CO223 – Computer Communication Networks I

Semester-3, 2017

Laboratory Session 2

# Network Tools for Investigation and Performance Measurement

---

*Instructions*:

- You are required to do each step (in part-1 and part-2) as instructed below.
- You are advised to discuss with the Instructors if you are not clear about any issues.
- You are required to write a report and submit within a week from your practical session. In your report, each problem/question should be addressed.
- You are advised to note any outputs and take trace files with you when you leave the laboratory (more information- in part-2) to recollect the activities later. These notes/files might help prepare a good report.
- Once this practical session is over, there will be 'Lab Evaluation' to test and evaluate the skills and knowledge gained in this and earlier sessions (Lab1 + Lab2). This evaluation is done individually.
- Marks: 60% from the Lab Evaluation and 40% from the reports (for Lab1 + Lab2).
- Time: 2 hours.

---

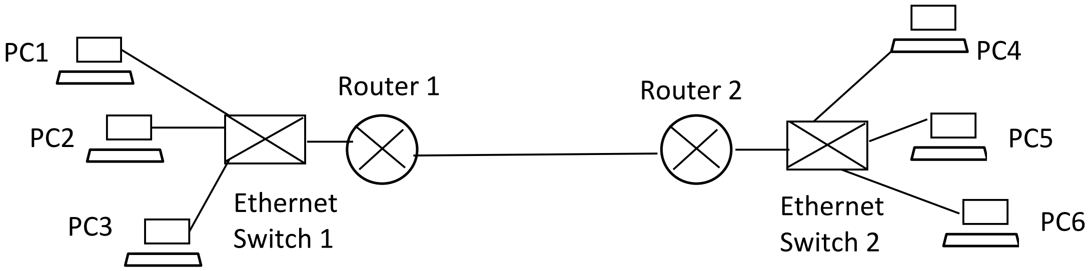

Fig. 1: A network

## Part-1: Network Tools

a. Get familiar with the network tool, **ping**,
   - Briefly describe its usefulness.
   - Test it in the network used in Lab-1 (Fig.1). Describe the different pieces of its output.
   - Identify how it can be used to measure 'delay'. Describe the type of delay it measures. Give your delay measurement in the network (Fig.1)

b. Get familiar with the network tool, **traceroute** (or **tracert**).
    - Briefly describe its usefulness. Describe how it differs from the network tool, ping.
    - Test it in the network (Fig.1). Describe the different pieces of its output.
    - Identify how it can be used to measure 'delay'. Describe the type of delay it measures. Give your delay measurement in the network (Fig.1).

c. With a PC connected to the Internet (through the university/home/other network), test with ping and traceroute tools for destinations: (1) www.ce.pdn.ac.lk, (2) www.google.com, and (3) other destinations of your choice [homework].
    - Compare your outputs for destinations (1) and (2). Sate reasons if there are any differences. Compare your outputs with the results seen in Part-1.a and Part-1.b above.
    - With the traceroute tool, do you observe that the delay *always* increases for each intermediate node (towards a destination such as www.google.com) starting from the source node? If not, what could possibly be the reasons for your observation?

d. Get familiar with network tools and commands such as 'ifconfig' (or 'ipconfig'), 'netstat', and 'tcpdump'.

## Part-2: Network Protocol Analyzer

- Discuss with the Instructors and get to know about 'packets' in computer networks.
- Discuss with the Instructors and get familiar with the network protocol analyzer, *Wireshark*.

a. Describe what a network protocol analyzer is and why it is used.

b. In Wireshark, get familiar with issues such as,
    - How to capture packets in a network
    - Where to set options when capturing packets (and how)
    - How to view the captured packets and their details
    - How to save the trace file and how to open a trace file for inspection
    - How to view the summary of results

c. Run the Wireshark at PCs in the network (Fig.1). Capture packets and observe any network traffic in the 'quiet network' with no network applications or tools running. Save the trace file (with the file name 'CO223_Lab2_2c_QuietNW').

d. Run ping and traceroute tools and capture packets to see the increased network activity. Save the trace files (with file names 'CO223_Lab2_2d_BusyNW_ping' and 'CO223_Lab2_2d_BusyNW_traceroute').

e. Compare the traces in Part-2.c and Part-2.d and briefly describe the differences.

Note: you are advised to take these trace files with you for later-inspection and for getting familiar with the Wireshark more. The Wireshark is freely available at https://www.wireshark.org.