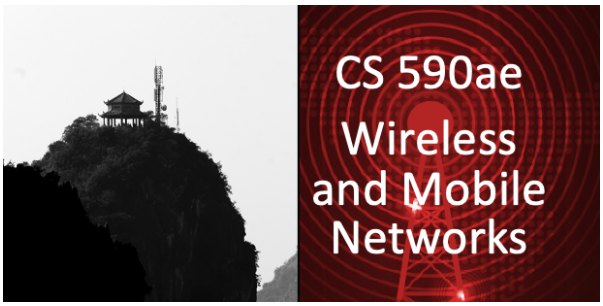
CS590ae: Lab 3

Assigned: 3/5/25
Due: 3/12/25

Spring 2025
Professor Jim Kurose

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



In this third lab for CS590ae, we'll take a look at link-layer information in a WiFi WLAN and in a 5G RAN. For this lab, you'll again work with traces provided to you, given the difficulty of capturing WiFi or 5G traces (see the discussion of these difficulties in Lab 2).

Investigating WiFi's link layer

Before starting this lab, you might want to review the material we've covered in class in the class on WiFi (slides: https://gaia.cs.umass.edu/wireless_and_mobile_networks/slides/WiFi.pptx, reading: https://gaia.cs.umass.edu/wireless_and_mobile_networks/readings/Chapter_4_WiFi.pdf) and the WiFi parts of the class on Edge Network Topics (slides: https://gaia.cs.umass.edu/wireless_and_mobile_networks/slides/Edge_topics.pptx , reading: https://gaia.cs.umass.edu/wireless_and_mobile_networks/readings/Chapter_6_Edge_topics.pdf). Of course, there is the "bible" of 802.11 - the 4,379-page standard itself , "ANSI/IEEE Std 802.11-2020," available here: https://gaia.cs.umass.edu/wireshark-labs/80211-2020.pdf But we've extracted Section 9.2.4.1 from this specification, *and* added in a handy cheat-sheet for 802.11 Wireshark display filters, here: 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.

Figure 1 shows the general setup for the 802.11 part of Lab 3.

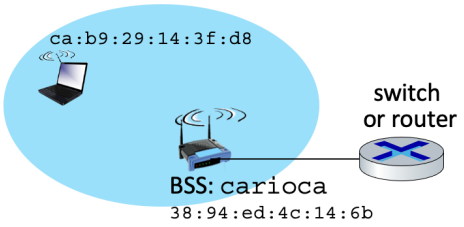


Figure 1: An 802.11 network, connected to a router

First let's take a look at WiFi link-layer functions. To do this, download the file https://gaia.cs.umass.edu/wireless_and_mobile_networks/files/carioca_Iphone_association.pcapng, which contains WiFi frames taken in the carioca WiFi network.

Let's take a look at packet number 3 in this trace, which contains a "beacon" 802.11 frame advertising the *carioca* WiFi network. Select packet 3 and look at the "details" of this packet (see Figure 3 in Lab 1 if you're unsure of the "packet details" section of the Wireshark display). Recall that a beacon packet is used by an AP to advertise itself and information about its capabilities.

1. **Which channel?** Which WiFi channel is being used by this access point?
2. **What frequency?** What is the frequency range associated with this channel (Hint: you'll need to dig into the `802.11 radio information` in this frame.
3. **What is the bandwidth** associated with this channel? (Hint: "bandwidth" in the technical sense of the width of the frequency band, rather than the transmission rate. Also while you can (and should) find the center of the carrier frequency from the beacon, to get the range, you'll need to look it up elsewhere, e.g., https://en.wikipedia.org/wiki/List_of_WLAN_channels).
4. **Beaconing interval?** What is the interval of time between the transmissions of beacon frames from this AP)? (Hint: this interval of time is contained in a field within the beacon frame itself).
5. ***Source* MAC address on beacon frame?** What (in hexadecimal notation) is the source MAC address on the beacon frame from this access point? Recall from our WiFi reading 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 here: here: https://gaia.cs.umass.edu/wireshark-labs/802.11-9.2.4.1_spec+wireshark_filters.pdf.
6. ***Destination* MAC address on beacon frame?** What (in hexadecimal notation) is the destination MAC address on the beacon frame from this access point?
7. ***BSS ID* MAC address on beacon frame?** What (in hexadecimal notation) is the BSS ID MAC address on the beacon frame from this access point?
8. **Supported data rates.** The beacon frame advertises that the AP can support four data rates and eight additional "extended supported rates." Indicate which of the follow rates below ***are*** supported among the base set of four rate or are in the set of sight extended supported rates?

Now let's take a look at 802.11 management frames that request measurement reports. You can use a Wireshark display filter of `wlan.fc.type_subtype ==13` to only show management frames of type ACTION (of which measurement requests and measurement replies are two such "actions"). Let's take a closer look at frame No. 4787 in our trace, which is a **measurement request frame.** You might want to consult Section 9.4.2.20.1 (page 967) and Section 9.4.2.20.7 (page 974) of the full ANSI/IEEE Std 802.11-2020 standard: https://gaia.cs.umass.edu/wireshark-labs/80211-2020.pdf You'll be pleased that I've pointed out the two relevant pages in the 4,377 page document!

9. Which node is the transmitter of this measurement request frame?
10. Which node is the addressed receiver of this measurement request frame?
11. What type of frame measurement is being requested [Hint: you'll want to expand the `IEEE 802.11 Wireless Management` field in the 802.11 frame. See Table 9-98 (page 969) in 802.11-2020 standard for full list of the types of measurements that can be made and Section 9.4.2.20.7, page 974.]

12. On what channel number should the requested measurement be made?
13. How long should the requested measurement be made?

Let's next take a look at 802.11 management frames that return measurement data in response to the earlier measurement requests. In particularl let's take a closer look at frame No. 4841, which is a **measurement report frame.**

14. What type of report is contained in this report (that is, what type of frame is being reported on)? [Hint: look for a `Measurement Report Type` field].
15. Which node is the transmitter of this measurement response frame?
16. Which node is the addressed receiver of this measurement response frame?
17. What is the reported value of the Received Channel Power Indicator (RCPI)?
18. What is the reported value of the Received Signal to Noise Indicator (RSNI)?

Investigating the 5G RAN: getting started

We learned in class 11 that the MIB and SIB blocks, broadcast from the gNB within the RAN allows devices to find the 5G network and information about that network. Let's look at MIB and SIB1 messages in a 5G trace was captured by our TA, Atharva Kale, on a 5G Android phone connected to a national cellular network provider (you'll learn the identity of the prover by digging into the SIB1 information block being broadcast by the provider's gNB in Amherst MA, as shown in Figure 2. You should download the trace file https://gaia.cs.umass.edu/wireless_and_mobile_networks/files/trace4-scatv2-5G-NR-feb-19-2025.pcapng for the second part of this lab.

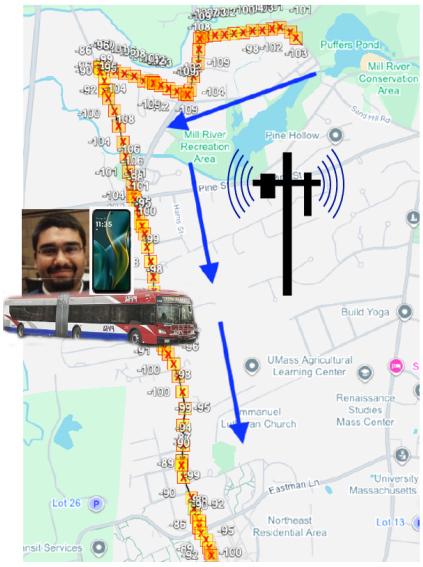


Figure 2: 5G trace scenario

As we learned in class, the 5G Master Information Block (MIB) contains critical information about the cellular network: the network owner/operator, channel bandwidth information, and a pointer to where the UE should listen for additional information in the System Information Blocks (SIBs), including the SIB1 block. Both the MIB and the

SIBs are broadcast on the Physical Broadcast Channel (PBCH). We'll look at a MIB and SIB1in this trace.

Let's start by focusing on packet 1 in this trace – a MIB message. Expand the NR Radio Resource Control (RRC) protocol line as well as the following BCCH-BCH-Message line, which shows the MIB message received on the PBCH.

19. What are the subcarrier spacings (channel widths) used in this 5G network? Two values are given, one for the case of the 410 MHz–7125 MHz range, and one for the case of the 24.25 GHz–52.6 GHz range. "scs15or60" would indicate 15 kHz in the lower frequency ranges and 60 kHz in the higher, millimeter ranges.
20. Is this network open for use? A cell that is open for use will not bar users from joining (or at least will allow UE to present credentials, after which the UE may or may be admitted to the network).

The `System Frame Number(SFN)` in the MIB helps the UE synchronize it slot timing boundaries to that of the gNB. A 10 ms interval is conceptually divided into 1024 smaller intervals. The `System Frame Number` indicates the current position of time in these 1024 intervals. Since both the UE and the gNB know the `SFN` they know the common current position with the 1024 subintervals in the current 10 ms long interval.

21. What is the value of the `SFN`?

Let's next focus on packet 2 in this trace – a SIB1 message. Let's see what's in there. Expand the NR Radio Resource Control (RRC) protocol line in this SIB1 message, and all other following lines. We're interested in the material in the `PLMN-Identity` fields. (As an aside, PLMN stands for Public Land Mobile Network - a mobile operator's cellular network in a given country). Here's where your phone finds the country and the identity of the network that is sending the SIB The country and the identity of the network is in this information! The Three `mcc` digits (311) are the country code; the three `mnc` digits given the network operator code. You will need to look up the names of the countries and network operators using these codes: here:
https://en.wikipedia.org/wiki/Mobile_network_codes_in_ITU_region_3xx_(North_America)

22. What country is the origin country for this network?
23. What company is the owner/operator of this network?
24. The RAN cell within this network has an identifier, what is that identifier?
25. The RAN cell within this network also has a tracking area code. We'll see how this code is use when we cover device mobility. What is the value of this code?

Hey! The SIB shows there is *another* country and provider associated with this network! It has a different MCC (**Mobile Country Code**) as part of its PLMN.

26. What is the MCC value of this second provider network?
27. Is the second owner/operator name (not number) the same as the name of the early owner/operator for the other in your answers above?

You might want to scroll further down the SIB1 message, where you find configuration information for the physical channels that we learned about in class. We can see how

through the use of the MIB and IB, the UE is able to bootstrap information about the network. Of course, the UE has yet to identify itself to the networks; we'll cover that topic shortly.

3. What to hand in for this lab.

Now that you've done all of the above, it's time to work on handing in the results of this lab. You'll do so on our class's Canvas page, where you'll be asked to upload your screenshots and answer the questions posed above, mostly using trace files and screen shots that have been captured for you.