WiFi Sniffer

Tobias Tefke[1], **Prof. Ralf C. Staudemeyer**[1]

[1] *Schmalkalden University of Applied Sciences, Schmalkalden, Germany*

October 9, 2025

Sniffing the network traffic can be used to find and debug potential network connection issues. This document describes how you can sniff the WiFi traffic of the PineCone with the use of the Wireshark tool.

Prerequisites

To be able to sniff the WiFi traffic, you have to do some steps first:

1. Install Wireshark:
   ```
   sudo apt install wireshark
   ```
2. Install the necessary Python libraries (note: activate your python environment first):
   ```
   pyenv activate bl_venv
   pip install -r ./tools/monitor/requirements.txt
   ```
3. Enable the sniffer in your project: add the following file to your `Makefile` (must be added before the last line):
   ```
   CFLAGS += -DWITH_SNIFFER
   ```

Sniffing

To start the sniffer, recompile your program with the set sniffer flag. Flash your application as usual. Before restarting the PineCone, start the monitor tool:

```
../../tools/monitor/monitor.py
```

Then, start Wireshark with the following parameters:

```
sudo wireshark -i /tmp/sniff
```

Click on `/tmp/sniff` in the capture selection dialog that opens. Now, restart the Pinecone. Any serial output is forwarded to the monitor tool. Using it is highly recommended when sniffing, as this tool filters out the captured packets that are also transferred over serial line.

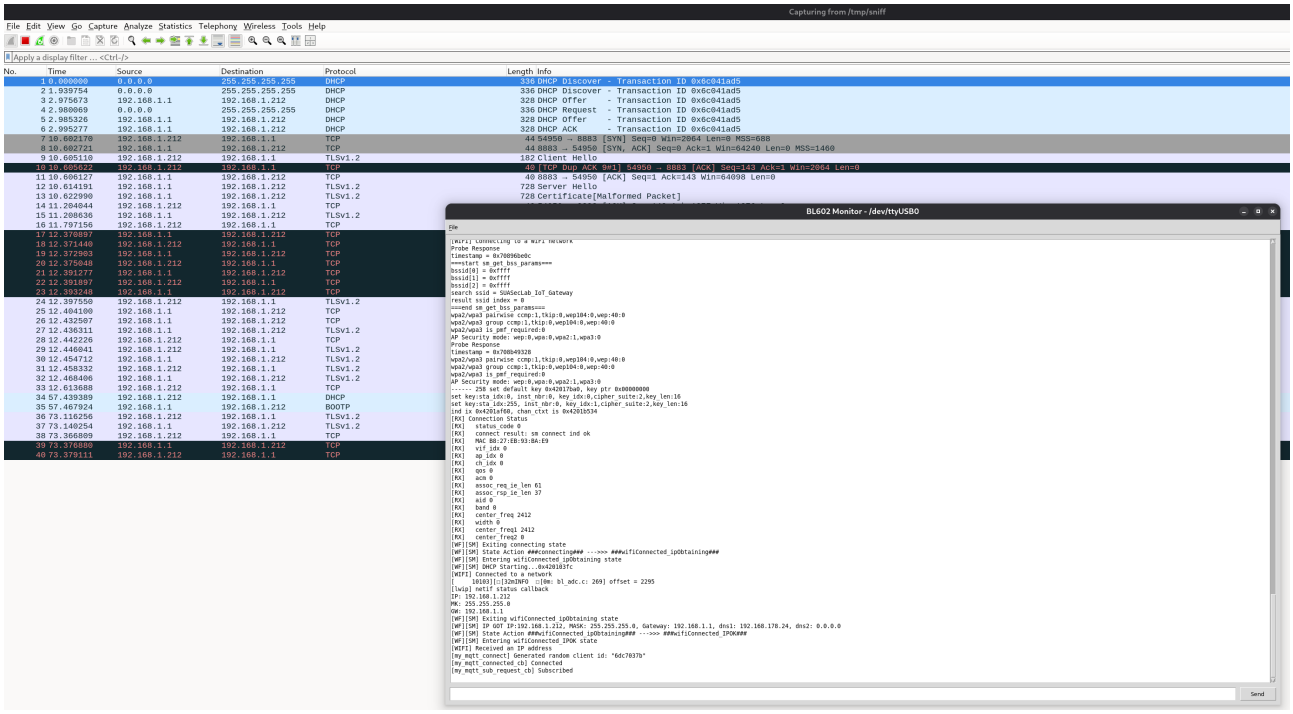

Figure 1: *The sniffer in action.*

As soon as there is some network traffic, it will be logged in Wireshark. There you can evaluate the traffic and look for potential issues. Your output should look similar to Figure 1.

Wireshark is a very versatile tool with regard to network sniffing and debugging. You can use it to examine all captured traffic in detail. For further information about Wireshark, refer to its documentation[1].

Hint: You can sniff several devices at the same time. You can have a look at the monitor tool's help for that:

```
../../tools/monitor/monitor.py -h
```

[1] `https://www.wireshark.org/docs/`