Assignment 02 Task 03: TCP Analysis

# TCP Traces

In the [download material given](https://www.dropbox.com/sh/mg13efpyhbgt5o9/AACFjcaAMMEDcZivbC0ezHR7a?dl=0) there are various traces, netstat outputs etc.

Unless otherwise mentioned, all traces are taken from my laptop, while on my home WiFi which has private addresses of the type 192.168.\*.\*. The public IP address of my home WiFi is 180.151.244.118. Also, surya’s (login.iitb) public IP address 103.21.126.139.

The following traces are included in respective directories. In some directories there is netstat output also

1. scpFromSurya: File being downloaded from surya. Here there are two traces: one from the laptop, one from surya. Note that to take the trace on surya, I had to have an ssh connection open to surya, before I could take the trace. Also netstat output was taken **every one second** from before the scp command was given till some time after the scp was completed.
2. scpToSurya: trace taken on laptop during scp-ing a file TO surya
3. sshToSurya: trace taken on laptop during ssh to surya.
4. hangout: trace taken on laptop during a two-person Google hangout session with another device on my home wireless LAN.
5. skype: trace taken on laptop during a two-person Skype session with another device on my home wireless LAN.
6. youtube: trace taken on laptop during a youtube viewing

All questions pertain to packet trace only of the major activity for which the trace was taken. You need to filter appropriately and ignore all other packets.

## Questions

1. Compare the sshToSurya trace with the scpToSurya trace. There is a difference in TCP flag settings in these traces. What is it and why is it so? (1 + 2 marks)
2. In the scpToSurya trace.
   1. what is the point at which you can be sure that the TCP congestion window size has increased beyond 1 packet? (State wireshark packet number range, which represents the "window full of packets"). At this point, what could be, in terms of number of packets, the window size? (2 marks)
   2. What is the smallest frame length? Briefly explain it. (2 marks for answer explanation)
   3. What is the maximum frame length? Briefly explain it. (2 marks for answer explanation)
   4. At which packet number do you think the actual file transfer started (as opposed to tcp and scp setup messages)? Explain why. (2 marks)

3) Now look at the scpFromSurya set of traces. (suryaTrace, and laptop trace).

3.1) In the suryaTrace, look at packet number 1590. It has been tagged by wireshark as a Duplicate Ack.

3.1.1) This indicates the delay/loss of which packet? (Refer to packets by their TCP sequence numbers). (1 mark)

3.1.2) What else does an arrival of a duplicate ACK indicate? (2 marks)

3.1.3) At this point, how many bytes have been sent by surya but not acknowledged yet? (2 marks)

3.1.4) What is happening in wireshark packet numbers 1591 and 1592? (1 marks)

3.2 Now look at laptopTrace.

3.2.1) Which is the first wireshark packet (number) that is related to

the duplicate ack arrival at surya? What is happening in that packet? (2 marks)

3.2.2) The TCP receive window on the laptop now has a "hole". How big

is ths hole (in bytes)? (2 marks)

3.3) In general look at this whole "duplicate acks" episode on both

the traces and explain what happens until normal transfer begins. You

must CORRELATE the two traces in your explanation. (4 marks) (mention fresh packet number started with)

3.4) Which TCP connection states do you see for the scp connection, in

the netstat output? (no marks)

3.4.1) How long does the TIME\_WAIT state last? Explain how you got this answer. (2 marks)

4) The youtube, hangout and skype traces are all of multimedia traffic.

4.1) Which IP address(es) is hangout connecting to the most? (1 + 1 marks for exp)

4.2) Which IP address(es) is skype connecting to? Who do they belong to? (2 + 2 marks

4.3) Compare and contrast these three traces, highlighting the

most meaningful conclusions (do not waste time on comparisons that

have no conceptual value.) Remember to mention points related to the

transport layer, and any other conclusions about how the applications

seem to work. (6 marks 2 youtube , hangout and skype)