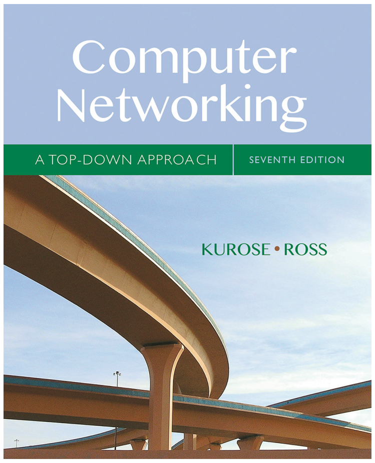
Wireshark Lab: 802.11 v7.0

Supplement to *Computer Networking: A Top-Down Approach, 7th 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 "Understanding 802.11 Frame Types," by Jim Geier, http://www.wi-fiplanet.com/tutorials/article.php/1447501. And, of course, there is the "bible" of 802.11 - the standard itself, "ANSI/IEEE Std 802.11, 1999 Edition (R2003)," http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf. In particular, you may find Table 1 on page 36 of the standard particularly useful when looking through the wireless trace.

In all of the Wireshark labs thus far, we've captured frames on a wired Ethernet connection. Here, since 802.11 is a wireless link-layer protocol, we'll be capturing frames "in the air." Unfortunately, many device drivers for wireless 802.11 NICs don't provide the hooks to capture/copy received 802.11 frames for use in Wireshark (see Figure 1 in Lab 1 for an overview of packet capture). Thus, in this lab, we'll provide a trace of captured 802.11 frames for you to analyze and assume in the questions below that you are using this trace. If you're able to capture 802.11 frames using your version of Wireshark, you're welcome to do so. Additionally, if you're really into frame capture, you can buy a small USB device, AirPcap, http://www.cacetech.com, that captures 802.11 frames and provides integrated support for Wireshark.

1. Getting Started

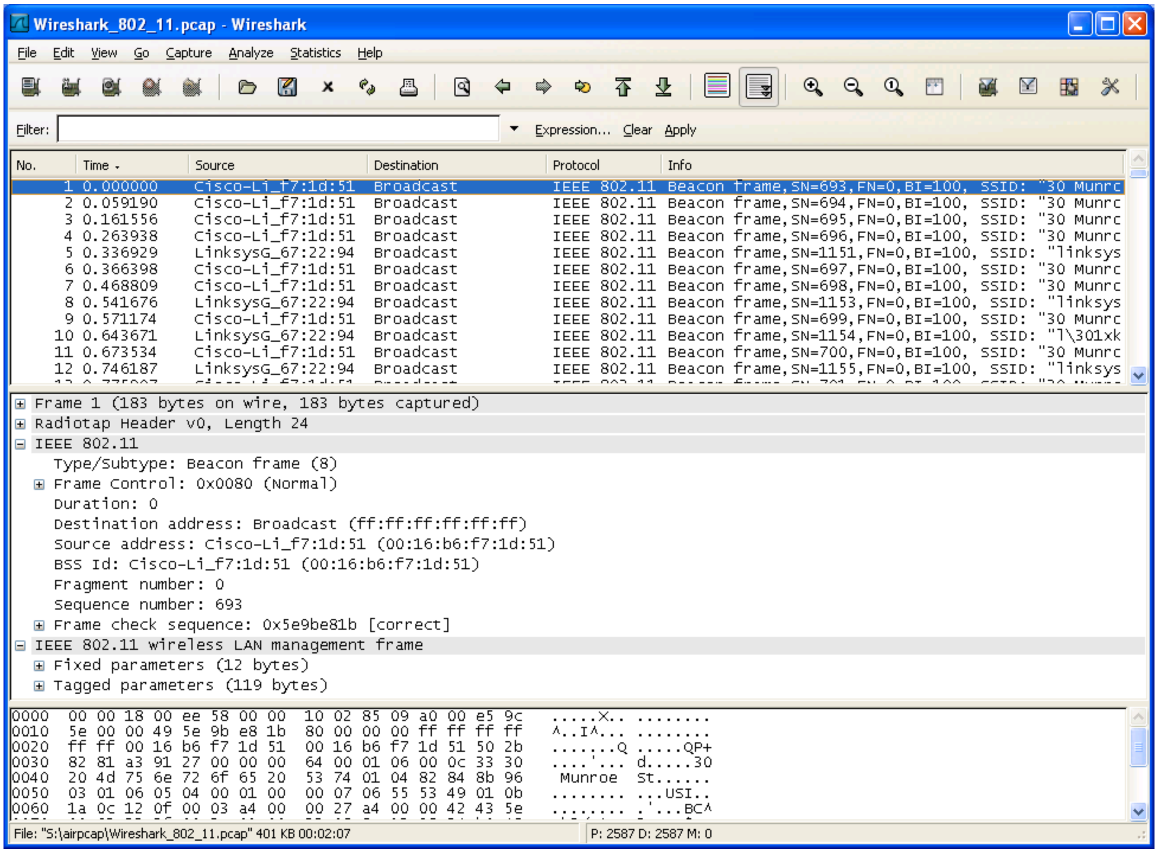
Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file Wireshark_802_11.pcap. This trace was collected using AirPcap and Wireshark running on a computer in the home network of one of the authors, consisting

[1] References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down Approach, 7th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.*

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 in neighboring houses available as well. In this trace file, we'll see frames captured on channel 6. Since the host and AP that we are interested in are not the only devices using channel 6, we'll see a lot of frames that we're not interested in for this lab, such as beacon frames advertised by a neighbor's AP also operating on channel 6. The wireless host activities taken in the trace file are:

- The host is already associated with the *30 Munroe St* AP when the trace begins.
- At *t = 24.82*, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12.
- At *t=32.82, t*he host makes an HTTP request to http://www.cs.umass.edu, whose IP address is 128.119.240.19.
- At *t = 49.58,* the host disconnects from the *30 Munroe St* AP and attempts to connect to the *linksys_ses_24086*. This is not an open access point, and so the host is eventually unable to connect to this AP.
- At *t=63.0* the host gives up trying to associate with the *linksys_ses_24086 AP,* and associates again with the *30 Munroe St* access point.

Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the Wireshark_802_11.pcap trace file. The resulting display should look just like Figure 1.



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

```
⊞ Frame 1 (183 bytes on wire, 183 bytes captured)
⊞ Radiotap Header v0, Length 24
⊟ IEEE 802.11
    Type/Subtype: Beacon frame (8)
  ⊞ Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Fragment number: 0
    Sequence number: 693
  ⊞ Frame check sequence: 0x5e9be81b [correct]
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊞ Tagged parameters (119 bytes)
```

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

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

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

2. Beacon Frames

Recall that beacon frames are used by an 802.11 AP to advertise its existence. To answer some of the questions below, you'll want to look at the details of the "IEEE 802.11" frame and subfields in the middle Wireshark window. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout[2] to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?
2. What are the intervals of time between the transmissions of the beacon frames the *linksys_ses_24086* access point? From the *30 Munroe St*. access point? (Hint: this interval of time is contained in the beacon frame itself).
3. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? 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 7 in the IEEE 802.11 standards document (cited above).
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*??
5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *30 Munroe St*?
6. The beacon frames from the *30 Munroe St* access point advertise that the access point can support four data rates and eight additional "extended supported rates." What are these rates?

3. Data Transfer

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

[2] What do we mean by "annotate"? If you hand in a paper copy, please highlight where in the printout you've found the answer and add some text (preferably with a colored pen) noting what you found in what you 've highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate.

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.
8. Find the 802.11 frame containing the SYNACK segment for this TCP session. 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).