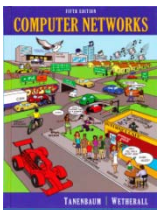
Lab Exercise – 802.11



Objective

To explore the physical layer, link layer, and management functions of 802.11. It is widely used to wireless connect mobile devices to the Internet, and covered in §4.4 of your text. Review that section first.

Requirements

Wireshark: This lab uses the Wireshark software tool to capture and examine a packet trace. A packet trace is a record of traffic at a location on the network, as if a snapshot was taken of all the bits that passed across a particular wire. The packet trace records a timestamp for each packet, along with the bits that make up the packet, from the lower-layer headers to the higher-layer contents. Wireshark runs on most operating systems, including Windows, Mac and Linux. It provides a graphical UI that shows the sequence of packets and the meaning of the bits when interpreted as protocol headers and data. It color-codes packets by their type, and has various ways to filter and analyze packets to let you investigate the behavior of network protocols. Wireshark is widely used to troubleshoot networks. You can download it from www.wireshark.org if it is not already installed on your computer. We highly recommend that you watch the short, 5 minute video "Introduction to Wireshark" that is on the site.

Step 1: Fetch a Trace

We provide a trace that you can use by starting Wireshark and selecting Open from the File menu. On Windows/Mac, you may locate the trace file and open it directly to launch Wireshark with the trace. You can now proceed to Step 2; the rest of this section is informational.

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.

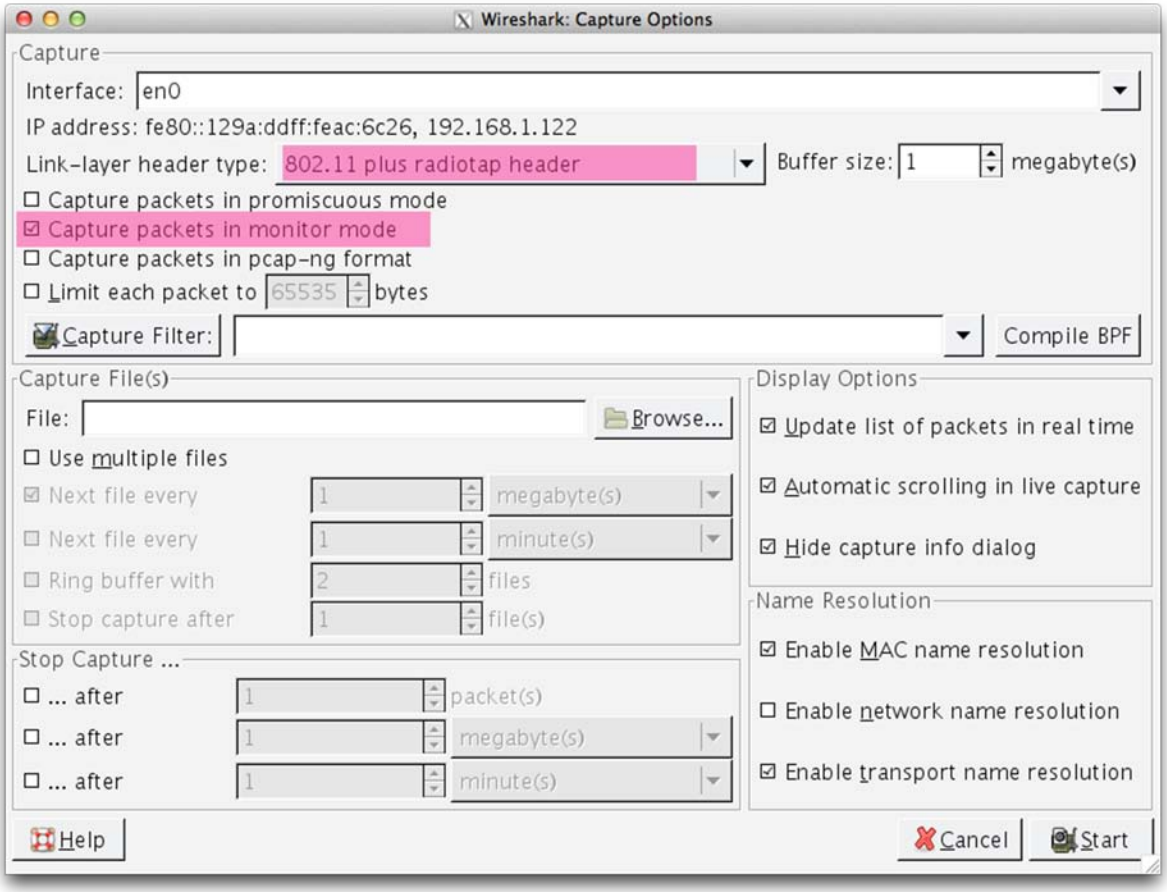


Figure 1: Capturing a wireless trace with Monitor mode (Mac)

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.

If you can handle these difficulties, you can gather your own wireless trace to do this lab.

Step 2: Inspect the Trace

To begin, we will take a look at the format of an 802.11 frame. There are many different kinds of 802.11 frames that will be captured in a trace; the Info field describes the type, such as Beacon, Data, and Acknowledgement. We will inspect a Data frame, which carries packets across 802.11 networks.

Find a Data frame in the trace and select it. Wireshark will let us select a frame (from the top panel) and view its protocol layers, in terms of both header fields (in the middle panel) and the bytes that make up the frame (in the bottom panel). You can do this simply by scrolling down until you find one, or by click-

ing on the Info column to sort by that key and then scrolling to the Data portion of the trace. We have selected a Data frame in the figure below.

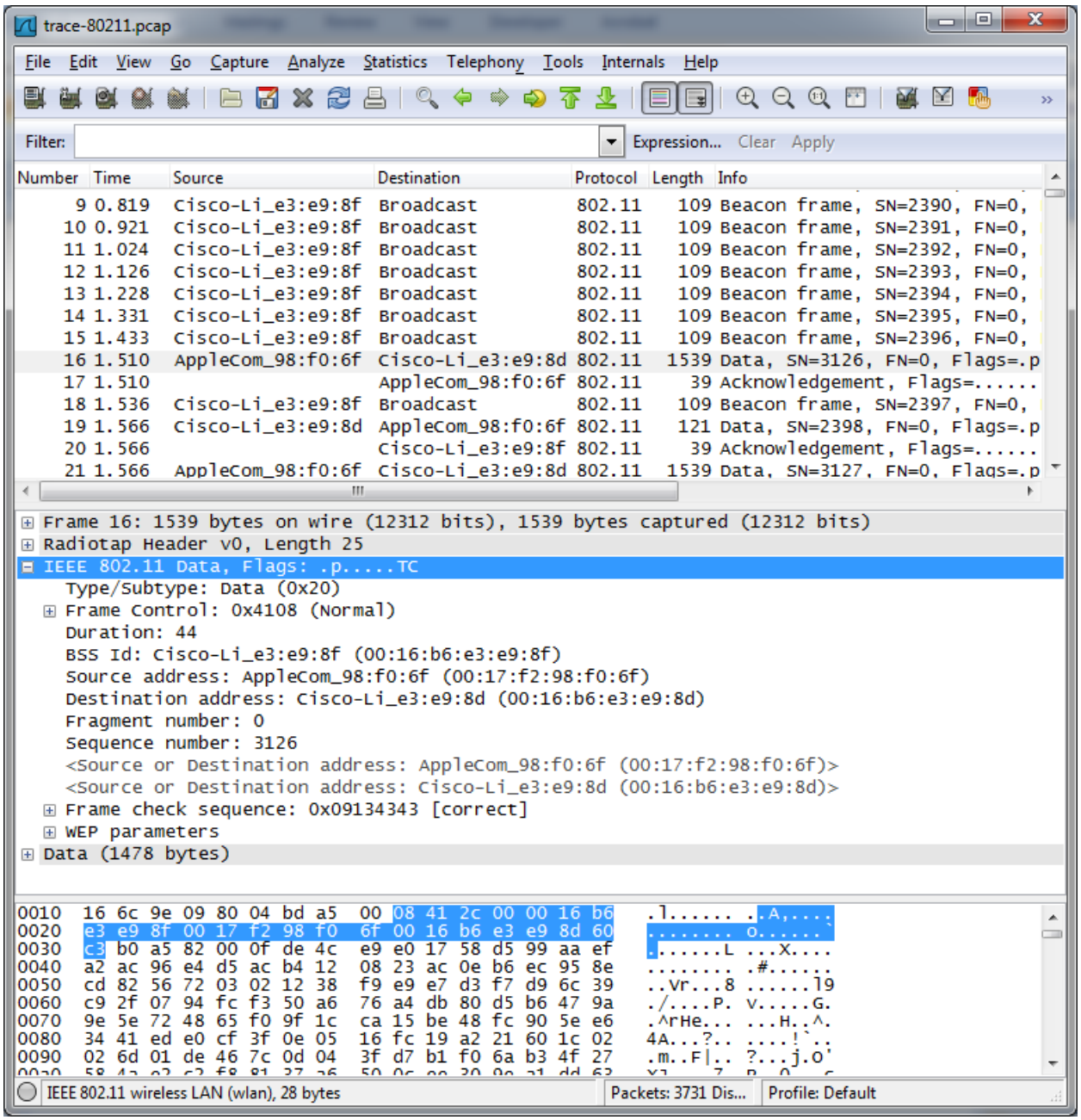


Figure 2: Inspecting an 802.11 Data frame

Inspect the protocol layers recorded with the frame for these protocols. Look in the 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".
- 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.

- 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 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).
- 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.

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.

Expand the IEEE 802.11 record of the Data frame and inspect the details of the various header fields. You can expand this block using the "+" expander or icon; it is shown expanded in our figure. To inspect the fields, you may compare them with Fig. 4-29. 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.

Finally, expand the Frame Control field and look at it in detail, including the Flags that you find within it. 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.
- 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.

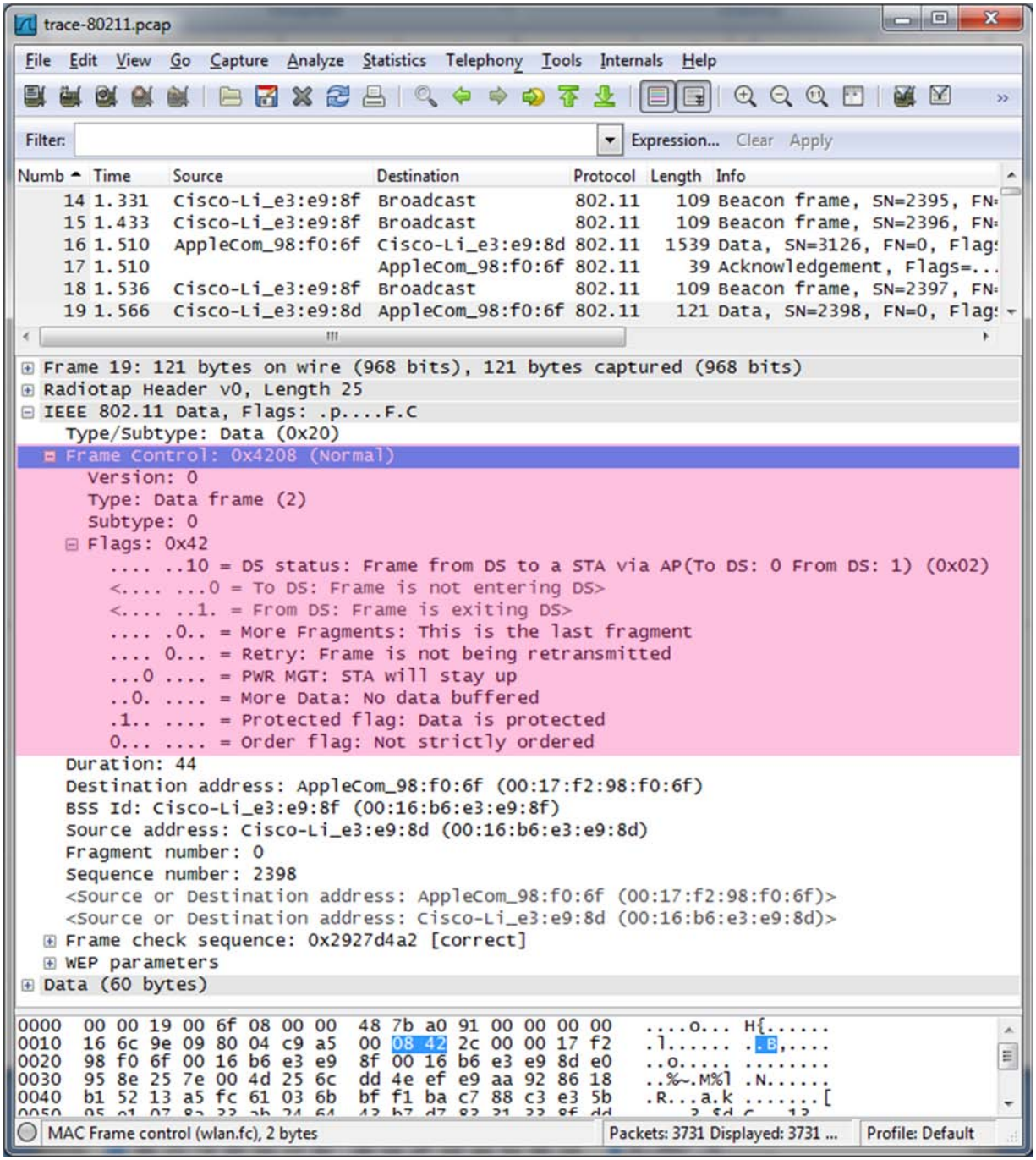


Figure3: Expanded view of the Frame Control fields and Flags

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 3: 802.11 Physical Layer

Now that we have some familiarity with 802.11 Data frames, 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 of these factors using information in the Radiotap header!

Answer the numbered questions in this step to explore the physical layer aspects, beginning with frequency. 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.

1. *What is the channel frequency?* To find the frequency, expand the Radiotap header of any frame and look for the Channel frequency.

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.

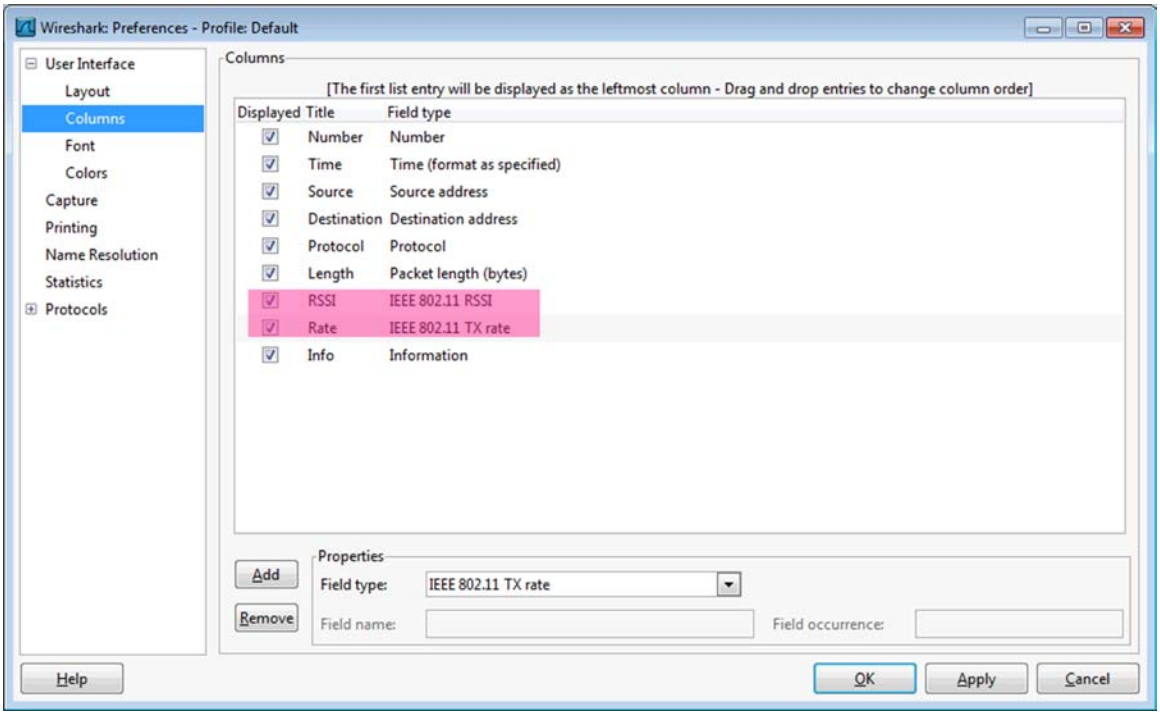


Figure 2: Adding columns for RSSI and Rate

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). 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.

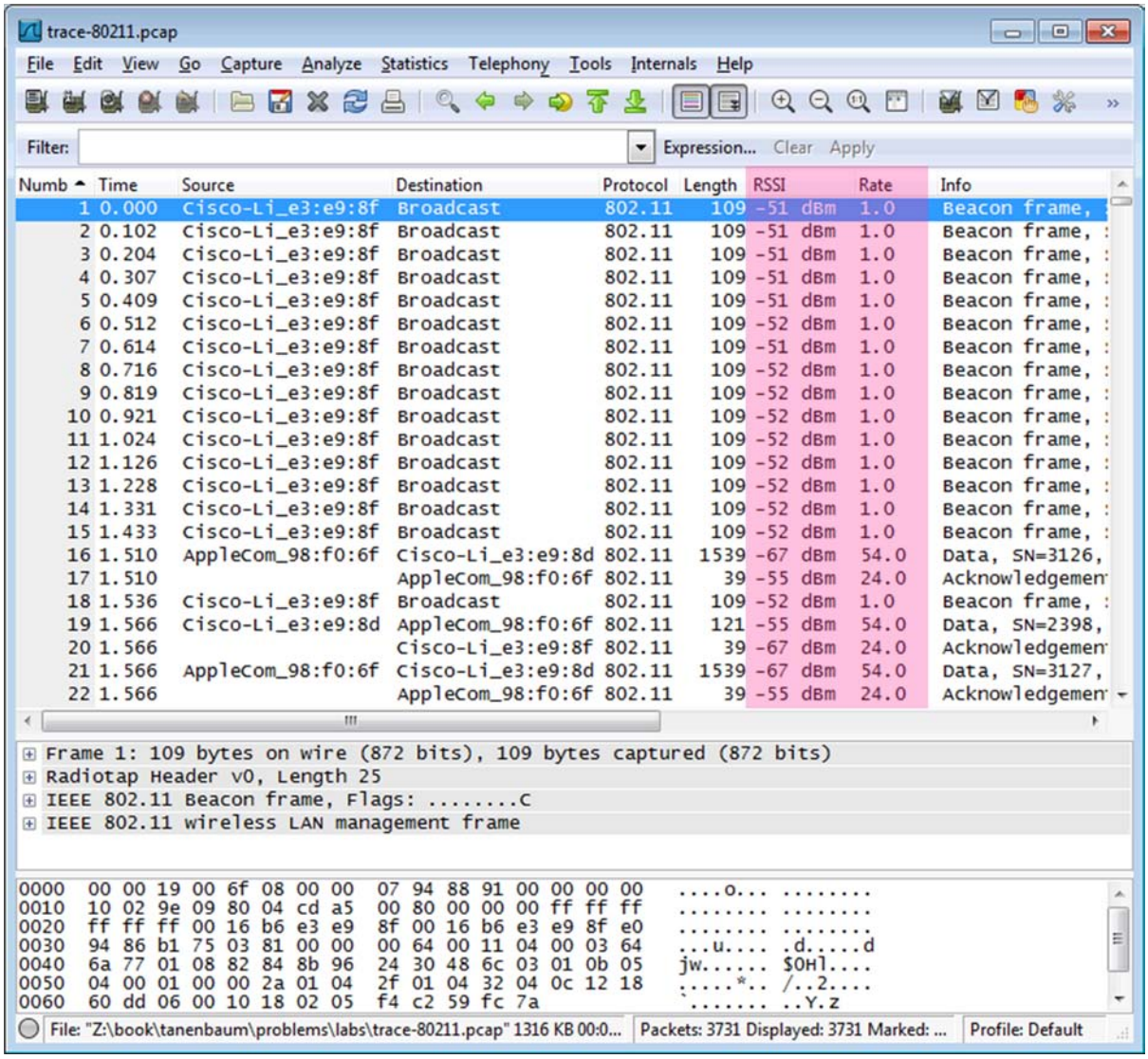


Figure 3: Wireless trace showing Rate and RSSI for each frame

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.

2. *What rates are used?* Give an ordered list of rates from lowest to highest. Hint: you can click the Rate column to sort by that value.

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. You should be gaining an appreciation for wireless technology!

3. *What is the range of RSSI and hence variation in SNRs in the trace?* Give this as the strongest and weakest RSSI and the dB difference between them.

Turn-in: Hand in your answers to the above questions.

Step 4: 802.11 Link Layer

Under the Statistics menu, select Conversations and WLAN (for wireless LAN, i.e., 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.

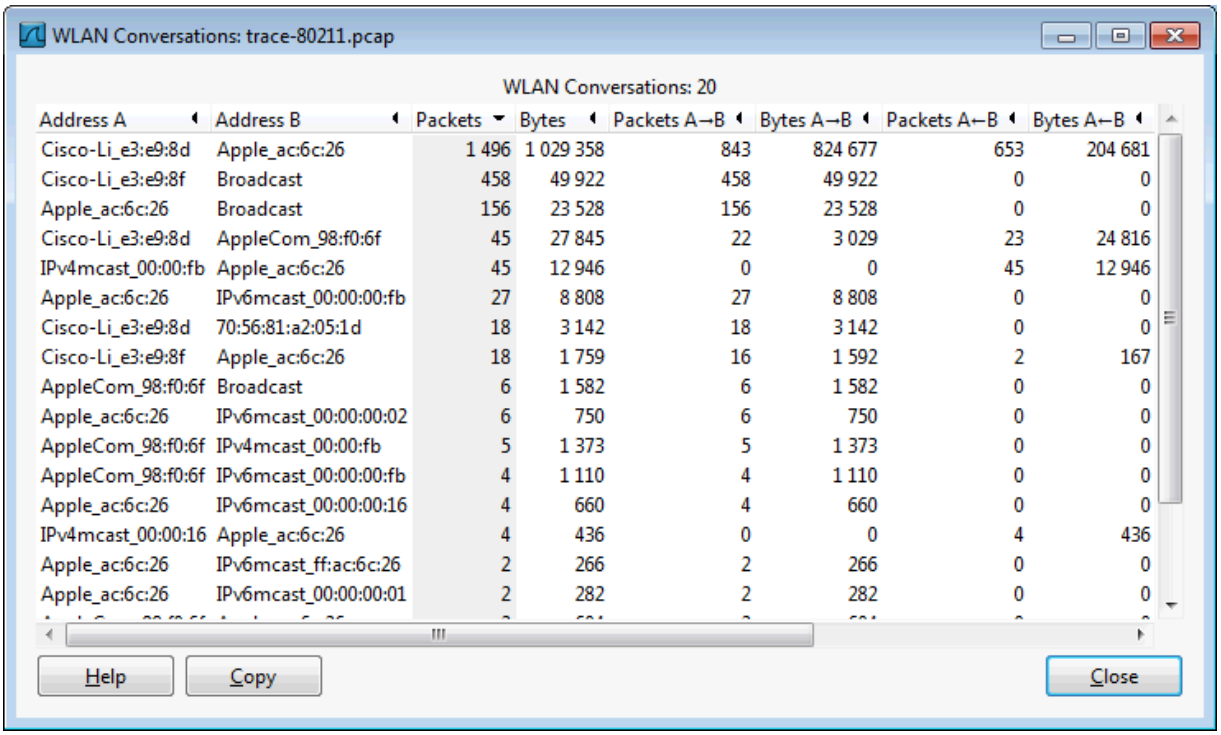


Figure 4: 802.11 conversations ordered by size

In our trace, and likely yours, 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.

Answer the numbered questions in this step to explore the link layer aspects of 802.11:

1. *What is the BSS ID used by the most active wireless conversations?* A BSS ID value identifies an AP, so this BSS ID identifies the most active AP, presumably the AP we are monitoring. To help find it, you can sort on the source or destination address by clicking on the column heading.

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.

Filter to see only Data frames by entering the expression `"wlan.fc.type==2"` *into the Filter box above the list of frames in the top panel.* 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`". When you enter this expression into your Filter box the display should resemble the figure below. 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.

2. *How many Data frames are in the trace, and what is the most common subtype of Data frame?*

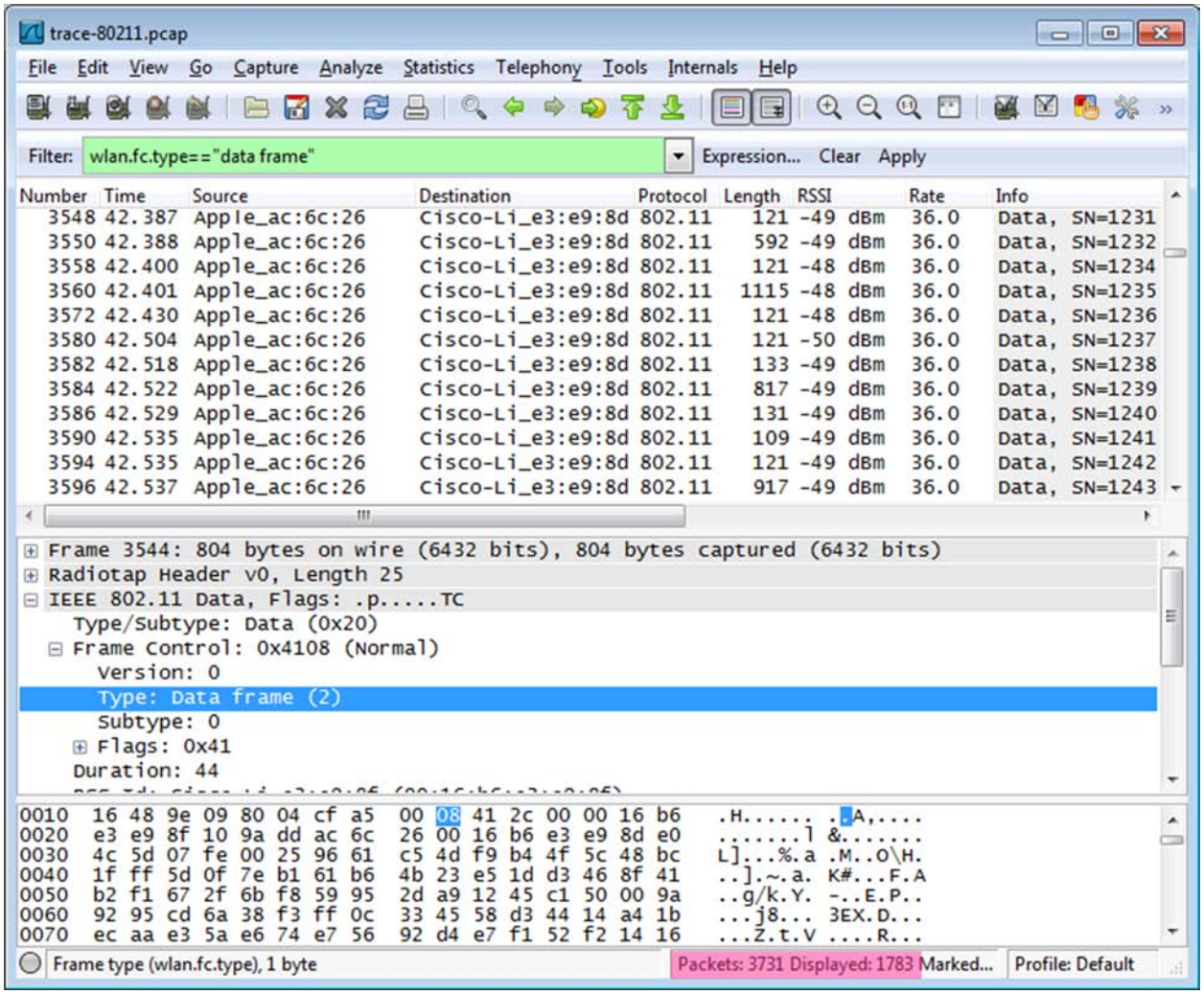


Figure 5: Filtering the wireless trace for Data frames

Perform the same exercise for Control (Type 1) and Management (Type 0) frames by changing the filter expression to search for a different Type value. This will let you find out how many of these frames are in the trace, and their most prevalent kinds.

3. *How many Control frames are in the trace, and what is the most common subtype?*
4. *How many Management frames are in the trace, and what is the most common subtype?*

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.

Inspect the IEEE 802.11 record of an Acknowledgement frame. We have looked at the format of Data frames, so let us turn to Acknowledgement frames. You should see that it has few fields compared to a Data frame, e.g., only one address, and that it is very short.

5. *List in the order they are sent the IEEE 802.11 fields in an Acknowledgement frame and their lengths in bytes.* Do not break down the Frame Control field into subfields, as we have already looked at these details.

We will investigate Management frames in the next step. To conclude our look at the link layer, 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 – let's see. 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.

Use 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.

6. *Give an estimate of the retransmission rate as the number of retransmissions over the number of original transmissions. Show your calculation.*

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.

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`".

7. *What fraction of the frames sent to the AP signal that the client is powering down?*

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.

Turn-in: Hand in your answers to the above questions.

Step 5: 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 and answer these questions:

1. *What is the SSID of the main AP?* This is one of the tagged parameters in the Beacon frame.
2. *How often are Beacon frames sent for the main AP?* You may 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".)
3. *What data rates does the main AP support?* The rates are listed under tagged parameters.
4. *What rate is the Beacon frame transmission?* The answer to this question will be found on the Radiotap header, or more conveniently displayed in the column you added in an earlier step.

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.

Find and examine an Association Request and Association Response frame to answer this question:

5. *What are the Type and Subtype values of Association Request / Association Response frames?*

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.

Find and examine a Probe Request and Probe Response frame to answer this question:

6. *What are the Type and Subtype values for the Probe Request / Probe Response frames?*

Turn-in: Hand in the answers to the above questions.

Congratulations, you now know a great deal about 802.11 in practice!

Explore on your own

We encourage you to explore 802.11 on your own once you have completed this lab. We have covered the basics of many topics, each of which you can delve into more deeply. Some ideas:

- Look to see how a given client uses different rates over time. This is called rate adaptation.
- See which clients are using power management and if you can understand their sleep behavior.
- See whether you can find clients that use the RTS/CTS mechanism.
- Look for Probe Request sequences to see when computers send them and what you can learn.
- Configure Wireshark with WEP/WPA2 keys to see witihin the 802.11 payload, starting with LLC.
- Try all of the above with a trace taken from your own network.

[END]