profile: Default

**Probe Response:**


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source              Destination                           Protocol  Length Info
  46 2.236634  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51                     802.11     54 QoS Null function (No data
  47 2.236730                      IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)… 802.11     38 Acknowledgement, Flags=...
  48 2.237689  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51                     802.11     54 QoS Null function (No data
  49 2.237786                      IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)… 802.11     38 Acknowledgement, Flags=...
  50 2.297613  IntelCor_1f:57:13   Broadcast                             802.11     79 Probe Request, SN=576, FN=
  51 2.300697  Cisco-Li_f7:1d:51   IntelCor_1f:57:13                     802.11    177 Probe Response, SN=2878, F
  52 2.302191  Cisco-Li_f7:1d:51   IntelCor_1f:57:13                     802.11    177 Probe Response, SN=2878, F
  53 2.304063  Cisco-Li_f7:1d:51   IntelCor_1f:57:13                     802.11    177 Probe Response, SN=2878, F
  54 2.305562  Cisco-Li_f7:1d:51   IntelCor_1f:57:13                     802.11    177 Probe Response, SN=2878, F
  55 2.308563  Cisco-Li_f7:1d:51   IntelCor_1f:57:13                     802.11    177 Probe Response, SN=2878, F
```

```
> Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
  > Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    1011 0011 1110 .... = Sequence number: 2878
    Frame check sequence: 0x6ed851bb [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
```

```
0030  d9 3f 5c 96 28 00 00 00  64 00 01 06 00 0c 33 30   ·?\·(··· d·····30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe  St······
0050  03 01 06 07 06 55 53 49  01 0b 1a 0c 12 0f 00 03   ·····USI ········
0060  a4 00 00 27 a4 00 00 42  43 5e 00 62 32 2f 00 2a   ···'···B C^·b2/·*
0070  01 00 32 08 8c 12 98 24  b0 48 60 6c dd 15 00 0a   ··2····$ ·H`l····
0080  f5 0a 02 40 c0 00 03 01  03 05 0e 04 ff 00 03 00   ···@···· ········
0090  11 01 01 dd 18 00 50 f2  02 01 01 0f 00 03 a4 00   ······P· ········
```

```
IEEE 802.11 Wireless Management (wlan.mgt), 125 bytes    Packets: 2364 · Displayed: 2364 (100.0%)    Profile: Default
```

| Time | Frame Type | Source MAC | Destination MAC | BSS ID MAC |
|---|---|---|---|---|
| 2.297613 | Probe Request | 00:12:f0:1f:57:13 | Ff:ff:ff:ff:ff:ff | ff:ff:ff:ff:ff:ff |
| 2.300697 | Probe Response | 00:16:b6:f7:1d:51 | 00:16:b6:f7:1d:51 | 00:16:b6:f7:1d:51 |

The purpose of a probe request is so that a host can actively scan to find an access point, and a probe response is sent by said access point back to the host that was sending the request.