[CS-335a] ASSIGNMENT 3

To TCP or to UDP? That is the question

Deadline: **28/11/2025** 11:00 a.m. **(morning)**
Professor: Maria Papadopouli
TA: Mario Alexios Savaglio

Part 1: Theory (45 points)

Question 1 [30 points]: Below, there are some statements concerning UDP and TCP. Comment on their validity. Provide a precise, clear and brief justification of your answers **[3 points each]**

- UDP is a connection-oriented protocol, while TCP is connectionless.
- The TCP congestion control and TCP flow control both involve buffers. If true, explain how.
- TCP transmits data faster than UDP because it doesn't check for errors.
- When transmitting data using UDP, the destination IP address needs to be specified, but the destination port does not.
- TCP provides reliable data transfer by using acknowledgments and retransmissions.
- Congestion control ensures that the sender will not overwhelm the receiver.
- UDP includes flow control, but not congestion control mechanisms.
- TCP segments are reassembled in the correct order by sequence numbers.
- SampleRTT is the measured time from segment transmission until its receipt.
- In a TCP connection, if the sender receives 3 additional ACKs for an already received segment ("triple duplicate ACKs"), it resends the unACKed segment with the largest sequence number.

Question 2 [15 points]: Provide brief and clear answers to the following questions:

1. Explain the process by which TCP establishes a reliable connection between two devices. Describe each step of the process, what information is exchanged and why. **[5 points]**

2. Describe how TCP ensures that data is delivered in the correct order. (Hint: Explain the role of sequence numbers and acknowledgment numbers and how they are used by the protocol.) **[5 points]**

3. Explain how TCP uses congestion control to adapt to the different traffic conditions. Describe slow start and congestion avoidance. **[5 points]**

Part 2: Problems on TCP (65 points)

Question 1 [35 points]: Assume two hosts A and B that communicate over a TCP connection. Host B has received all the bytes from Host A until the 523th byte. Afterwards, Host A sends two segments to Host B one after another. The first segment contains a payload of 20 bytes, while the second one contains 50 bytes. The source port from Host's A side is 92 and the destination port is 88. Host B sends an acknowledgment each time it receives a TCP segment.

- Draw the TCP flow diagram between Host A and Host B, assuming that the two segments arrive in the correct order, without any packet lost. You can ignore Host's B sequence number as no relevant information is given. What is the sequence number of the second segment? Explain. **[10 points]**

- What are the source and destination port numbers of the ACK segments sent from Host B to Host A? **[7.5 points]**

- Assume that the second segment reaches Host B before the first segment. What is the acknowledgement number returned by Host B as a response to the arrival of the second segment? explain. **[7.5 points]**

- Assume that the two segments arrive at Host B in the correct order but both of the responses of Host B are lost. Draw the TCP flow diagram between Host A and Host B, and include the retransmission that will happen in the diagram. Which TCP mechanism will trigger the retransmission? Can Host A be certain about what actually happened? **[10 points]**

Question 2 [30 points]: The diagram below demonstrates an example of the behavior of a specific TCP flow over time. Answer the following questions, with sufficient justification.

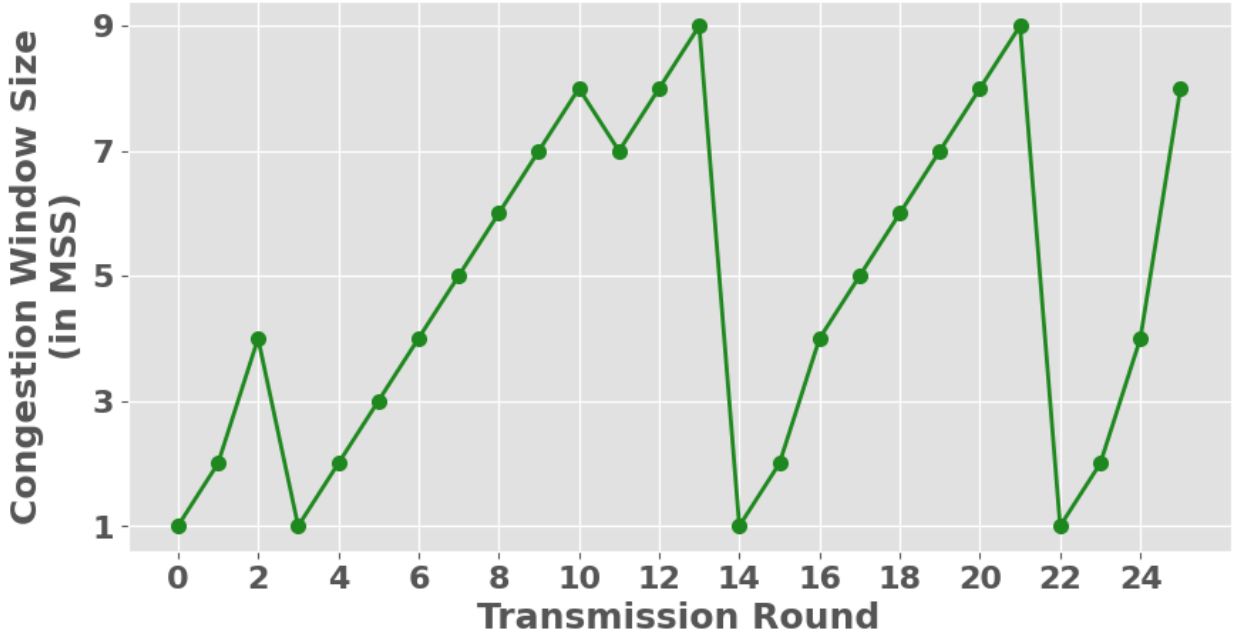

Figure 1. Congestion window size as a function of time. The x-axis represents transmission rounds (in RTTs), and the y-axis indicates the congestion window size (in segments).

- Identify the time intervals when TCP slow start operates. How can we understand that? **[5 points]**
- Identify the time intervals when TCP congestion avoidance operates. How can we understand that? **[5 points]**
- After the 21st transmission round, a severe drop to the size of the congestion window is observed. What could have caused that? Speculate about the traffic in the network at this time period. **[5 points]**
- After the 10th transmission round, a less severe drop of the size of the congestion window is observed. What could have caused that? Speculate about the traffic on the Internet at this time period? **[5 points]**
- What is the value of cwnd during the 11th transmission round? Justify your answer. **[5 points]**
- What is the value of ssthresh during the 14th transmission round? Explain. **[5 points]**

Part 3: Hands-on Exercise — Measurements & Analysis (20 points)

Question 1 [20 points]: Here you need to employ Wireshark. Import the following trace file (https://kevincurran.org/com320/labs/wireshark/trace-tcp.pcap) which contains a trace of a TCP flow between a host and a server. Answer the following questions by explaining your answers and providing screenshots from Wireshark.

- What is the IP address of the host initiating the TCP connection? Which are the source and destination port numbers that this host uses on its TCP segments? Provide screenshots to back up your answer. **[5 points]**

- Identify the TCP segments that correspond to the 3-way handshake. Indicate the flags and their values in the header of these segments? Provide screenshots to back up your answer. Do the flags set on these packets agree with what you have learned in theory? **[5 points]**

- Select a random TCP segment. Indicate the sequence number, the ACK number, and its payload size. Provide screenshots to back up your answer. What is the expected ACK number from the other side as a response to this segment? Does it agree with the corresponding response ACK shown in Wireshark? **[5 points]**

- Determine the length (in bytes) of each of the TCP header fields by examining a random TCP segment. Provide screenshots to back up your answer. **[5 points]**