
Measuring PC-Island Response Times through Ethernet and WLAN

In this assignment, we evaluate the temporal response of the Modbus over TCP/IP protocol over two physical media: cable (Ethernet) and wireless (WLAN). Recall that different time behaviours can be observed due to two sets of reasons:

- The media have different medium access mechanisms and propagation characteristics;
- The Ethernet network is local to the room you're in; the WLAN network we will be using (*eduroam*) is local to FEUP, and thus packet routes are longer (i.e., go through more machines).

To observe the difference in time response, we will collect samples of the time interval elapsed between a Modbus query and response when Ethernet or WLAN is used. The tool Wireshark and some Excel data processing will be used. The measurements will be done first with WLAN.

1. Your bench PC should be equipped with a WLAN USB pen. Open the Windows' *'Control Panel' > 'Network and Internet' > 'Adapter Settings'*. This window shows you all the network interfaces in your PC. Disable the Ethernet configuration. Do not close the window.

2. Open the network configuration button on the Task Bar of Windows, in the bottom right of the screen. The button is symbolized by a signal power scale (or a PC, if the previous step was not successful). Select the '*eduroam*' network; input your credentials (**XXXXXX@fe.up.pt:<password>**). Now your connection to the Internet is via Wireless Local Area Network (WLAN).

3. Ping the island in your bench. Open the windows **command** terminal with command "**ping 192.168.113.XXX**". The address is written on the island. Check for a successful ping.

4. Trace the route that packets followed between your PC and the island: "**tracert 192.168.113.XXX**". This command lets you know all the machines that your packets went through before reaching the island. As mentioned earlier, the *eduroam* access point is not connected directly to the lab's cabled LAN as in the case of the Ethernet interface. Take note of how many hops the packets went through for later comparison with the Ethernet case (e.g., take a print screen of the terminal).

5. Open the **ModbusPoll** software in your computer. Set up a connection to the island by inserting the IP address in the appropriate connection field.

6. Open **Wireshark** and select the wireless interface. Once capture has started, select the filter input form (bar on the top of the capture window) and write '**mbtcp**', to restrict visualized packets to the Modbus over TCP/IP connection (as you did in the first lab assignment of this course).

7. After a few seconds of capture, stop it (hit the red 'Stop' button on the top toolbar of Wireshark). Make sure you collected a statistically significant number of Modbus query/response pairs (+100).

8. Identify the consecutive sets of "Query" and "Response" packets. Inspect the time interval between a query and the corresponding response. These are network response times over a wireless network.

9. On the top bar of Wireshark, select 'File' > 'Export Specified Packets'. Choose K12 format, that will provide you a human-readable, Notepad-friendly format of the logs. Call the file 'capture_wlan' or similar.

10. Open the file in Notepad++ and inspect it; you will see something like the figure below. Each entry is composed of a timestamp in the format “HH:MM:SS,milisecs,microsecs” and the packet in hexadecimal coding.

11. Let's do some light processing to facilitate importing into Excel. In Notepad++, open the 'Replace' tab (Ctrl+f) and check the option 'Match full word'. Replace all occurrences of 'ETHER' by '|ETHER', '|0' by '|||0', of commas ',' by an empty string (''), and of the packet delimiter '+-----+-----+-----+' by an empty string (''). Save the file. Ask help to your colleagues or professor if you hit any difficulties.

12. Import the file to Excel. An import support tool should pop up; when queried, indicate that the delimiter is '|', otherwise proceed along.

13. To learn which packets are the Modbus queries and the response, you need to get back to Wireshark and inspect them. Click on a few query and response packets and compare their hexadecimal code, particularly the last line as it corresponds to the **ModbusTCP** PDUs. Identify the minimum set of bytes necessary to distinguish queries from responses.

14. Once you identified a query, subtract consecutive time instants to get the time intervals between query and the corresponding response. Plot the histogram. To help you with the subtraction, consider the formula “=HOUR(A1)*3600 + MINUTE(A1)*60 + SECOND(A1)” to convert the HH:MM:SS into the second index for that day. In the unlikely event of unpaired queries, the **TRANSACTION IDENTIFIER** field may be of help.

15. The measurements using WLAN are complete, and the procedure must now be repeated with Ethernet. Go back to point 1, but now activate the Ethernet interface, and disable the WLAN interface. Repeat points 2 to 15; it should not take long be fast as now you have all the workflow set up.