**Wireshark 3: TCP**

**Group Details:**

Bahareh Farhadi 1003975282

Jingfeng Chen 1000411262

**Mark:**

|  |  |  |
| --- | --- | --- |
|  | **Question** | **Answer** |
| 1 | What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? | IP: 192.168.1.102 Port: 1161 |
| 2 | What is the IP address of gaia.cs.umass.edu? On what port number is it sending  and receiving TCP segments for this connection? | IP: 128.119.245.12 Port: 80 |
| 3 | What is the IP address and TCP port number used by your client computer  (source) to transfer the file to gaia.cs.umass.edu? | No, I do not have my own trace file.  (I tried and the data collected looked weird and did not contain what I was looking for) |
| 4 | What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it  in the segment that identifies the segment as a SYN segment? | Sequence: 0 (relative) or 0dd601f4    SYN flag is 1: |
| 5 | What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a  SYNACK segment? | Sequence: 0 (relative) or 34a27419  ACK: 1 (relative) or 0dd601f5  SYN-ACK sequence will always be SYN sequence + 1  Both flags is 1 |
| 6 | What is the sequence number of the TCP segment containing the HTTP POST command? | Sequence: 1 (relative) or 0dd601f5 |
| 7 | Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received?  Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value after the  receipt of each ACK? | Sequence: 1, 566, 2026, 3486, 4946, 6406  Time sent: 0.026477, 0.041737, 0.054026, 0.054690, 0.077405, 0.078157  Time Received: 0.053937, 0.077294, 0.124085, 0.169118, 0.217299, 0.267802  RTT: 0.02746, 0.035557, 0.070059, 0.114428, 0.189645  EstimateRTT: 0.02746, 0.043654, 0.104561, 0.158797, 0.264862 |
| 8 | What is the length of each of the first six TCP segments? | Length: 565, 1460, 1460, 1460, 1460, 1460 |
| 9 | What is the minimum amount of available buffer space advertised at the received  for the entire trace? Does the lack of receiver buffer space ever throttle the  sender? | Minimum: 6780 and no it did not throttle the sender. |
| 10 | Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question? | No, there is no retransmitted segments in the first 10 packets. Because there is no duplicated sequence number. |
| 11 | How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment | 1404 or 2808 bytes. The receiver will acknowledge every other received packets when all the packets up to the expected sequence number have arrived and acknowledged.  Example: |
| 12 | What is the throughput (bytes transferred per unit time) for the TCP connection?  Explain how you calculated this value. | Throughput = data size / transmition time.  148539 \* 8 / (5.651141 - 0.026477) = 211268 bits / s |
| 13 | Use the Time-Sequence-Graph (Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP’s slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we’ve studied in the text. | Within the first 0.2 second, TCP is in slow start. It then enters congestion avoidance where the transmission rate slows down apone reaching the threshold. After that the rate is kept at a constant rate of 6 packets at a time. This is different from linearly increase the transmission. |
| 14 | Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu | This is the graph from my own trace, which does not look correct because the entire transmission should remain in a slow start state. |