[CS-335a] ASSIGNMENT 3

To TCP or to UDP? That is the question

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. **Answer: False** TCP requires a connection to be established before data transfer; UDP does not.
- The TCP congestion control and TCP flow control both involve buffers. If true, explain how. **Answer:** True, Flow control involves the buffer of the TCP receiver; congestion control the buffers of the routers.
- TCP transmits data faster than UDP because it doesn't check for errors. **Answer: False** UDP is faster because it skips error checking and connection setup.
- When transmitting data using UDP, the destination IP address needs to be specified, but the destination port does not. **Answer: False** Both the destination IP and port need to be specified.
- TCP provides reliable data transfer by using acknowledgments and retransmissions. **Answer: True** TCP ensures data delivery through ACKs and by resending lost packets.
- Congestion control ensures that the sender will not overwhelm the receiver. **Answer: False** This is flow control.
- UDP includes flow control, but not congestion control mechanisms. **Answer: False** UDP does not have flow or congestion control.
- TCP segments are reassembled in the correct order by sequence numbers. **Answer: True** TCP uses sequence numbers to ensure data is reassembled correctly.
- SampleRTT is the measured time from segment transmission until its receipt. **Answer: False** measured time from segment transmission until ACK receipt, not considering retransmissions
- 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. **Answer: False** It resends the segment with the smallest 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]** **Answer:** TCP establishes a reliable connection between two devices using a process called the three-way handshake. First, the client sends a SYN packet with an initial sequence number to request a connection. The server responds with a SYN-ACK packet, acknowledging the client's request and providing its own sequence number. Finally, the client sends an ACK packet back to confirm receipt of the server's message. This exchange ensures both devices are synchronized and ready to send and receive data reliably, allowing TCP to provide accurate and ordered communication using the sequence numbers.

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]** **Answer:** TCP ensures that data is delivered in the correct order by using sequence numbers and acknowledgments (ACKs). Each byte of data sent over TCP is assigned a sequence number, allowing the receiver to identify the exact order of the segments. When the receiver gets a segment, it sends back an acknowledgment with sequence number X+1 (byte), where X is the largest sequence number of packets up to which it has received without gaps. If packets arrive out of order, TCP temporarily stores them and rearranges them based on their sequence numbers before delivering the data to the application, ensuring reliable and ordered communication.

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

1. Slow Start

The Slow Start phase allows TCP to quickly find the available bandwidth at the start of a connection or after a timeout.

- For each acknowledgment (ACK) received, the cwnd increases by one MSS, meaning it doubles every round-trip time (RTT) (exponential growth).
- This continues until the cwnd reaches the slow start threshold (ssthresh) or until packet loss is detected.

2. Congestion Avoidance

Once cwnd exceeds ssthresh, TCP switches to Congestion Avoidance mode.

- In this phase, TCP increases cwnd more slowly, roughly by one MSS per RTT (linear growth).
- This prevents the sender from overwhelming the network as it approaches its capacity.

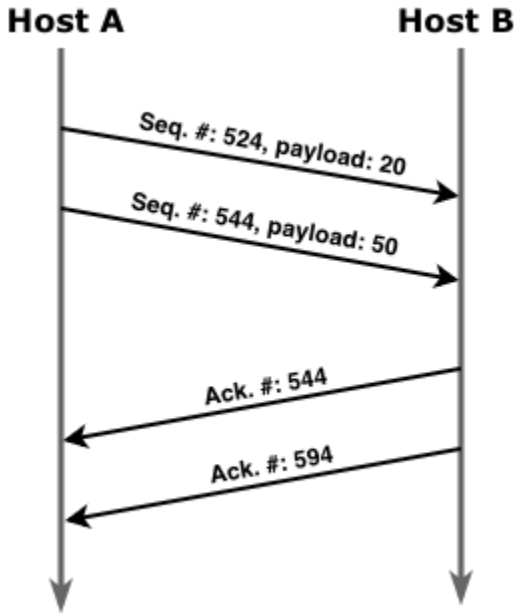
If packet loss occurs, ssthresh is again set to half of cwnd, and TCP may either enter Fast Recovery (if duplicate ACKs are received) or return to Slow Start (if a timeout occurs).

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]**

Answer: The sequence number of the second segment is Seq. # of segment 1 + payload of segment 1. Thus, it is equal to 524 + 20 = 544.



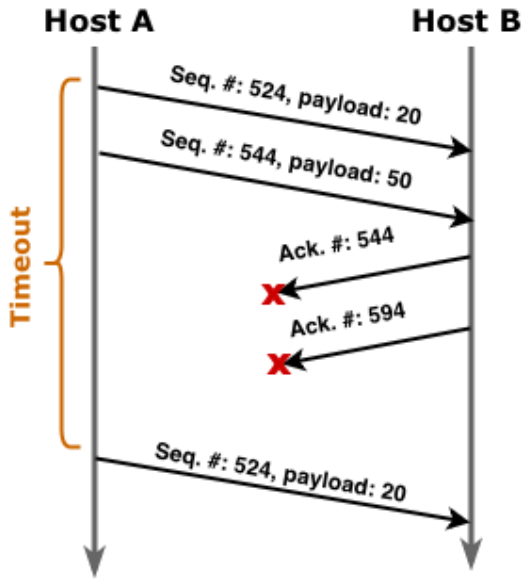
- What are the source and destination port numbers of the ACK segments sent from Host B to Host A? **[7.5 points] Answer:** Source port number is 88 / destination port number is 92

- 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] Answer:** Host B is expecting the 524th byte but he receives the 544th . So, his ACK number would be 524.

- 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]**

Answer: The retransmission will be triggered by a timeout. Host A cannot know whether the segments reached host B.



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.

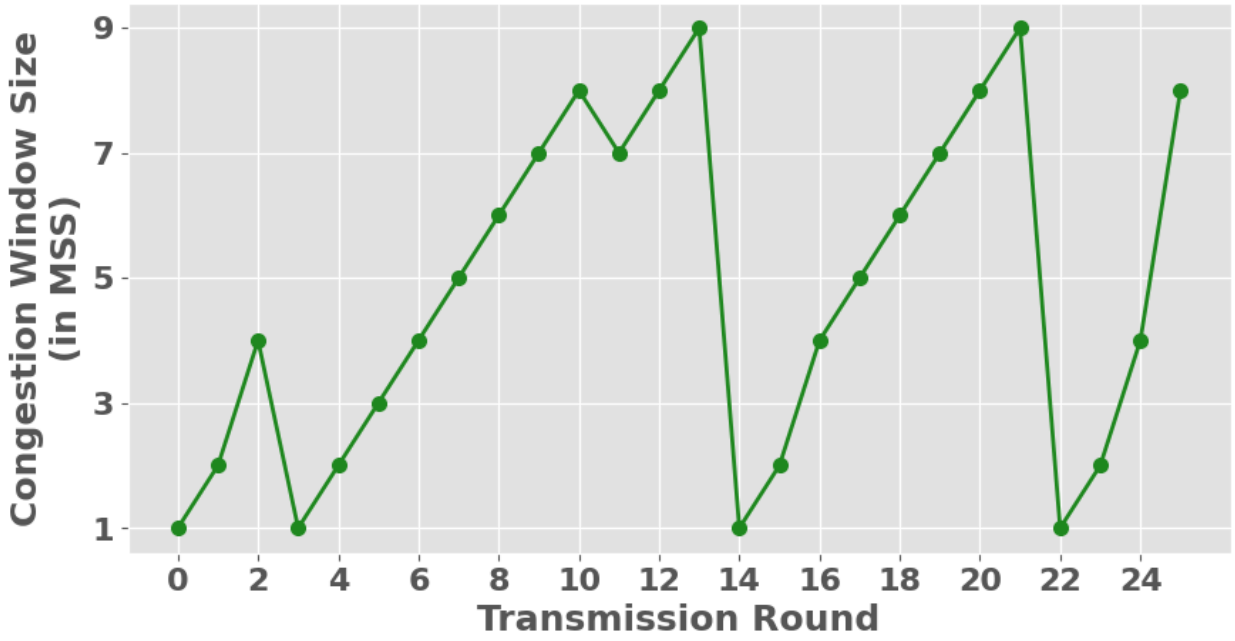


Figure 1. Congestion window size as a function of time. The x-axis represents transmission rounds (in RTTs), and the y-axis indicates the congestion window size (in segments).

- Identify the time intervals when TCP slow start operates. How can we understand that? **[5 points]** **Answer:** [0-4], [14-16], [22-25]. This can be deduced from the fact that the congestion window doubles each round.

- Identify the time intervals when TCP congestion avoidance operates. How can we understand that? **[5 points]** **Answer:** [5-13], [16-21]. This can be deduced from the fact that the congestion window increases by one MSS each round.

- After the 20th 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]** **Answer:** This was caused by a timeout, since it reset the congestion window size to 1 MSS and it switched to slow start.

- After the 9th 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]** **Answer:** This was caused by a triple duplicate ACK, since it set the congestion window size to half its current size and it remained in congestion avoidance.

- What is the value of cwnd during the 10th transmission round? Justify your answer. **[5 points]** **Answer:** Since the drop was caused by a triple duplicate ack, the congestion window is set as cwd = cwd / 2 + 3. Since the congestion window had a size of 8 when the drop happened, the new size will be 8 / 2 + 3 = 7.

- What is the value of ssthresh during the 13th transmission round? Explain. **[5 points]** **Answer:** Since the drop was caused by a timeout, the threshold is set as ssthresh = cwd / 2. Since the congestion window had a size of 6 when the drop happened, the threshold will be set to 6 / 2 = 3.

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]**