CWM Programmable Networks

Exercise 1: Traffic capture

Introduction

As part of this exercise, you will learn how to capture network traffic, and how to inspect packets, using wireshark.

This exercise needs to be submitted as a pdf file via Canvas.

Setup

In this exercise you will use two machines: your lab machine, and a Raspberry Pi, connected directly using a single Ethernet cable. The cable should be connected from the lab machine's USB adapter to the Raspberry Pi's Ethernet port (no adapter).

To get started, open two terminals on the lab machine:

- One terminal will be used for measurements from the lab machine
- One terminal will be used for measurements from the Raspberry Pi
    - Connect to the Raspberry Pi using ssh (or use the second monitor, keyboard and mouse):
      ssh pi@192.168.10.2
- Identify the name of the Ethernet interface on your lab machine

  ```
  ip address show
  ```

  The Ethernet interface will have the IP address 192.168.10.1

- Start Wireshark on the lab machine:
  `wireshark &`

Traffic capture

- Select the Ethernet interface name that you have previously identified and start capture (capture->start or press the shark fin button)
  Do you see any packets captured? Describe the type of packets that are captured.
  Stop the capture.
- Start the capture again, this time capture on the network interface of the lab machine connected to the departmental network (ip address of the form 10.200.x.x).
  Try and capture http traffic.
  (Hint: use the filter line, look for examples under Capture->Capture Filters).
  Stop the capture.
  Describe what you had to do to capture http traffic, and provide a screen capture.
- Next, we capture on the Raspberry Pi using tcpdump.
  To capture using tcpdump run on the Raspberry Pi:
  `sudo tcpdump -i eth0`
  Such a run needs can break using ctrl+c
  Alternatively, use:
  `sudo tcpdump -i eth0 -c <number of packets> -w <output file>`

Example:

```
sudo tcpdump -I eth0 -c 10 -w captured.pcap
```

Captured packets can be read using -r option. Example:

```
tcpdump -r captured.pcap
```

(no sudo required!)

Provide a screen capture of the captured packets.

Sending traffic

- On the lab machine, change folder to the folder of the CWM's repository, assignment 1:
  ```
  cd ~/CWM-ProgNets/Assignment1
  ```
- Use the provided script to send 100 packets:
  ```
  python send.py <number of packets> <interface name> <source ip> <destination ip>
  ```
  Example:
  ```
  python send.py 100 eth0 192.168.10.1 192.168.10.2
  ```
  Make sure to use your machine's interface name!
- Make sure that wireshark is working, and start capturing on the interface connected to Raspberry Pi (192.168.10.1).
  ssh to the Raspberry Pi and change folder to the folder of the CWM's repository, assignment 1:
  ```
  cd ~/CWM-ProgNets/Assignment1
  ```
  Use the provided script to send 100 packets:
  (same as before)
  Check that the packets were captured on the lab machine, and answer the following questions:

1. Can you define a filter to capture only the packets you sent?
2. What is the packet size?
3. What is the protocol used (TCP or UDP)?

- Modify the script send.py to send TCP packets, source port 5555, 512B in size.

  Submit the file – either as a link to your repository, or as part of the pdf.

Upload the completed exercise to Canvas as a pdf.