L50 - Lab 2, Traffic Capture

Prof Andrew W. Moore after Dr Noa Zilberman

Michaelmas, 2021/2022

The goal of this lab is to learn about traffic capture and to get some hands-on experience in setting up traffic capture experiments.

As part of this lab you will not be required to write any scripts, or even command lines, and we expect that the majority of the lab will focus on the experimental setup and on the debug of the apparatus.

The lab allows you to compare between two capture tools:
tcpdump (based upon libpcap like wireshark), which is software based, and
Endace DAG, which is a hardware/software toolset.

As part of the lab we will use OSNT (an open source network tester) for traffic generation. We will not discuss OSNT or its limitations as part of this lab — this will be part of Lab 3. The experiments are conducted in a way that eliminates effects caused by the traffic generation tools.

1 Optical Tap

The experiments today will be using an optical network tap, which takes the inputs from Ports A and B, and sends a copy of each as an output on a third port. Note that the third port is output only — it has no input port, rather two outputs. The network tap's connectivity is illustrated in Figure 1.

Note that in the lab the connectivity is also drawn on the optical tap itself.

When connecting to the DAG, only the Rx of the DAG (the Tx of the tap) matters for traffic capture. In experiments 2.1 and 2.2 (a to d) you will normally connect the fibre to the DAG.

In experiment 2.2e, however, both outputs of the taping port will be used - one connecting to DAG port 0 and the other to DAG Port 1. Make sure to connect the fibre to the Rx of each port - the Rx is illustrated in Figure 2, and the setup is detailed in the notebook.

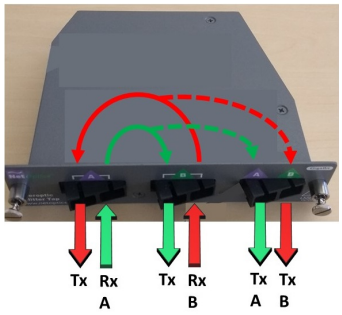

Figure 1: Optical Network Tap

Figure 2: Optical Transceiver

2 Saving Your Experiments

Make sure to back up your experiments, including (but not limited to) Jupyter notebooks, dump files and scripts. Remember that multiple teams may use the same test machines, so be careful when handling data.
All the measurements are saved under your crsid folder, so backing up the entire folder is a good idea. To copy a remote directory onto your local machine:
`sftp root@<hostname>.nf.cl.cam.ac.uk` and `get -r <directory>`.
There are also other ways to copy a remote directory, you are welcome to use those as well. You may wish to compress results files in order to save space.
Exporting a Notebook as `.tex` will save graphs as separate files, which you can then include in your lab report.

Please do not push any changes, data or results directly to L50 repository. You can fork the repository to your own user and push changes there. If you would like to suggest a correction or an enhancement to a notebook or a script, please use pull-requests.

3 Understanding Your Measurements

A single lab report will be required for the first three labs. Instructions for the lab report will be provided separately.
The following items are intended to help you understand your results, and may provide supporting evidence for your report. However, they are just suggestions - feel free to approach the data differently!

- Discuss the limitations of each of the capture tools.
- Compare and contrast software and hardware based packet capture.
- Explain how the test setup can affect measurements results and discuss how such effects can be mitigated.
- Explain how the limitations of traffic generation tools are mitigated in this lab.
- Explore the limitations of the experiments conducted in this lab, and explain where the quality of the experiment (e.g., setup, methodology) could have been improved.

You should always look for odd or surprising results, and try to explain them. Note that sometimes exceptional results indicate a problem in your setup or scripts.