# Lab Exercise – 802.11

## Objective

To explore the physical layer, link layer, and management functions of 802.11. **IEEE 802.11** is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands. They are the most widely used wireless computer networking standards used in most home and office networks to allow laptops, printers, and smartphones to talk to each other and access the Internet without connecting wires. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997 and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the marketplace, each revision tends to become its own standard

## Background on capturing Wireless traffic

Unlike for the other labs, it may be difficult to gather your own trace, for several reasons. The main issue is that Windows lacks driver support to gather 802.11 frames for most wireless NICs. When we captured traffic previously, the operating system made it appear to come via a wired Ethernet (even if it actually came via a wireless network) and discarded any 802.11 frames without a higher layer data payload (such as Acknowledgements).

On some systems, typically Mac and Linux, it is possible to tell the operating system to gather 802.11 frames directly, without this conversion. This is called “Monitor mode”. If your system supports it, then the Wireshark capture options for your wireless interface will allow you to select Monitor mode, and to set the format of captured traffic to “802.11 plus radiotap header” rather than Ethernet. An example is shown below. If there is no way to select Monitor mode then your system likely cannot capture 802.11.

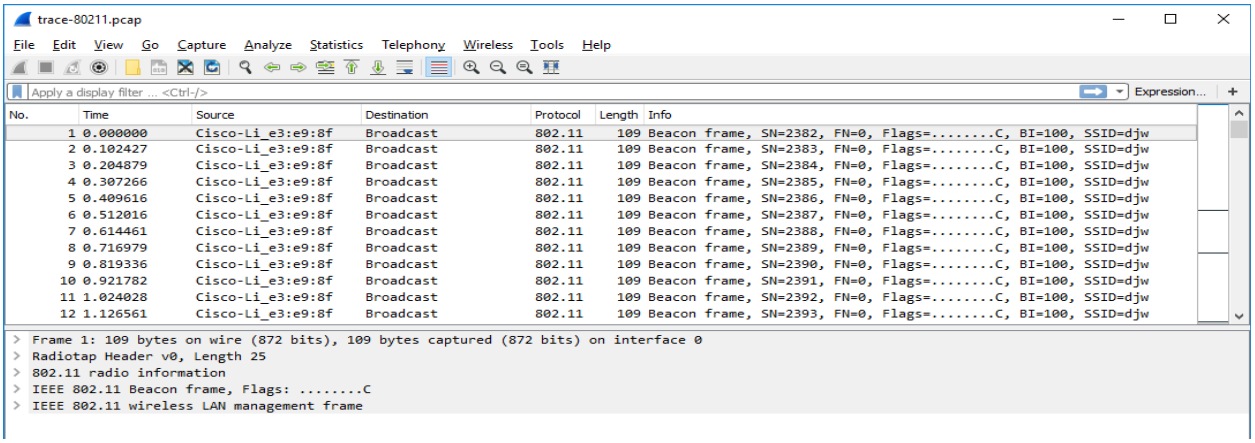
A second difficulty is that when an interface captures wireless traffic in monitor mode, it is often not available for regular use. This means that you need at least two computers: one computer to send test traffic and a second monitor computer to capture a trace of wireless activity.

Finally, note that capturing a trace in monitor mode will record all wireless activity in the vicinity. Since 802.11 wireless devices are pervasive, it is likely that your trace will capture unwanted traffic from other nearby computers. This behavior makes it difficult to cleanly observe your own traffic.

## Step 1: Inspect a Trace

**1. Open the sample trace at: https://kevincurran.org/com320/labs/wireshark/trace-80211.pcap**

You should see a screen as follows.

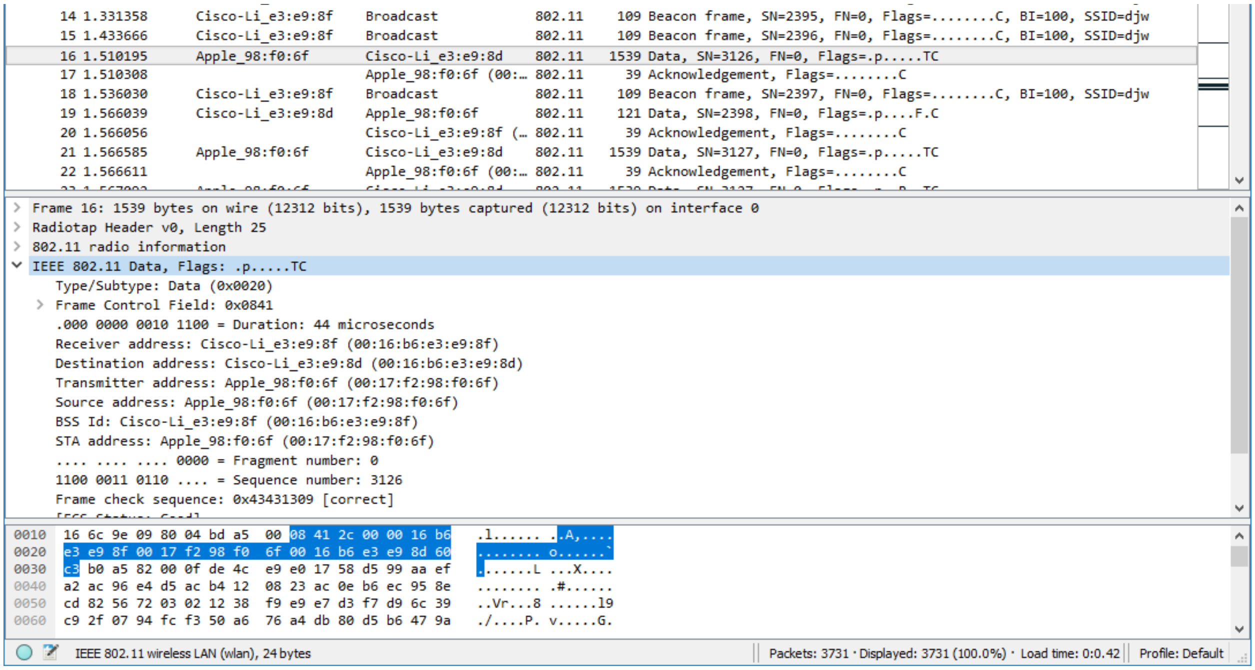

trace-80211.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.     Time        Source              Destination         Protocol  Length  Info
      1 0.000000    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2382, FN=0, Flags=........C, BI=100, SSID=djw
      2 0.102427    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2383, FN=0, Flags=........C, BI=100, SSID=djw
      3 0.204879    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2384, FN=0, Flags=........C, BI=100, SSID=djw
      4 0.307266    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2385, FN=0, Flags=........C, BI=100, SSID=djw
      5 0.409616    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2386, FN=0, Flags=........C, BI=100, SSID=djw
      6 0.512016    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2387, FN=0, Flags=........C, BI=100, SSID=djw
      7 0.614461    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2388, FN=0, Flags=........C, BI=100, SSID=djw
      8 0.716979    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2389, FN=0, Flags=........C, BI=100, SSID=djw
      9 0.819336    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2390, FN=0, Flags=........C, BI=100, SSID=djw
     10 0.921782    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2391, FN=0, Flags=........C, BI=100, SSID=djw
     11 1.024028    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2392, FN=0, Flags=........C, BI=100, SSID=djw
     12 1.126561    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2393, FN=0, Flags=........C, BI=100, SSID=djw

> Frame 1: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
> IEEE 802.11 wireless LAN management frame
```

Figure 1: 802.11 sample trace

We will look at the format of an 802.11 frame. There are many kinds of 802.11 frames that will be captured in a trace; the Info field describes the type, such as Beacon, Data, and Acknowledgement.

**2. Inspect the #16 Data frame, which carries packets across 802.11 networks.**

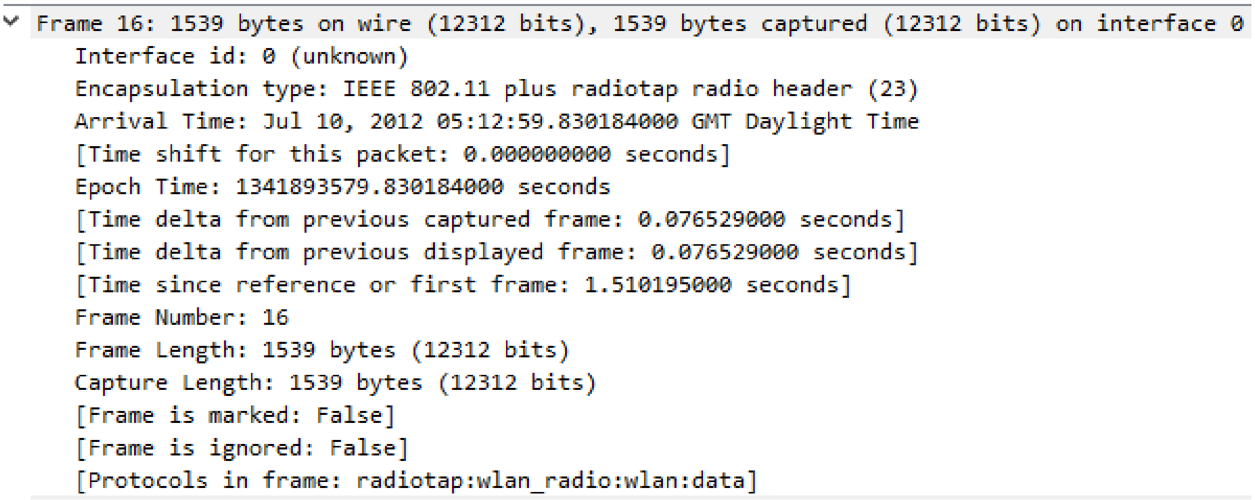


```
     14 1.331358    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2395, FN=0, Flags=........C, BI=100, SSID=djw
     15 1.433666    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2396, FN=0, Flags=........C, BI=100, SSID=djw
     16 1.510195    Apple_98:f0:6f      Cisco-Li_e3:e9:8d   802.11    1539 Data, SN=3126, FN=0, Flags=.p.....TC
     17 1.510308                        Apple_98:f0:6f (00:… 802.11     39 Acknowledgement, Flags=........C
     18 1.536030    Cisco-Li_e3:e9:8f   Broadcast           802.11     109 Beacon frame, SN=2397, FN=0, Flags=........C, BI=100, SSID=djw
     19 1.566039    Cisco-Li_e3:e9:8d   Apple_98:f0:6f      802.11     121 Data, SN=2398, FN=0, Flags=.p....F.C
     20 1.566056                        Cisco-Li_e3:e9:8f (… 802.11     39 Acknowledgement, Flags=........C
     21 1.566585    Apple_98:f0:6f      Cisco-Li_e3:e9:8d   802.11    1539 Data, SN=3127, FN=0, Flags=.p.....TC
     22 1.566611                        Apple_98:f0:6f (00:… 802.11     39 Acknowledgement, Flags=........C

> Frame 16: 1539 bytes on wire (12312 bits), 1539 bytes captured (12312 bits) on interface 0
> Radiotap Header v0, Length 25
> 802.11 radio information
v IEEE 802.11 Data, Flags: .p.....TC
    Type/Subtype: Data (0x0020)
  > Frame Control Field: 0x0841
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_e3:e9:8f (00:16:b6:e3:e9:8f)
    Destination address: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
    Transmitter address: Apple_98:f0:6f (00:17:f2:98:f0:6f)
    Source address: Apple_98:f0:6f (00:17:f2:98:f0:6f)
    BSS Id: Cisco-Li_e3:e9:8f (00:16:b6:e3:e9:8f)
    STA address: Apple_98:f0:6f (00:17:f2:98:f0:6f)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0110 .... = Sequence number: 3126
    Frame check sequence: 0x43431309 [correct]

0010  16 6c 9e 09 80 04 bd a5  00 08 41 2c 00 00 16 b6   .l...... ..A,....
0020  e3 e9 8f 00 17 f2 98 f0  6f 00 16 b6 e3 e9 8d 60   ........ o......`
0030  c3 b0 a5 82 00 0f de 4c  e9 e0 17 58 d5 99 aa ef   .......L ...X....
0040  a2 ac 96 e4 d5 ac b4 12  08 23 ac 0e b6 ec 95 8e   ........ .#......
0050  cd 82 56 72 03 02 12 38  f9 e9 e7 d3 f7 d9 6c 39   ..Vr...8 ......l9
0060  c9 2f 07 94 fc f3 50 a6  76 a4 db 80 d5 b6 47 9a   ./....P. v.....G.

IEEE 802.11 wireless LAN (wlan), 24 bytes   Packets: 3731 · Displayed: 3731 (100.0%) · Load time: 0:0.42   Profile: Default
```

Figure 2: Inspecting an 802.11 Data frame

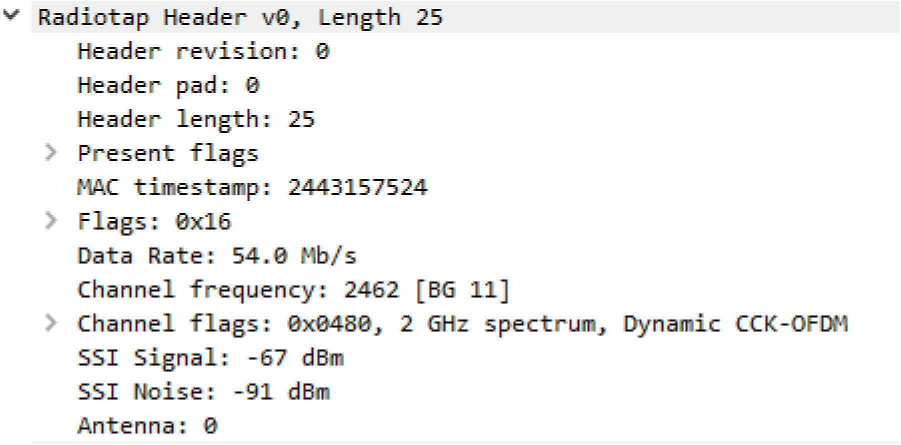
***3.* Inspect the protocol layers recorded with the frame for these protocols by looking in middle panel.**

- Frame is a record added by Wireshark with information about the time and length of the frame; it does not capture bits that were sent “over the air”.



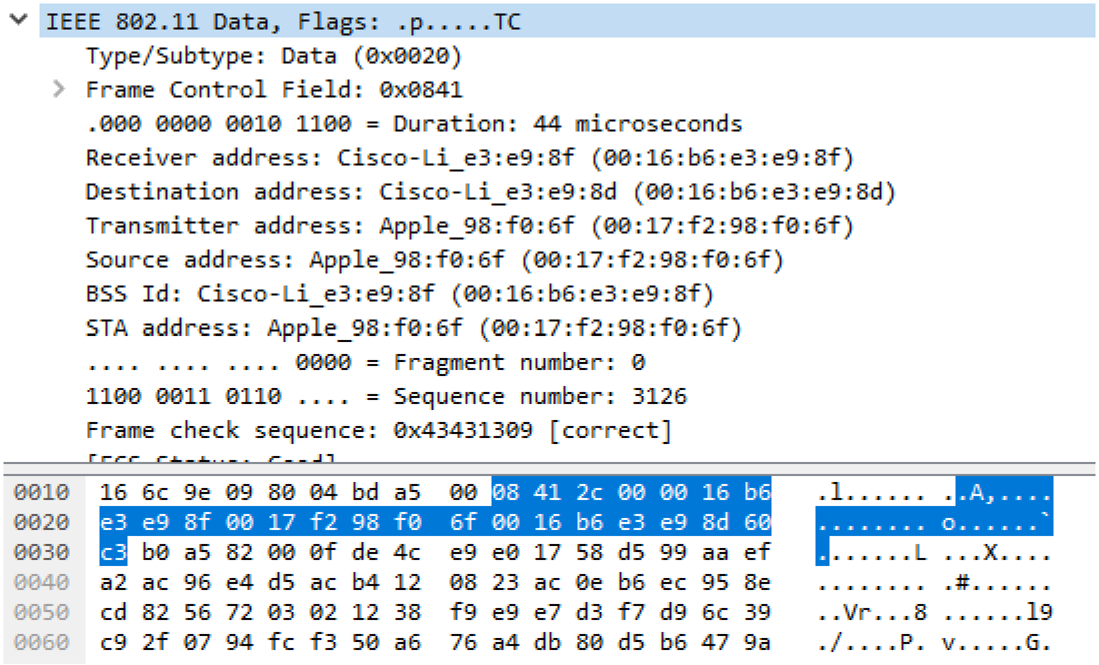
```
Frame 16: 1539 bytes on wire (12312 bits), 1539 bytes captured (12312 bits) on interface 0
   Interface id: 0 (unknown)
   Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
   Arrival Time: Jul 10, 2012 05:12:59.830184000 GMT Daylight Time
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1341893579.830184000 seconds
   [Time delta from previous captured frame: 0.076529000 seconds]
   [Time delta from previous displayed frame: 0.076529000 seconds]
   [Time since reference or first frame: 1.510195000 seconds]
   Frame Number: 16
   Frame Length: 1539 bytes (12312 bits)
   Capture Length: 1539 bytes (12312 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: radiotap:wlan_radio:wlan:data]
```

- Radiotap is also a record created by Wireshark to capture physical layer parameters, such as the strength of the signal and the modulation. Skip this record for now; we will investigate it later.



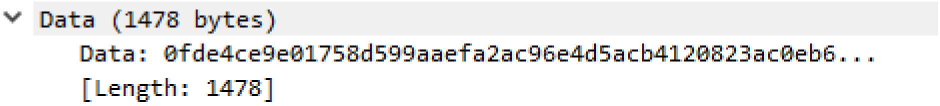
```
Radiotap Header v0, Length 25
   Header revision: 0
   Header pad: 0
   Header length: 25
 > Present flags
   MAC timestamp: 2443157524
 > Flags: 0x16
   Data Rate: 54.0 Mb/s
   Channel frequency: 2462 [BG 11]
 > Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
   SSI Signal: -67 dBm
   SSI Noise: -91 dBm
   Antenna: 0
```

- IEEE 802.11 is the bits of the 802.11 Data frame. This is the record we are looking for, and we will go into its details shortly. It is selected and expanded in the next figure so that you can see the internal fields (in the middle panel) and the portion of the frame it occupies (highlighted in the lower panel and identified at bottom as 28 bytes long).



```
IEEE 802.11 Data, Flags: .p.....TC
    Type/Subtype: Data (0x0020)
  > Frame Control Field: 0x0841
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_e3:e9:8f (00:16:b6:e3:e9:8f)
    Destination address: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
    Transmitter address: Apple_98:f0:6f (00:17:f2:98:f0:6f)
    Source address: Apple_98:f0:6f (00:17:f2:98:f0:6f)
    BSS Id: Cisco-Li_e3:e9:8f (00:16:b6:e3:e9:8f)
    STA address: Apple_98:f0:6f (00:17:f2:98:f0:6f)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0110 .... = Sequence number: 3126
    Frame check sequence: 0x43431309 [correct]
    [FCS Status: Good]

0010  16 6c 9e 09 80 04 bd a5  00 08 41 2c 00 00 16 b6   .l...... ..A,....
0020  e3 e9 8f 00 17 f2 98 f0  6f 00 16 b6 e3 e9 8d 60   ........ o......`
0030  c3 b0 a5 82 00 0f de 4c  e9 e0 17 58 d5 99 aa ef   .......L ...X....
0040  a2 ac 96 e4 d5 ac b4 12  08 23 ac 0e b6 ec 95 8e   ........ .#......
0050  cd 82 56 72 03 02 12 38  f9 e9 e7 d3 f7 d9 6c 39   ..Vr...8 ......l9
0060  c9 2f 07 94 fc f3 50 a6  76 a4 db 80 d5 b6 47 9a   ./....P. v.....G.
```

- Data is a record containing the frame payload data, i.e., that has higher-layer protocols such as LLC, IP packets, etc. Alternatively, you may see the higher-layer protocols themselves.



```
Data (1478 bytes)
    Data: 0fde4ce9e01758d599aaefa2ac96e4d5acb4120823ac0eb6...
    [Length: 1478]
```

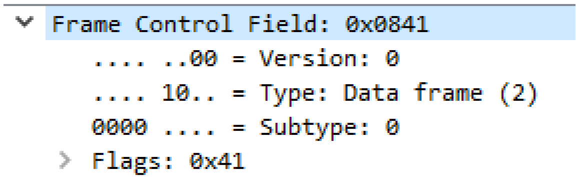
*Note that If Wireshark can understand the contents of the Data frame payload, then it will create protocol records for them. However, in many wireless settings (such as the sample trace) the payload contents are encrypted and simply appear as one record. All frames are then listed as protocol 802.11, rather than higher layer protocols such as TCP. It is possible to tell Wireshark the wireless network key and have it decrypt the payloads. However, we will skip that step since our interest is the 802.11 headers.*

**4. Expand the IEEE 802.11 record of the Data frame & inspect the details of the various header fields.**

You can expand this block using the “+” expander or icon. The fields in Wireshark are:

- Frame Control. It encodes the frame Type and Subtype, e.g., Data, as well as various flags. We will look at these fields in more detail shortly.
- Duration. This field tells computers how much time is needed on the wireless medium for additional packets that are part of this exchange.
- BSS identifier, source address, and destination address, in an order that depends on the specifics of the Data frame. These address fields identify who transmitted the packet and who should receive it. The BSS identifier is the address of the wireless access point.
- Fragment and sequence number. These fields number the frame for reassembly and retransmission, if needed. The sequence number is incremented with each new transmission.
- Frame check sequence. This is a CRC over the frame. It comes at the end (click it and you will see its position in the frame) but is listed with the other 802.11 header fields for convenience.
- There may also be a WEP or WPA2 field with security parameters in the case that the frame payload is encrypted. We are not delving into wireless security here, so you can ignore that field.

**5. Expand the Frame Control field and look at it in detail. You find within it.**



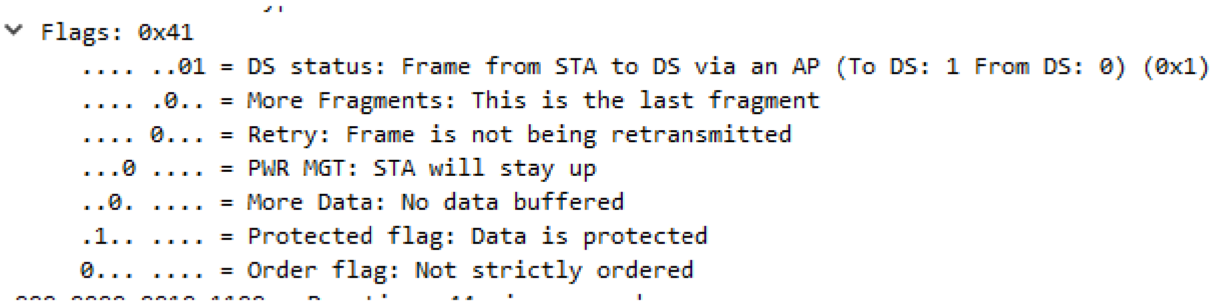
```
v Frame Control Field: 0x0841
     .... ..00 = Version: 0
     .... 10.. = Type: Data frame (2)
     0000 .... = Subtype: 0
   > Flags: 0x41
```

All 802.11 frames begin with a Frame Control field, and the details of the subfields and flags determine the format of the rest of the message; it may be like the Data frame we explored above or very different such as an Ack frame we will look at later. The subfields are:

- Version, with a value of zero for the current version.
- Type and Subtype specify the type of frame, e.g., Data or Ack.

**6. Expand the Flags field and look at it in detail. You find within it.**

- To DS. This flag is set if the frame is sent from a computer to the wired network via the AP.
- From DS. This flag is set if the frame is sent from the wired network to a computer via the AP.
- More fragments. Set if there are more frames in this message.
- Retry. Set if the frame is a retransmission.
- Power management. Set if the sender will go into power-save sleep after transmission.
- More data. Set if the sender has more frames to send.
- Protected. Set if the frame is encrypted with WEP/WPA2.
- Order. Set if the receiver must keep the frames in order.



```
v Flags: 0x41
     .... ..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
     .1.. .... = Protected flag: Data is protected
     0... .... = Order flag: Not strictly ordered
```

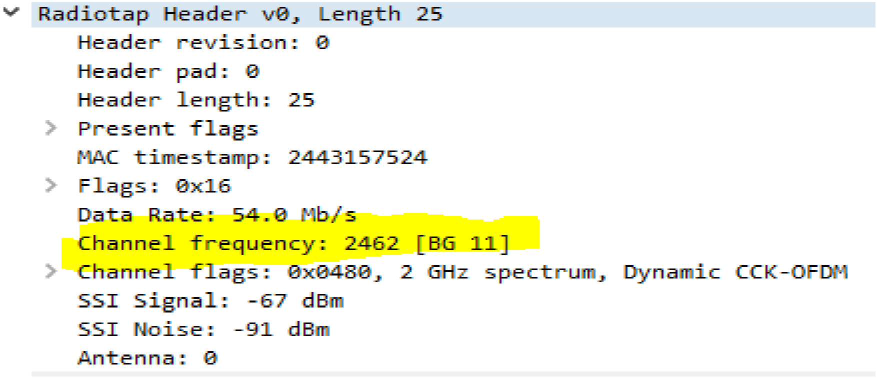
Different computers may use these flags differently depending on how they implement 802.11. For example, some computers may make heavy use of power-save or encryption features while others may not. Combined with the fact that there are dozens of different types of frames, this means that you will see all sorts of wireless traffic in most traces. Explore a bit if you are curious...

## Step 2: 802.11 Physical Layer

We will take a closer look at different parts of the wireless system, starting with the physical layer. At the lowest layer, sending and receiving messages is all about the frequency band, modulation, the signal-to-noise ratio with which the signal is received.  We can look at all these factors using information in the Radiotap header. The frequency or channel is the same for all frames in the trace, since the wireless network interface is set to listen on a fixed frequency.

**7. Find the frequency by expanding the Radiotap header of any frame & look for Channel frequency.**

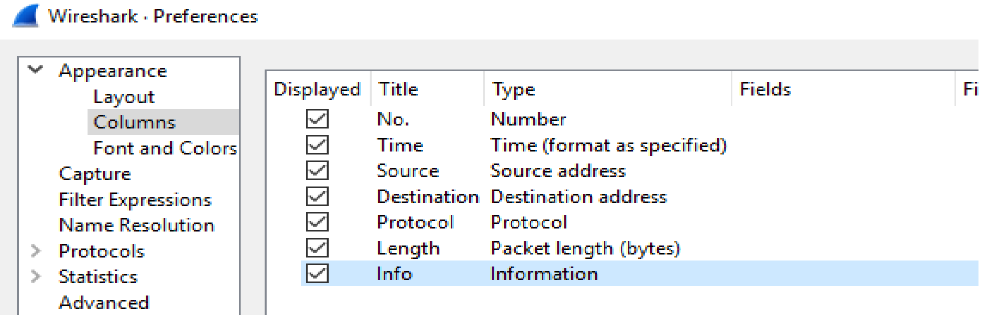
As you'll see, the Channel frequency is 2462 MHz, or 2.462 GHz. It is known as "802.11b/g channel 11".



```
v Radiotap Header v0, Length 25
     Header revision: 0
     Header pad: 0
     Header length: 25
   > Present flags
     MAC timestamp: 2443157524
   > Flags: 0x16
     Data Rate: 54.0 Mb/s
     Channel frequency: 2462 [BG 11]
   > Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
     SSI Signal: -67 dBm
     SSI Noise: -91 dBm
     Antenna: 0
```

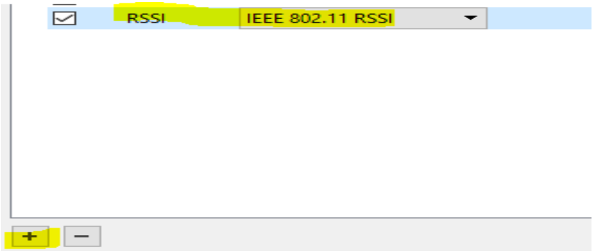
To look at the modulation we can observe the Data Rate value, and to look at the SNR we can observe the SSI Signal value (combined with the SSI Noise value). The SSI Signal value is more commonly known as the RSSI (Received Signal Strength Indication). These fields will vary with different frames. To see them, first we must add new columns to the main display.

***8. Add two new display columns for the TX Rate (or Data Rate) and RSSI (or SSI Signal value) by going to the Preferences panel (under the Edit menu) and selecting Columns (by expanding the User Interface block).***



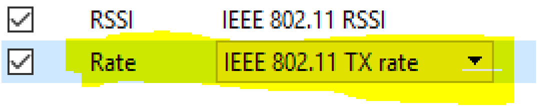
| Displayed | Title | Type | Fields | Fi |
|---|---|---|---|---|
| ☑ | No. | Number | | |
| ☑ | Time | Time (format as specified) | | |
| ☑ | Source | Source address | | |
| ☑ | Destination | Destination address | | |
| ☑ | Protocol | Protocol | | |
| ☑ | Length | Packet length (bytes) | | |
| ☑ | Info | Information | | |

*Click the + to add a new column. Change the title to RSSI and in the dropdown menu in the Type field, choose IEEE 802.11 RSSI.*



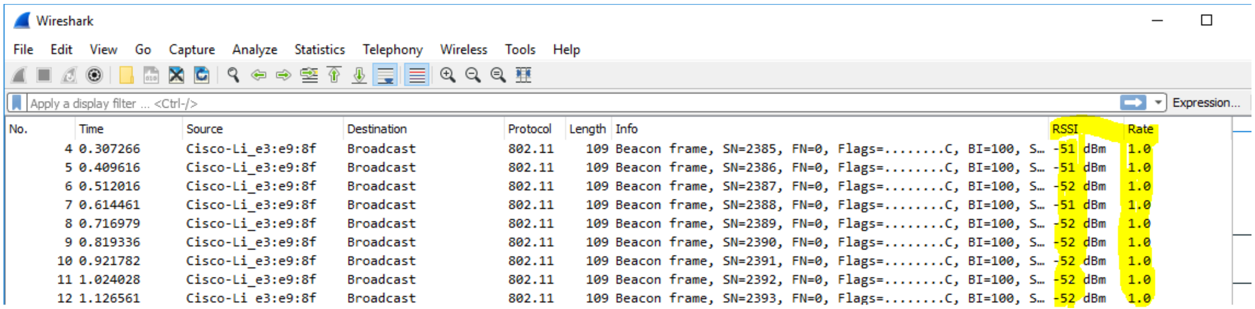
| | | |
|---|---|---|
| ☑ | RSSI | IEEE 802.11 RSSI |

*Next, click the + button again, and add a new column with the title Rate and the Type IEEE 802.11 TX rate.*



| | | |
|---|---|---|
| ☑ | RSSI | IEEE 802.11 RSSI |
| ☑ | Rate | IEEE 802.11 TX rate |

The columns in our figure are called Rate, with a field of type IEEE 802.11 TX Rate, and RSSI, with a field type of IEEE 802.11 RSSI. You may reorder the columns so that these columns are to the left of Info for visibility. When you return to the main display you will have Rate and RSSI information for each frame.



```
No.     Time      Source             Destination  Protocol  Length Info                                                        RSSI     Rate
      4 0.307266  Cisco-Li_e3:e9:8f  Broadcast    802.11       109 Beacon frame, SN=2385, FN=0, Flags=........C, BI=100, S…  -51 dBm  1.0
      5 0.409616  Cisco-Li_e3:e9:8f  Broadcast    802.11       109 Beacon frame, SN=2386, FN=0, Flags=........C, BI=100, S…  -51 dBm  1.0
      6 0.512016  Cisco-Li_e3:e9:8f  Broadcast    802.11       109 Beacon frame, SN=2387, FN=0, Flags=........C, BI=100, S…  -52 dBm  1.0
      7 0.614461  Cisco-Li_e3:e9:8f  Broadcast    802.11       109 Beacon frame, SN=2388, FN=0, Flags=........C, BI=100, S…  -51 dBm  1.0
      8 0.716979  Cisco-Li_e3:e9:8f  Broadcast    802.11       109 Beacon frame, SN=2389, FN=0, Flags=........C, BI=100, S…  -52 dBm  1.0
      9 0.819336  Cisco-Li_e3:e9:8f  Broadcast    802.11       109 Beacon frame, SN=2390, FN=0, Flags=........C, BI=100, S…  -52 dBm  1.0
     10 0.921782  Cisco-Li_e3:e9:8f  Broadcast    802.11       109 Beacon frame, SN=2391, FN=0, Flags=........C, BI=100, S…  -52 dBm  1.0
     11 1.024028  Cisco-Li_e3:e9:8f  Broadcast    802.11       109 Beacon frame, SN=2392, FN=0, Flags=........C, BI=100, S…  -52 dBm  1.0
     12 1.126561  Cisco-Li e3:e9:8f  Broadcast    802.11       109 Beacon frame, SN=2393, FN=0, Flags=........C, BI=100, S…  -52 dBm  1.0
```

Wireless trace showing Rate and RSSI for each frame

You should see a variety of rates. That is, unlike wired Ethernet for which frames are sent at a fixed rate (after negotiation of the kind of Ethernet), wireless rates vary depending on the conditions and capabilities of the computers. *The rates are 1, 6, 12, 18, 24, 38, 48, and 54 Mbps. This is most of the possible 802.11b/g rates.*

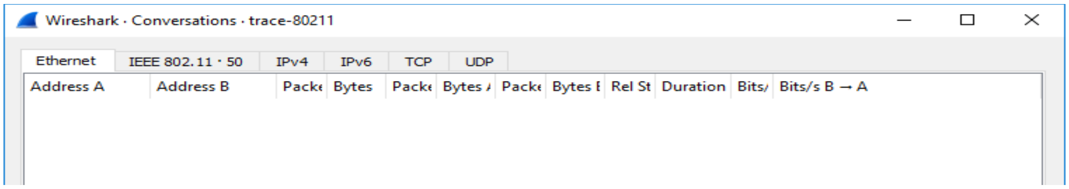
You should also see a variety of RSSI values, such as "-60 dBm". RSSI is measured on a log scale in which 0 dBm means 1 milliWatt of power and each +10 means a factor of 10 larger and each -10 means a factor of 10 smaller. Thus -60 dBm means one million-th of 1 mW, or $10^{-9}$ Watts, a tiny amount of power.

The SNR is the signal level relative to the noise level, a roughly fixed value given in the Radiotap header to be -90 dBm. These values add or subtract on the logarithmic scale. Thus a signal level of -60 dBm is 30 dB or a factor of 1000 larger than the noise level of -90 dBm. This means a frame with an RSSI of -60 dBm has an SNR of 30 dB. RSSIs may vary greatly, which means that some frames will have a much weaker or stronger signal than other frames. Variations of 40 dB are common, meaning that one frame may be 10,000 times weaker or stronger than another frame received by the same network interface.

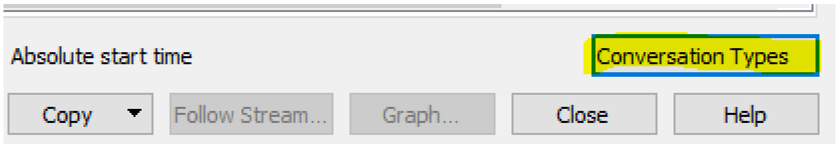
Note also how the RSSIs range from -44 dBm (strongest) to -69 dBm (weakest signal). This is a variation of 25 dB or around a factor of 300 in the SNR.

## Step 3: 802.11 Link Layer

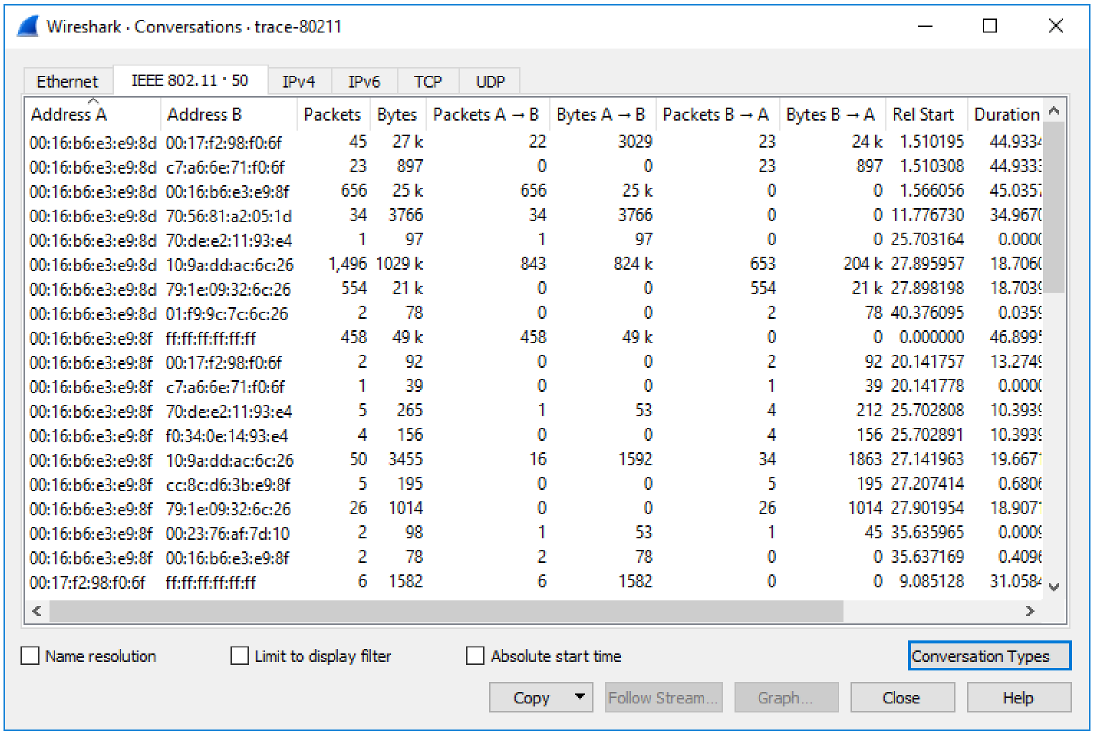
*9.* Under the **Statistics** menu, select **Conversations**. You will see a blank screen as follows.



10. In bottom right, select the **Conversation Types** button and select **802.11**



This will pull up a window like that of the figure below which lists each pair of communicating computers. You can sort this list by size by clicking on the Packets or Bytes column headings. This view will help us further explore the trace, starting with a summary of the link layer activity.



| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration |
|---|---|---|---|---|---|---|---|---|---|
| 00:16:b6:e3:e9:8d | 00:17:f2:98:f0:6f | 45 | 27 k | 22 | 3029 | 23 | 24 k | 1.510195 | 44.9334 |
| 00:16:b6:e3:e9:8d | c7:a6:6e:71:f0:6f | 23 | 897 | 0 | 0 | 23 | 897 | 1.510308 | 44.9333 |
| 00:16:b6:e3:e9:8d | 00:16:b6:e3:e9:8f | 656 | 25 k | 656 | 25 k | 0 | 0 | 1.566056 | 45.0357 |
| 00:16:b6:e3:e9:8d | 70:56:81:a2:05:1d | 34 | 3766 | 34 | 3766 | 0 | 0 | 11.776730 | 34.9670 |
| 00:16:b6:e3:e9:8d | 70:de:e2:11:93:e4 | 1 | 97 | 1 | 97 | 0 | 0 | 25.703164 | 0.0000 |
| 00:16:b6:e3:e9:8d | 10:9a:dd:ac:6c:26 | 1,496 | 1029 k | 843 | 824 k | 653 | 204 k | 27.895957 | 18.7060 |
| 00:16:b6:e3:e9:8d | 79:1e:09:32:6c:26 | 554 | 21 k | 0 | 0 | 554 | 21 k | 27.898198 | 18.7039 |
| 00:16:b6:e3:e9:8d | 01:f9:9c:7c:6c:26 | 2 | 78 | 0 | 0 | 2 | 78 | 40.376095 | 0.0359 |
| 00:16:b6:e3:e9:8f | ff:ff:ff:ff:ff:ff | 458 | 49 k | 458 | 49 k | 0 | 0 | 0.000000 | 46.8995 |
| 00:16:b6:e3:e9:8f | 00:17:f2:98:f0:6f | 2 | 92 | 0 | 0 | 2 | 92 | 20.141757 | 13.2749 |
| 00:16:b6:e3:e9:8f | c7:a6:6e:71:f0:6f | 1 | 39 | 0 | 0 | 1 | 39 | 20.141778 | 0.0000 |
| 00:16:b6:e3:e9:8f | 70:de:e2:11:93:e4 | 5 | 265 | 1 | 53 | 4 | 212 | 25.702808 | 10.3939 |
| 00:16:b6:e3:e9:8f | f0:34:0e:14:93:e4 | 4 | 156 | 0 | 0 | 4 | 156 | 25.702891 | 10.3939 |
| 00:16:b6:e3:e9:8f | 10:9a:dd:ac:6c:26 | 50 | 3455 | 16 | 1592 | 34 | 1863 | 27.141963 | 19.6671 |
| 00:16:b6:e3:e9:8f | cc:8c:d6:3b:e9:8f | 5 | 195 | 0 | 0 | 5 | 195 | 27.207414 | 0.6806 |
| 00:16:b6:e3:e9:8f | 79:1e:09:32:6c:26 | 26 | 1014 | 0 | 0 | 26 | 1014 | 27.901954 | 18.9071 |
| 00:16:b6:e3:e9:8f | 00:23:76:af:7d:10 | 2 | 98 | 1 | 53 | 1 | 45 | 35.635965 | 0.0009 |
| 00:16:b6:e3:e9:8f | 00:16:b6:e3:e9:8f | 2 | 78 | 2 | 78 | 0 | 0 | 35.637169 | 0.4096 |
| 00:17:f2:98:f0:6f | ff:ff:ff:ff:ff:ff | 6 | 1582 | 6 | 1582 | 0 | 0 | 9.085128 | 31.0584 |

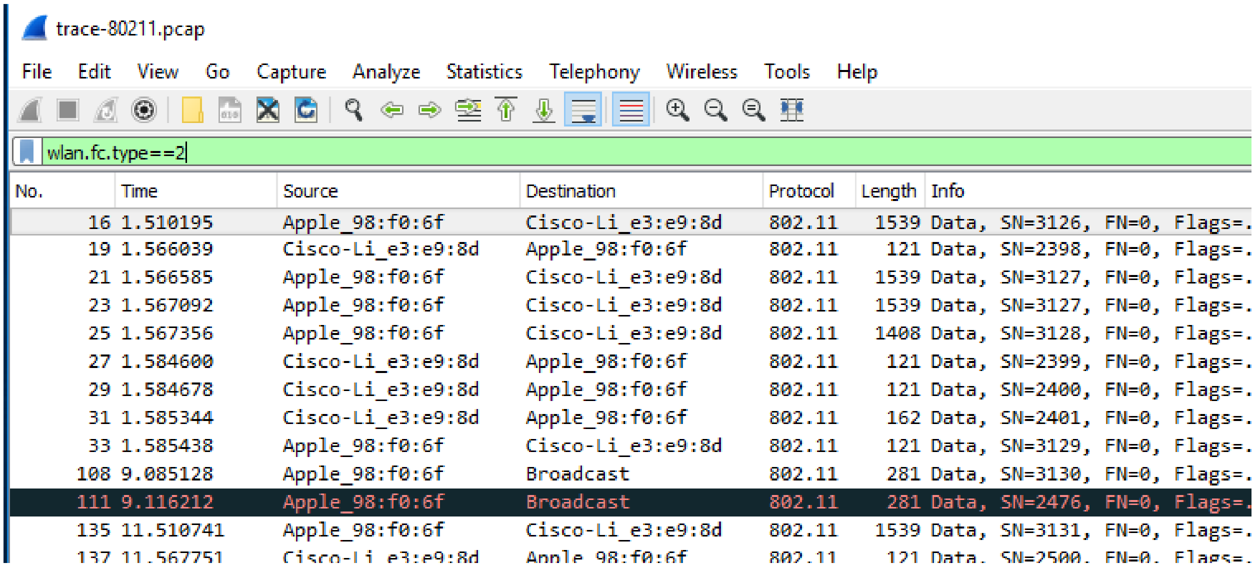
☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Most of the activity is in a relatively small fraction of the conversations. The low activity conversations are due to background traffic from idle computers, and from a small number of packets that are occasionally captured from adjacent wireless networks.

A BSS ID value identifies an AP. To find the BSS ID used by the most active wireless conversations we can sort on the source or destination address by clicking on the column heading. If you do this, you will find the most active AP has a BSS ID of 00:16:b6:e3:e9:8f.

We can also look to see the amounts we have of different types of traffic. 802.11 frames are either Data, Control, or Management frames. These frames are distinguished by the value in the Type subfield of the Frame Control field.  You can inspect different packets to see the values for different types of frames.

*To Filter to see only Data frames, we can enter the expression* "`wlan.fc.type==2`" *into the Filter box above the list of frames in the top panel.* Do this by returning to main menu and entering the filter as shown below.



wlan.fc.type==2

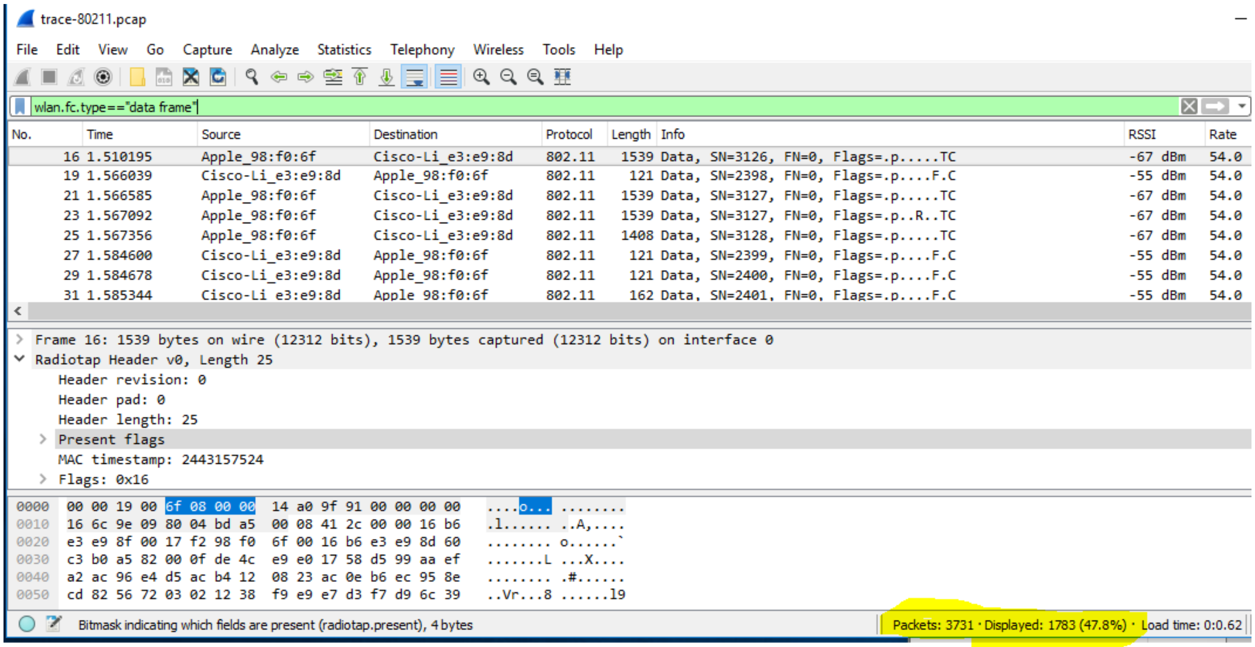
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 16 | 1.510195 | Apple_98:f0:6f | Cisco-Li_e3:e9:8d | 802.11 | 1539 | Data, SN=3126, FN=0, Flags=. |
| 19 | 1.566039 | Cisco-Li_e3:e9:8d | Apple_98:f0:6f | 802.11 | 121 | Data, SN=2398, FN=0, Flags=. |
| 21 | 1.566585 | Apple_98:f0:6f | Cisco-Li_e3:e9:8d | 802.11 | 1539 | Data, SN=3127, FN=0, Flags=. |
| 23 | 1.567092 | Apple_98:f0:6f | Cisco-Li_e3:e9:8d | 802.11 | 1539 | Data, SN=3127, FN=0, Flags=. |
| 25 | 1.567356 | Apple_98:f0:6f | Cisco-Li_e3:e9:8d | 802.11 | 1408 | Data, SN=3128, FN=0, Flags=. |
| 27 | 1.584600 | Cisco-Li_e3:e9:8d | Apple_98:f0:6f | 802.11 | 121 | Data, SN=2399, FN=0, Flags=. |
| 29 | 1.584678 | Cisco-Li_e3:e9:8d | Apple_98:f0:6f | 802.11 | 121 | Data, SN=2400, FN=0, Flags=. |
| 31 | 1.585344 | Cisco-Li_e3:e9:8d | Apple_98:f0:6f | 802.11 | 162 | Data, SN=2401, FN=0, Flags=. |
| 33 | 1.585438 | Apple_98:f0:6f | Cisco-Li_e3:e9:8d | 802.11 | 121 | Data, SN=3129, FN=0, Flags=. |
| 108 | 9.085128 | Apple_98:f0:6f | Broadcast | 802.11 | 281 | Data, SN=3130, FN=0, Flags=. |
| 111 | 9.116212 | Apple_98:f0:6f | Broadcast | 802.11 | 281 | Data, SN=2476, FN=0, Flags=. |
| 135 | 11.510741 | Apple_98:f0:6f | Cisco-Li_e3:e9:8d | 802.11 | 1539 | Data, SN=3131, FN=0, Flags=. |
| 137 | 11.567751 | Cisco-Li_e3:e9:8d | Apple_98:f0:6f | 802.11 | 121 | Data, SN=2500, FN=0, Flags=. |

Clicking on the Type subfield tells us in the status display at bottom that Wireshark knows this field by the name wlan.fc.type. Thus, the expression to filter for Data frames with Type value 2 is "`wlan.fc.type=="data frame"`" or "`wlan.fc.type==2`".

After you apply this filter, the status line at bottom will tell you how many of the trace packets are displayed. This tells you how many Data frames there are in the trace. There may be several different kinds of Data frames depending on the value of the Subtype sub-field, as indicated in the Info column. You can click on this column heading to sort by frame type to see what kinds are prevalent.

*We can now see how many Data frames are in the trace, and what is the most common subtype of Data frame. We do this by performing the same exercise for Control (Type 1) and Management (Type 0) frames by changing the filter expression to search for a different Type value.* i.e wlan.fc.type==”data frame”.

This will let you find out how many of these frames are in the trace, and their most prevalent kinds.


trace-80211.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type=="data frame"
```

```
No.  Time      Source             Destination        Protocol Length Info                                       RSSI    Rate
  16 1.510195  Apple_98:f0:6f     Cisco-Li_e3:e9:8d  802.11   1539 Data, SN=3126, FN=0, Flags=.p.....TC   -67 dBm  54.0
  19 1.566039  Cisco-Li_e3:e9:8d  Apple_98:f0:6f     802.11    121 Data, SN=2398, FN=0, Flags=.p....F.C   -55 dBm  54.0
  21 1.566585  Apple_98:f0:6f     Cisco-Li_e3:e9:8d  802.11   1539 Data, SN=3127, FN=0, Flags=.p.....TC   -67 dBm  54.0
  23 1.567092  Apple_98:f0:6f     Cisco-Li_e3:e9:8d  802.11   1539 Data, SN=3127, FN=0, Flags=.p..R..TC   -67 dBm  54.0
  25 1.567356  Apple_98:f0:6f     Cisco-Li_e3:e9:8d  802.11   1408 Data, SN=3128, FN=0, Flags=.p.....TC   -67 dBm  54.0
  27 1.584600  Cisco-Li_e3:e9:8d  Apple_98:f0:6f     802.11    121 Data, SN=2399, FN=0, Flags=.p....F.C   -55 dBm  54.0
  29 1.584678  Cisco-Li_e3:e9:8d  Apple_98:f0:6f     802.11    121 Data, SN=2400, FN=0, Flags=.p....F.C   -55 dBm  54.0
  31 1.585344  Cisco-Li_e3:e9:8d  Apple_98:f0:6f     802.11    162 Data, SN=2401, FN=0, Flags=.p....F.C   -55 dBm  54.0

> Frame 16: 1539 bytes on wire (12312 bits), 1539 bytes captured (12312 bits) on interface 0
v Radiotap Header v0, Length 25
    Header revision: 0
    Header pad: 0
    Header length: 25
  > Present flags
    MAC timestamp: 2443157524
  > Flags: 0x16

0000  00 00 19 00 6f 08 00 00  14 a0 9f 91 00 00 00 00   ....o... ........
0010  16 6c 9e 09 80 04 bd a5  00 08 41 2c 00 00 16 b6   .l...... ..A,....
0020  e3 e9 8f 00 17 f2 98 f0  6f 00 16 b6 e3 e9 8d 60   ........ o......`
0030  c3 b0 a5 82 00 0f de 4c  e9 e0 17 58 d5 99 aa ef   .......L ...X....
0040  a2 ac 96 e4 d5 ac b4 12  08 23 ac 0e b6 ec 95 8e   ........ .#......
0050  cd 82 56 72 03 02 12 38  f9 e9 e7 d3 f7 d9 6c 39   ..Vr...8 ......l9

Bitmask indicating which fields are present (radiotap.present), 4 bytes    Packets: 3731 · Displayed: 1783 (47.8%) · Load time: 0:0.62
```

Filtering the wireless trace for Data frames

We can see there are 1783 Data frames, or 48% of the total (3731) frames. The most common Data frame is simply called “Data” with subtype 0. The fraction of Data frames will depend heavily on whether there are active data transfers during the trace; there is a small transfer during this trace.

There are 1391 Control frames or 37% of the total. The most common Control frame is the Acknowledgement frame with subtype 13. The fraction of Control frames should be comparable but likely lower than the fraction of Data frames due to Acknowledgements (as each non-broadcast Data frame is acknowledged).

As you look at these different types of frames, note their lengths. Data frames may be long, up to 1500 bytes, while Management frames are typically much shorter, and Control frames are very short. You should conclude that most of the bytes in the trace are taken up in Data frames, even though there are many other frames. This is reassuring, since the whole goal of 802.11 is to transfer data.

There are 557 Management frames or 15% of the total. The most common Management frame is the Beacon frame with subtype 8. Management frames are likely to occur at a regular background rate due to Beacons. The fraction of the trace they occupy depends on whether there are active data transfers.

If we inspect the IEEE 802.11 record of an Acknowledgement frame we should see that it has few fields compared to a Data frame, e.g., only one address, and that it is very short.

The fields are Frame Control (2 bytes), Duration (2 bytes), Receiver Address (6 bytes), and Frame Check Sequence (4 bytes).

Let us consider reliability and features such as power management. We expect that wireless transmissions are not highly reliable, like well-engineered wired transmissions, but the wireless error rate should not be very large or much of the medium would be wasted. We can estimate the retransmission rate or by checking to see how many frames have their Retry bit set in the Frame Control field. This bit indicates that a frame is a retransmission of an original.

*We can do that by using filter expressions to find the number of data frames that are originals and retransmissions.* For example, "`wlan.fc.type==2 && wlan.fc.retry==0`" will find original Data frames.

We will then find that there are 1430 original Data frames and 353 retransmission Data frames. Our estimate of the retransmission rate is 353/1430 or 25%. This is not surprising – many packets do need to be retransmitted due to errors, but packets still have a reasonable chance of correct reception.

Finally, we will look at power management. Increasingly, 802.11 client devices use power management functionality to go to a low-power sleep mode when they are finished sending or receiving traffic. Clients that are going to sleep set the Power Management flag in the Frame Control field.

*We can use a filter expression to search for frames that indicate a client is going to sleep.* You can find all frames indicating sleep with the expression "`wlan.fc.pwrmgt==1`".

You only want to consider power saving behavior in frames going from a client to the AP, as frames coming from the AP will not indicate that a client is going to sleep. These frames will have the "to DS" flag set ("`wlan.fc.tods==1`"). To search for both conditions, you can combine filter expressions with "`&&`" or "`and`".

Note that 16 out of 822 or 2% of the frames sent to the AP have their power management bit set, indicating that they are about to sleep. This is a low fraction; it would likely be higher if the trace included mobile phones or other devices that sleep more frequently, and it is likely to grow higher in the future as mobile devices make greater use of power saving technologies.

As you browse the frames that use power management, you are likely to see some unusual types. For instance, the "Null function" frame carries no data. Instead, it is sent by a client to signal sleep.

# Step 4: 802.11 Management

As well as the Data and Acknowledgment frames, we will look at several types of Management frames that are used to connect a computer to an AP so that it may send and receive messages.

## Beacon Frames

*Select a Beacon frame in your trace whose BSS ID is that of the main AP from Step 4.* Beacon frames are sent out periodically by an AP to advertise its existence and capabilities to nearby computers. The IEEE 802.11 record for this frame will be similar to the record for a Data frame that we reviewed above, with different type and subtype codes to indicate that it is a Beacon frame.

However, the payload of this frame will differ: it is an IEEE 802.11 wireless LAN management frame record. You will see that after some fixed parameters it has a series of tagged parameters that list the capabilities of the AP. These include the SSID name of the AP (a text string to go with the BSS ID), the data rates it supports, and the channel on which it is operating.

*Expand the payload of the Beacon frames to view its parameters.*

1. *The SSID of the main AP is "djw". This can be seen in the tagged parameters, or in the Info field.*

2. *To see how often Beacon frames are sent for the main AP*, you will find the Beacon interval given in the Beacon frame itself or change the Time display to be show the interval since the last frame. (Under View, select Time Display Format, and "Seconds Since Previous Displayed Packet".). Here you will find that Beacon frames are sent by the "djw" AP every 102.4 milliseconds, or a rate of roughly 10/second. Beacons show up regularly in the trace, and when there is no active data transfer they are often the main traffic.

3. The data rates that the main AP support are listed under tagged parameters. The AP supports 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. The rates are given in two tagged parameters as supported rates and extended supported rates (since there are many of them). The 1, 2, 5.5, and 11 Mbps rates are marked "B", meaning that they are 802.11b legacy rates rather than 802.11g rates.

4. *You can find the rate of the Beacon frame transmission* from the Radiotap header, or more conveniently displayed in the column you added in an earlier step. The Beacon frames for this AP are all transmitted at a rate of 1 Mbps. This is typical. A low rate is used to allow the Beacons to be received over a larger area around the AP (since a lower rate can generally be received with a weaker signal).

## Association

Once a computer has learned of an AP via a Beacon or otherwise, it must associate with the AP and possibly authenticate itself before it can use the wireless network. You will see the computer send the Association Request to the AP until it is acknowledged. If association is successful then the AP will return an Association Response, which the computer will acknowledge.  After the usual IEEE 802.11 header fields, the Association Request and Response carry information that describes the capabilities of the AP and computer, such as what rates it supports. In this way, both endpoints can know the other's abilities.

*Note the Association Request is Type 0 (Management) and Subtype 0. Association Response is Type 0 (Management) and Subtype 1*

You may also see Authentication Request and Authentication Response frames before the association. This is legacy behavior; the type of authentication is usually "Open", meaning that it provides no security. Instead, the computer and AP share a pre-configured key with WEP, and for WPA2 (the modern scheme) an 802.1X authentication dialogue happens after association using higher layer protocols.

## Probe Request/Response

Finally, we will look briefly at Probe frames. Instead of a computer waiting to learn about an AP from Beacons, a computer may probe for specific APs. A Probe Request is sent by a computer to test whether an AP with a specific SSID is nearby. If the sought after AP is nearby then it will reply with a Probe Response. Like Beacon and Association frames, each of these frames has the usual header and carries a list of parameters describing the capabilities of the computer and AP. It is common for computers to send Probe Requests for wireless networks that they have previously used to speed up connection to a known network, e.g., when a laptop has returned home for the day. Thus you may see a sequence of probes for many different SSIDs. Only the SSIDs that are present will reply.

*Note the Probe Request is Type 0 (Management) and Subtype 4. Probe Response is Type 0 (Management) and Subtype 5.*