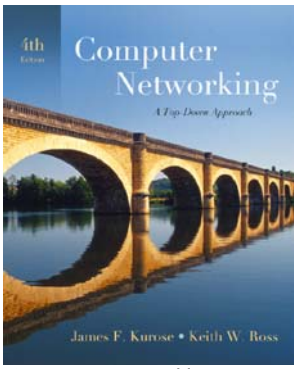
Wireshark Lab: 802.11



Computer Networking: A Top-down Approach, 4th edition.

Version: 2.0
© 2007 J.F. Kurose, K.W. Ross. All Rights Reserved

In this lab, we'll investigate the 802.11 wireless network protocol. Before beginning this lab, you might want to re-read Section 6.3 in the text. 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 802.11 Protocol," 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, most of the device drivers for wireless 802.11 NICs (particularly for Windows operating systems) 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 under Windows.

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 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* AP. 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.

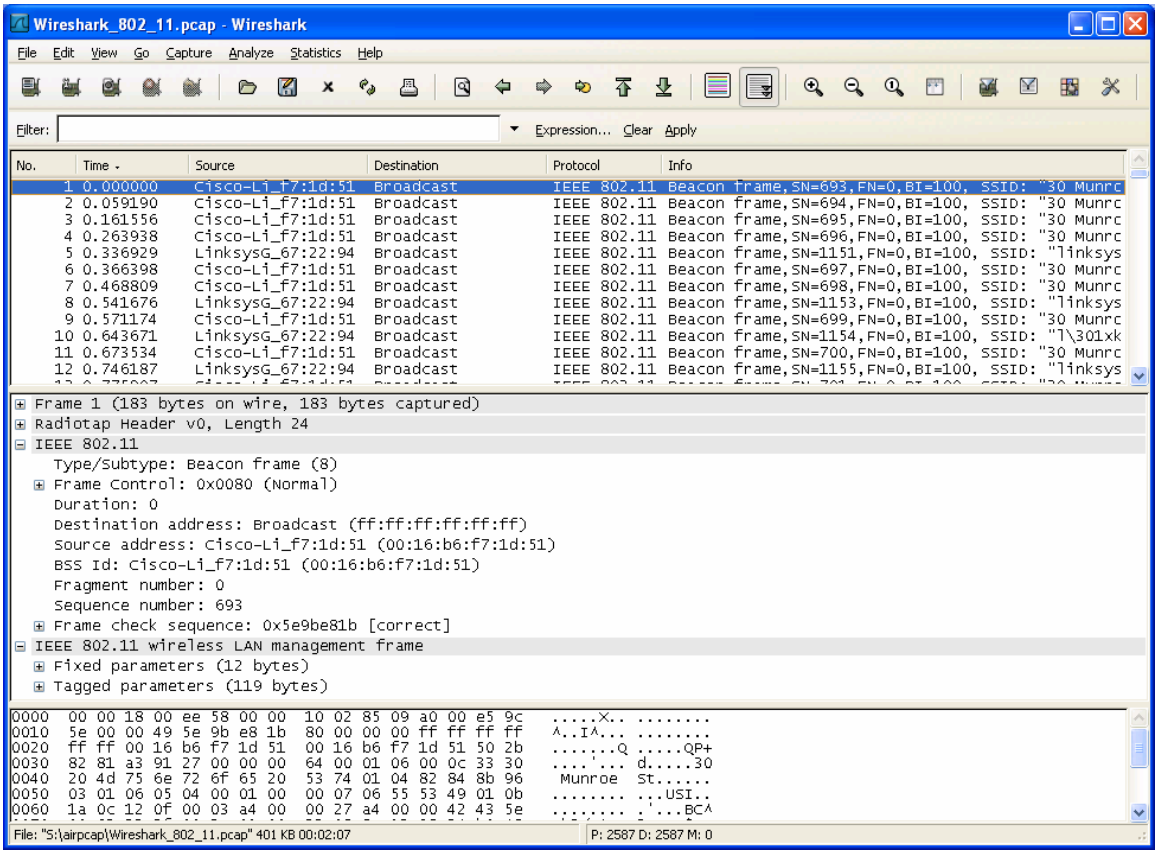


Figure 1: Wireshark window, after opening the Wireshark_802_11.pcap file

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.

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 transmission 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 6.13 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.

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). At what time is the TCP SYN sent? 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. (Hint: review Figure 5.19 in the text if you are unsure of how to answer this question, or the

corresponding part of the next question. It's particularly important that you understand this).

8. Find the 802.11 frame containing the SYNACK segment for this TCP session. At what time is the TCP SYNACK received? What are three MAC address fields in the 802.11 frame containing the SYNACK? 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?

3. Association/Disassociation

Recall from Section 6.3.1 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 Figure 6.13 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). For a detailed explanation of each field in the 802.11 frame, see page 34 (Section 7) of the 802.11 spec at http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf.

9. 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, and at what times are these frames sent? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?
10. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. When is the first AUTHENTICATION frame sent from the wireless host to the *linksys_ses_24086* AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around *t=49?* .
11. Does the host want the authentication to require a key or be open?
12. Do you see a reply AUTHENTICATION from the *linksys_ses_24086* AP in the trace?
13. Now let's consider what happens as the host gives up (sometime after $t = 63.0$) trying to associate with the *linksys_ses_24086* AP and now tries to associate with the *30 Munroe St* AP. Look for AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the *30 Munroe St.* AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)
14. Let's continue on with the association between the wireless host and the *30 Munroe St* AP that happens after $t = 63.0$. An ASSOCIATE from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the *30 Munroe St* AP? When is the corresponding

ASSOCIATE REPLY sent? (Note that you can use the filter expression "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

15. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

4. Other Frame types

Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.

16. Consider the first PROBE REQUEST and the soonest subsequent PROBE RESPONSE PAIR occurs after $t = 2.0$ seconds in the trace. When are these frames sent and what are the sender, receiver and BSS ID MAC addresses for these frames? What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).