Assignment
Wireshark (Transport Layer - TCP)

Assignment Questions (Transport Layer)

1. Download a large file (i. ubuntu image from **Internet** and ii. Ubuntu image from **intranet**). 60 seconds of observation is sufficient. Plot the following metrics from wireshark
    a. Plot the estimated Round Trip Time (RTT) variation for intranet and internet download (2 marks)
    b. Plot the TCP Congestion window (or the difference in ack numbers - bytes delivered) for both intranet and internet download. X-axis is time and Y-axis is byted delivered (X ticks for each RTT , hence sum up the bytes delivered over each RTT). (3 marks)
    c. Get the flow graph (Statistics - flow graph) (2 marks).
    d. What is the average throughput observed in both cases (2 marks)
    e. Plot the the receiver congestion window advertised over time (2 marks)
    f. Plot the number of 1-duplicate ack, 2-duplicate ack and 3-duplicate acks received over time (1+1+1 = 3 marks)
2. Download a small file and identify the the TCP 3 way handshake?
3. Ping a host and and capture the packets with wireshark. What kind of packets are generated by the ping command?
4. Use nmap (using command nmap –PS [neighbours ip address]) to perform the host scan (same as used in previous question) and

capture the packets with wireshark. What kind of packets are generated by nmap?

Note:

1. For all the experiments write the inferences which you have observed.
2. Put the screenshot in the report for better clarity. Submit the pdf file of report in google classroom with filename as your roll number.

Check Web sources for more information