Wireshark for Transport Layer Protocols

Capture and analyze the packet traces using the Wireshark to answer all the questions. Use appropriate filters, helper windows, properties in Wireshark. Place the screenshots of wireshark where appropriate inline to answers, as a proof of analysis in answering the question.

Task1: iperf3 to remote server in UDP

You will require iperf3 software to execute this experiment. (Follow the instructions from the initial tutorial session on Wireshark).

Start the Wireshark packet sniffer and start capturing.
Open a terminal
Start iperf3 in client with reverse mode destined to ping.online.net as
iperf3 -u -t 10 -c ping.online.net -p 5208 -R
Once the iperf3 communication is complete stop the Wireshark packet capture

1. How many UDP packets are exchanged in this communication between iperf3 client and remote server ?

2. Who is sending bulk data to whom ? What is the average size of the packet sent ?

3. Calculate the throughput (bytes transferred per unit time) for this UDP conversation using UDP's length field. Explain how you calculated this value using Wireshark capture in this experiment along with relevant screenshots. Verify your calculation with the one done by Wireshark using "Capture File properties" as well with the one displayed by iperf3 terminal. If you observe the major difference in your calculation and with the other two listed here, comment why and how ?

Task2: Bulk File Download with TCP

Start the Wireshark packet sniffer and start capturing. Visit http://ping.online.net/ on browser.
From the bottom most list in the site "Download test files from this server :".

a. Click on 2Mo.dat to download and save the respective file to your host machine successfully. Stop the wireshark capture and save the file for further analysis.
b. Click on 50Mo.dat to download and save the respective file to your host machine successfully. Stop the wireshark capture and save the file for further analysis.
c. Click on 200Mo.dat to download and save the respective file to your host machine. While this file gets downloaded cancel the download after 2-3 seconds. Stop the wireshark capture and save the file for further analysis.

For #a and #b downloads listed above, answer the following using the respective captured files.

1. How many TCP packets are exchanged in this communication client and remote server?

2. What is the minimum amount of available buffer space advertised at the client/receiver for the entire trace?

3. Pick any 5 TCP segments from server to client which are **not** part of initial TCP connection establishment and final connection termination.
   3.1. Make a table listing for each of these segments, the length of each of these TCP segments, the sequence number, time when the segment was sent, time when the respective ACK for each segment was received, length of the respective ACK segment. Place the screenshot of Wireshark of at least one such segment with respective ACK as a proof of observation and calculation.
   What is the maximum length out of all ?

   3.2. Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of these segments? What is the EstimatedRTT value after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation (From chapter 3 of the referred text book in the class) for all subsequent segments. Place these calculated values appropriately in the table formed in #b above.

$$EstimatedRTT = (1 - \alpha) \times EstimatedRTT + \alpha \times SampleRTT$$

$$where\ \alpha = 0.125\ (that\ is,\ 1/8)\ [RFC\ 6298]$$

   3.3. Plot the RTT Graph for any TCP segment out of these using the graph feature of Wireshark. Plot another graph manually from the table above for Sample RTT and estimated RTT (Similar to “RTT samples and RTT estimates” graph from section “Round-Trip Time Estimation and Timeout” of the referred textbook in the class).

   3.4. Comment on your understanding of Estimated RTT calculation and plotted RTT graphs.

4. Calculate the overall throughput (bytes transferred per unit time) for this TCP conversation using different fields of TCP from the captured file. Explain how you calculated this value using Wireshark capture in this experiment along with relevant screenshots. Verify your calculation with the one done by Wireshark using “Capture File properties”. If you observe the major difference in your calculation and one calculated by Wireshark, comment why and how ?

5. Using any active TCP segment (pick the packet of bulk data length, e.g: 5668) involved in the download process from server to client, capture the TCP's functioning using the Time-Sequence-Graph (Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the server to the client. Can you identify where TCP's slow start phase begins and ends, and where congestion avoidance takes over? If not possible, why ?

Only for #c above, observe and clearly explain with screenshots, how TCP connection gets terminated in this case, as well as which fields of TCP influence this, due to canceling of the download in between.

Submission

Prepare a detailed **observation and analysis report** for listed questions with specific details asked in individual tasks along with **respective wireshark trace files**. Zip all these files into a single zip file **<assignment3_roll no>.zip** and submit to google classroom in the posted assignment section.

PLAGIARISM STATEMENT <Include it in your report>

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.

Name of the student
Roll No