Packet Trace Analysis

An exercise in understanding all you learnt in this course through packet traces and network diagnostic tools.

### Team size:2, Due: Friday December 4th, 2020

In this assignment you will take a direct look at packet traces and outputs of other networking commands and see packet switched networking in action. You will observe evidence of almost everything we learnt in our journey through the 5 layers of Computer Networks - PHY, LINK, NET, TRANSPORT, APPLICATION. The headers and their values we saw in theory, you will actually see rendered on the packet analyzer. You will be able to see the impact of networking mechanisms that you can’t actually observe, because they happen somewhere else in the network, through some values and other behaviour seen in the packet trace you have. You will also try out some related networking commands that lead to better understanding of how the Internet works.

This assignment has multiple parts - few packet traces will be supplied to you and some questions will be suggested as practice of how a packet trace can be analyzed, and how other system commands can be used to understand what’s happening. The last part will involve you capturing a packet trace yourself, and studying it. This last part is fairly open-ended and will allow each team to be as curious as it wants and find out as much as it wants.

In all these lab statements, ignore the marks written next to the questions, they are merely indicative, we may not grade according to those marks. *Also, a few more questions may get added to these labs over next few days, but you can get started.*

1. [Task 1 - A warmup lab](https://docs.google.com/document/d/1wpQ9RNlkZDI0ujs-nK01M-pIZxfhA4Gt_M26sP0-BZo/edit#heading=h.i69n4oyt3ra1)
2. [Task 2 - An IP focussed lab](https://docs.google.com/document/d/1kfjvOf5hk1Su5bgOHhXMRQWg7dnE8Z1o5lBtyImP8N8/edit#heading=h.px41pftamu32)
3. T[ask 3 - A TCP focussed lab](https://docs.google.com/document/d/1C-5m1S5B4c15MPQDuvVJzUu9g25zKkfM1fafcSFwg_E/edit#)

All packet traces are in the studentShare on DROPBOX under the packetraces sub folder.

### Task 4

This task requires you to install wireshark on your laptop, and in general be able to issue commands such as netstat, route, ping, traceroute etc. Detailed hand-holding guidance will not be provided for these, you should use ‘man’ (in Linux) or google searches to learn. Almost all of these are available on your windows also (command prompt)

Pick 1-2 multimedia applications that you use a lot (and was not already studied in the tasks above). Examples -

* MS Teams
* Zoom
* Facebook audio/video
* Some music website

E.g. if you pick zoom - run experiments such as a video conference between you and your partner while capturing packets and issuing other commands such as netstat.

Run packet tracing and other experiments to find out essentially all you can think of and curious about. Example questions (more will get added over some time)-

* Details about your own network (your laptop IP configuration, your Gateway router info), your public IP address, anything about your ISP - what seems to be the address space it owns?. These questions both team members should explore.
* Server IPv4 and v6 addresses
* Where are the servers located?
* What transport layer is being used
* How many Simultaneous Transport layer sessions
* Is the communication peer to peer
* What’s the application layer protocol for the streaming part
* What seems to be the application layer session setup protocol
* What is the bandwidth requirement per user? How does it grow with number of users (multiple teams can collaborate for this)
  + What is it with video, without video, etc
* What are the round trip times, what are the one-way delays
* What is the route, how many hops?
* What is the jitter (variance of packet interarrival times)
* What is the transport layer protocol behaviour - what seems to be the nature of the packet traffic when it *leaves* your laptop - how does it change when it *arrives* at the other end? (try and see if you can plot this and compare). Packet traffic is characterized by :
  + Packet size, inter-packet delay or packet size and packet sending/arrival rate, and all of this should also be viewed in the units of bit rate
* //more questions will be added

You can also think of other questions and answer them. Asking good questions will get as much credit as answering above questions.