18-452/750 Monitor Mode Support and Wireshark Setup Check

This guide helps you to check if your laptop is ready for the experiments in Project 1. You will have to answer 3 questions and submit to the "Information for course and Project 1" form on Gradescope:

1. Does your laptop support monitor mode?
2. Can you set Wireshark running in monitor mode?
3. Can you monitor physical layer data in Wireshark?

If monitor mode is not supported in question 1, it is very likely that you cannot satisfy question 2 and 3. We will have other solutions in this case.

Project 1 Goal

Monitor two devices communicating over WiFi using Wireshark (installed on device A).

Figure 1: Overview Diagram of Experiment Setup: Device A is running Wireshark, Device B can be any device communicating with Device A.

Check for Monitor Mode Support

Monitor mode allows a wireless card to monitor all the traffic transferring over a specific wireless channel, including physical layer data. Not all laptops support monitor mode, it is very dependent on the wireless card and the wireless chipset inside.

- For MacOS laptops, they use Apple's own wireless adapters, and all of them support Monitor Mode (10.4.x and above). Therefore, we highly recommend you using a MacOS laptop for this project. See this website for more information: `https://wiki.wireshark.org/CaptureSetup/WLAN#macos-mac-os-x`

- For PC laptops, see the following instructions to check if your laptop support monitor mode and enable it (in case of Linux).

Linux

1. Use **iw dev** command to find out the device name of your wireless card, for example, phy0. Here you can also find the default wireless interface running on managed mode (normal mode), e.g., wlan0. Take a note of the frequency this interface is running on, e.g., 2437 MHz.

2. Use **iw phy *device name* info** command, e.g., **iw phy phy0 info** to list interface modes that your card supports. If you find "monitor" in the Supported interface modes section, monitor mode is supported and follow the next steps to manually enable monitor mode.

   Question 1: Does your laptop support monitor mode?

3. Add a new wireless interface named mon0, which runs on monitor mode using the following command: **sudo iw phy phy0 interface add mon0 type monitor**.

4. Use **iw dev** command again and make sure that the mon0 interface has shown up. Use **sudo ifconfig mon0 up** and **sudo iw dev mon0 set freq 2437** command to enable the new interface and set its frequency to the same frequency as the wlan0 interface (replace 2437 with your frequency).

5. Continue to the Wireshark instructions.

Windows

1. Use **netsh wlan show wirelesscapabilities** command and find "Network monitor mode" under your Wi-Fi interface name to see if your wireless card supports monitor mode. Windows is quite limited. There are many cases where a wireless card supports monitor mode in Linux but not in Windows. This website provide addition information about monitor mode support on Windows: `https://wiki.wireshark.org/CaptureSetup/WLAN#windows`. If monitor mode is supported, you can enable it in Wireshark.

   Question 1: Does your laptop support monitor mode?

2. Continue to the Wireshark instructions.

Wireshark Setup

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. In this tutorial, we introduce the instructions on how to use Wireshark in Monitor Mode to capture network traffic on 802.11 wireless networks.

1. **Preparation:** (1) You need one laptop (Device A in Figure. 1) running Wireshark (Installation: `https://www.wireshark.org/download.html`). (2) You need another device (Device B in Figure. 1) to communicate with your Device A. Device B can be another laptop, a Wi-Fi router, etc. In the following steps, we assume you are using your Wi-Fi router as Device B.

   Note: If you're using Windows, when installing Wireshark, select the option to install Npcap, but not WinPcap. Enable the "Support raw 802.11 traffic (and monitor mode) for wireless adapters" option when installing Npcap.

2. **Establish a wireless connection** between the two devices by simply connecting them on the same Wi-Fi network.

3. **Wireshark in Monitor Mode**.

   (a) Open Wireshark on Device A. In the drop down menu for "Capture" ensure that 'Wireless' is selected. It should display 'Wi-Fi' below with a graphical display of the number of messages received over time next to it.

   (b) Click on the 'Capture' drop down menu, and select 'Options ...'. In the new window that opens, ensure that for the Wi-Fi Interface (mon0 in case of Linux), 'Monitor' box is checked. With the 'Wi-Fi' Interface highlighted, click the 'Start' button. If you can check the 'Monitor' box, Wireshark is running in monitor mode.

   Question 2: Can you set Wireshark running in monitor mode?

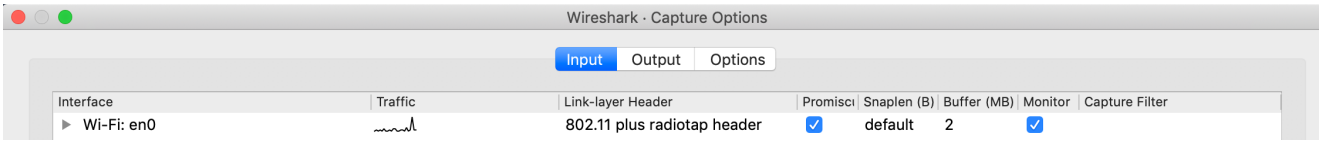

Figure 2: Setting Monitor Mode on Wireshark

4. **Check for Physical Layer Data**. If Wireshark is operating in Monitor Mode and the wireless hardware, when a packet is selected (i.e. clicked on) a packet dissection will be shown below. In the packet dissection, there should be a category titled '802.11 radio information'. Select this to view the values obtained.

   If there is an '802.11 radio information' category, you are ready for project 1! Congrats! The '802.11 radio information' category should include data for: 'PHY type', 'Data rate', 'Frequency', 'Signal strength (dBm)', 'Noise level (dBm)', 'Bandwidth', and 'TSF timestamp'. Observe the value of 'Signal strength (dBm)'.

   Question 3: Can you monitor physical layer data in Wireshark?