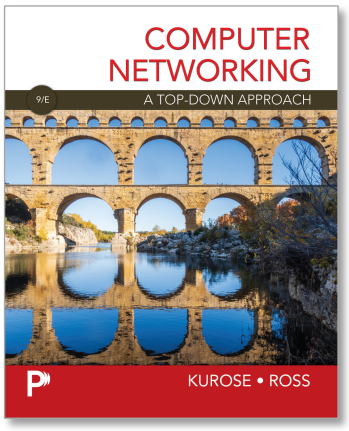
Wireshark Lab: 802.11 WiFi v9.0

Supplement to *Computer Networking: A Top-Down Approach, 9th ed.,* J.F. Kurose and K.W. Ross



"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

---

In this lab, we'll investigate the 802.11 wireless network protocol. Before beginning this lab, you might want to re-read Section 7.3 in the text[1]. Since we'll be delving a bit deeper into 802.11 than is covered in the text, you might want to check out "A Technical Tutorial on the 802.11Protocol," by Pablo Brenner (Breezecom Communications), http://www.sss-mag.com/pdf/802_11tut.pdf And, of course, there is the "bible" of 802.11 - the 4,379-page standard itself, "ANSI/IEEE Std 802.11-2020," https://gaia.cs.umass.edu/wireshark-labs/80211-2020.pdf. But we've extracted out section 9.2.4.1 from the specification, and added in a handy cheat-sheet for 802.11 Wireshark display filters, https://gaia.cs.umass.edu/wireshark-labs/802.11-9.2.4.1_spec+wireshark_filters.pdf, both of which will be *very* useful for this lab.

In this lab, we'll capture a trace from a wireless 802.11 WiFi interface on our computer/laptop. Here are the actions taken, assuming you're already connected to a WiFi network (which we'll refer to as your *home* network), when trace collection starts:

1. Make an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt
2. Make a request to http://www.cs.umass.edu
3. Disconnect from your home network
4. (optional step) Try to connect to another 802.11 wireless network whose beacon advertisements are being received, and for which you do *not* have access, and therefore your connection attempt will fail.
5. Connect again (successfully) to you home network.

Figure 1 shows the general setup for this 802.11 Wireshark lab.

[1] References to figures and sections are for the 9th edition of our text, *Computer Networks, A Top-down Approach, 9th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2025.* Our authors' website for this book is http://gaia.cs.umass.edu/kurose_ross You'll find lots of interesting open material there..

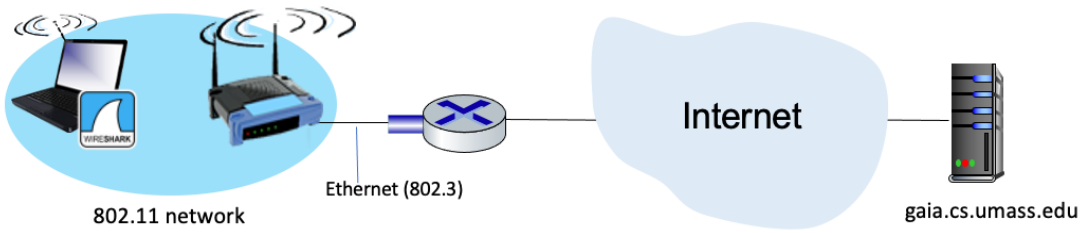


Figure 1: An 802.11 network, connected to a router, connected to the Internet

As usual, we've provided a trace file[2] of captured 802.11 frames for you to analyze in case you are not able to take the actions above. If you're doing this lab as part of a class, your teacher will provide details about how to hand in assignments, whether written or in an LMS.[3] The questions below assume you are analyzing this provided trace (in particular, with respect to access point (AP) names, and timings in the trace). Of course, you're encouraged to gather your own trace, taking the five actions above, and answering the questions below from your own trace.

1. Getting Started

Let's take a look at our trace file. This trace was collected using on a computer in the home network of one of the authors, 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. The author is fortunate to have other access points (APs) in neighboring houses available as well, so 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. You'll find the following wireless host activities in the trace file:

- The host is already associated with the *30 Munroe St* AP when the trace begins.
- At *t = 24.8282*, 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=32.8259, t*he host makes an HTTP request to http://www.cs.umass.edu, whose IP address is 128.119.240.19.
- At *t = 49.5836,* the host disconnects from the *30 Munroe St* AP by issuing a DHCP Release message.
- At *t=63.0592* the host associates again with the *30 Munroe St* AP.

[2] If you're unable to run Wireshark on a live network connection, you can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-9e.zip and extract the trace file Wireshark_801_11.pcapng.

[3] For the author's class, when answering the following questions with hand-in assignments, students print out the GET and response messages (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the message they've found the information that answers a question. They do this by marking paper copies with a pen or annotating electronic copies with text in a colored font. There are LMS modules for teachers that allow students to answer these questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm

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_801_11.pcapng trace file. The resulting display should look like Figure 2.

There are lots of captured frames in this trace, so we'll use display filters to display just selected types of frames as we analyze this trace. A handy reference for Wireshark Display filters for 802.11 frames is at http://gaia.cs.umass.edu/wireshark-labs/wireshark_802.11_filters_-_reference_sheet.pdf.

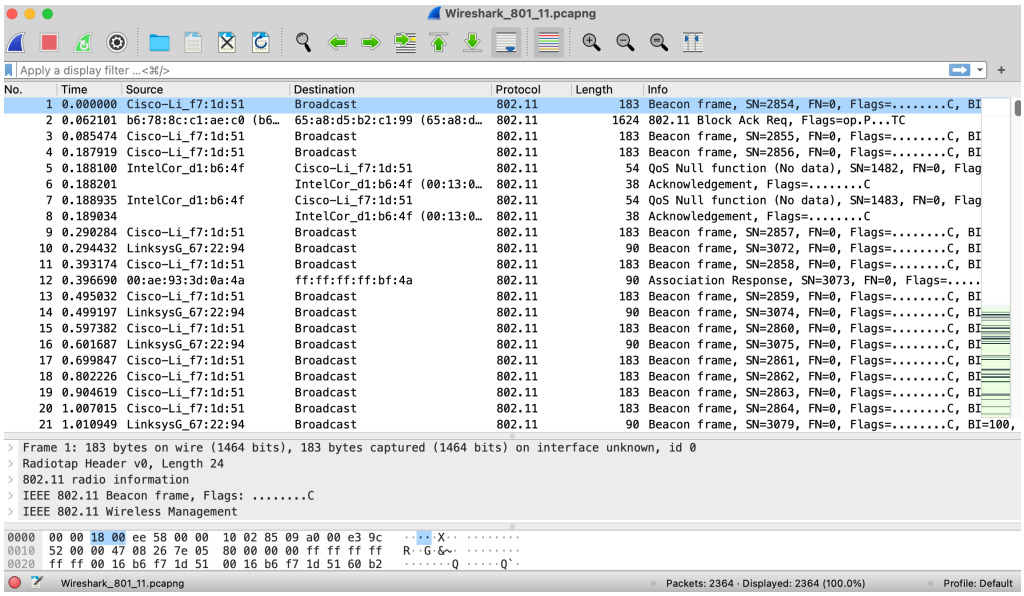


Figure 2: Wireshark window, after opening the Wireshark_801_11.pcapng file

2. Beacon Frames

First, let's take a look at 802.11 beacon frames. Recall that beacon frames are used by an 802.11 AP to advertise its existence. Let's use our 802.11 filter cheat-sheet (https://gaia.cs.umass.edu/wireshark-labs/802.11-9.2.4.1_spec+wireshark_filters.pdf): enter `wlan.fc.type_subtype == 8` into Wireshark's display filter window, so that Wireshark only displays beacon frames (which have an 802.11 subtype of 8). Your Wireshark window should look similar to Figure 3.

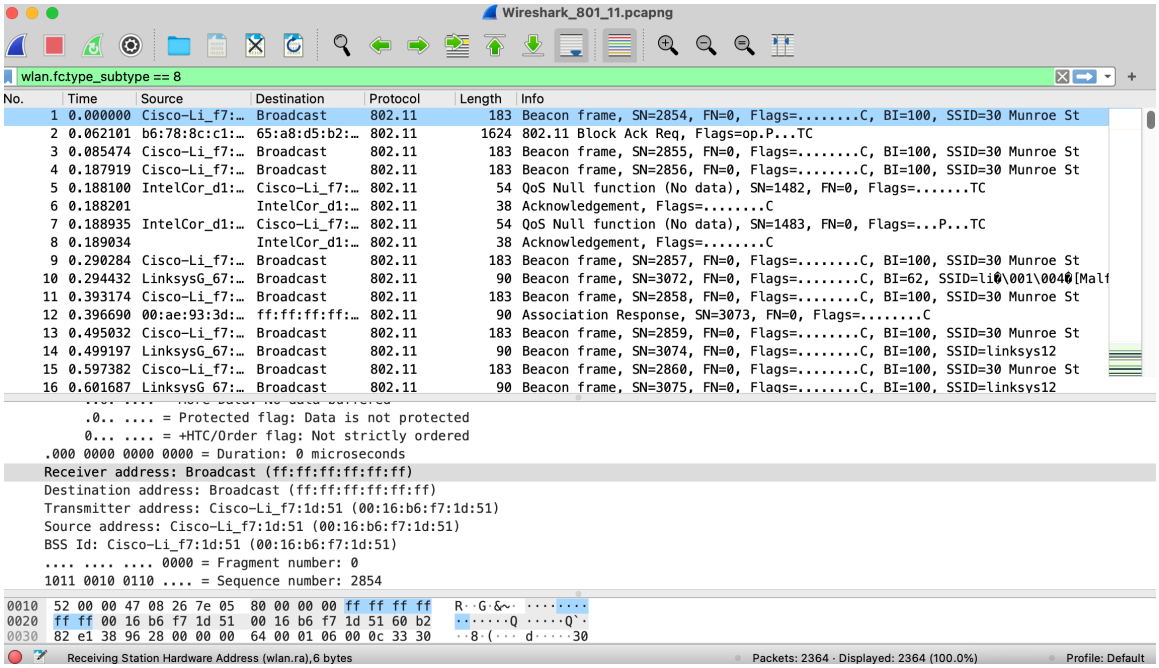


Figure3: Wireshark window, showing beacon frames

To answer some of the questions below, you'll want to look at the details in the *Info* field in the rightmost column of the Wireshark display; to answer other questions you'll need to dig into the "802.11 Protocol" 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? [Hint: look at the *Info* field. To display only beacon frames, neter `wlan.fc.type_subtype == 8` into the Wireshark display filter].
2. What 802.11 channel is being used by both of these access points [Hint: you'll need to dig into the radio information in an 802.11 beacon frame]

Now let's take a look at the beacon frame sent at t=0.085474.

3. What is the interval of time between the transmissions of beacon frames from this access point (AP)? (Hint: this interval of time is contained in a field within the beacon frame itself).
4. What (in hexadecimal notation) is the source MAC address on the beacon frame from this access point? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 9.2.3-9.2.4.1in the IEEE 802.11 standards document, excerpted https://gaia.cs.umass.edu/wireshark-labs/802.11-9.2.4.1_spec+wireshark_filters.pdf.
5. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*??
6. What (in hexadecimal notation) is the MAC BSS ID on the beacon frame from *30 Munroe St*?

7. 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? [Note: the traces were taken on a rather old AP].

3. Data Transfer

Since the trace starts with the host already associated with the AP, let's next 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.

8. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt) at t=24.8110. 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 for the TCP syn segment?
9. Does the destination IP address of this TCP SYN correspond to the host, access point, first-hop router, or the destination web server?
10. Find the 802.11 frame containing the SYNACK segment for this TCP session received at t=24.8277 What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).

3. Disassociation/Authentication/Association

Recall from Section 7.3.1 in the text that 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 subtype 0, see Section 7.3.3 in the text) 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 ASSOCIATE REQUEST). And *before* an association is performed, the host and AP must agree on the form that authentication that will be used when the host associated with the AP; this agreement is done using the AUTHENTICATION frame.

Recall that our trace began with our host already associated with an access point. Around t=49 the host disassociates from the access point, waits a bit, and then again re-authenticates and re-associates with the access point

11. What two actions are taken (i.e., frames are sent) by the host in the trace just after *t=49*, to **end** the association with the *30 Munroe St* AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action).

Now let's look at the process of authenticating and associating with an access point. We'll look at four specific frames captured at the times shown in Figure 4.

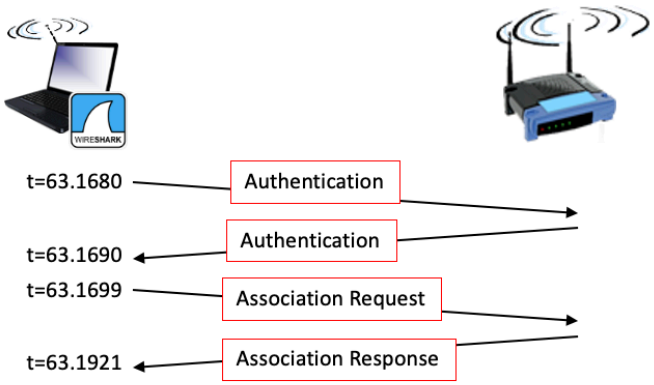


Figure 4: Authentication and Association

12. Let's look first at AUTHENTICATION frames. At *t = 63.1680,* our host tries to associate with the *30 Munroe St* AP. Use the Wireshark display filter `wlan.fc.subtype == 11` to show AUTHENICATION frames sent from the host to and AP and vice versa. What form of authentication is the host requesting?
13. What is the `Authentication SEQ` value (authentication sequence number) of this authentication frame from host to AP?
14. The AP response to the authentication request is received at *t = 63.1690.* Has the AP accepted the form of authentication requested by the host?
15. What is the `Authentication SEQ` value of this authentication frame from AP to Host?

Now let's look at the ASSOCIATION REQUEST sent at *t = 63.1699* and ASSOCIATION RESPONSE received at *t = 66.1921.* Note that you can use the filter expression wlan.fc.subtype < 2 and wlan.fc.type **==** 0 to display ASSOCIATION REQUEST and RESPONSE frames.

16. What rates are indicated in the frame as SUPPORTED RATES**.** Do ***not*** include in your answers below any rates that are indicates as EXTENDED SUPPORTE RATES.
17. Does the ASSOCIATION RESPONSE indicate a Successful or Unsuccessful association response?
18. Does the fastest (largest) Extended Supported Rate the host has offered match the fastest (largest) Extended Supported Rate the AP is able to provide?