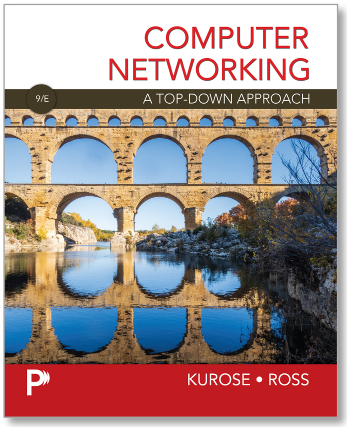
Wireshark Lab: WiFi Radio v9.0

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 take a look at radio information provided to Wireshark in a WiFi network. 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.

For this lab, you'll need to work with traces provided to you, as it is notoriously hard to capture WiFi frames that have radio information[2]. Using the *airtool2* software, we've captured a trace file[3] of 802.11 frames for you to analyze for this lab The questions below assume you are analyzing this provided trace.

Let's take a look at the radio information available in a WiFi 802.11 trace by starting with packet number 3 in this trace, which contains a "beacon" 802.11 frame advertising the *carioca* WiFi network. We'll learn about beacon frames in another lab; for now, all we care about is the radio information associated with WiFi frames broadcast by the *carioca* access point. Select packet 3, and look at the "details" of this packet.

[1] References to figures and sections are for the 9th edition of our text, *Computer Networks, A Top-down Approach, 9h 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..

[2] To collect WiFi traces with radio information your computer would need to be put into "monitor mode," which allows your computer to promiscuously capture all WiFi traffic on a given channel. But you'd need to figure out which WiFi channel to listen to. To complicate matters further, when in monitor mode you can't run applications, so you'd need to generate traffic on another computer that would then be captured on your monitor-mode computer.

[3] Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-9e.zip and extract the trace file carioca_Iphone_association_selected_packets_only.pcapng

There are two fields that give more information about the WiFi radio channel: the `radio tap V0` field and the `802.11 radio information` field. Both fields contain radio-related (i.e., physical-layer) information from the receiver's device driver for the 802.11 interface that captured this 802.11 frame. This radio information is *not* part of the 802.11 protocol but rather information provided by the driver about the radio when the frame was received. For the trace captured on this particular machine on this particular wireless network, the `radio tap V0` field and the `802.11 radio information` fields contain mostly redundant information about the wireless physical layer, so we'll just consider the `radio tap V0` field.

Expand the `radio tap V0` field and answer the following questions. You can find details about the radiotap header fields here: https://www.radiotap.org/fields/defined

1. What WiFi channel number is this frame being carried on? You might find it useful to refer to Figure 7.23 in our textbook (WiFi channels in the 2.4 and 5 GHz bands).
2. What is the frequency of this channel?
3. What is the bandwidth of this channel?
4. What is the data rate of this channel?
5. Which modulation technique is being used for this channel?
6. How many antennas are there on the receiver's wireless interface (where this trace was taken)?
7. What is the radio signal strength measured in dBm at the receiver's antenna?
8. What is this signal strength measured in milliwatts?
9. What is the radio's noise strength measured in dBm at the receiver's antenna
10. What is this noise signal strength measured in milliwatts?
11. What is the SNR at the receiver's antenna?

Now let's take a look at another beacon frame being sent by the *carioca* AP. In particular, take a look at frame 258, and answer the following questions:

12. What WiFi channel number is frame 258 being carried on?
13. Consider the radio signal strength measured in dBm at the receiver's antenna for frame 258. How many orders of magnitude stronger or weaker is this received signal than that of frame 3?
14. Consider the noise signal strength measured in dBm at the *receiver's* antenna for frame 258. How many orders of magnitude stronger or weaker is this noise signal than that of frame 3?