**Wireshark Assignment**

**Question and 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?**

Source IP Address: 192.168.1.102

Source TCP Port Number: 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?**

Destination IP Address: 128.119.245.12

Destination TCP Port Number: 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?**

Source (Local) IP Address: 192.168.1.21

Source (Local) TCP Port Number: 65013

**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?**

* The sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.ucmass.edu is 0.
* The segment that identifies the segment as a SYN segment is the SYN flag in the Transmission Control Protocol which is set to SET, whereas all the others are set to NOT SET.

**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?**

* The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.
* The value of the acknowledgement field in the SYNACK segment is 1.
* This value of the acknowledgement field is determined by adding 1 to the initial sequence number. The initial sequence number here is 0. Hence the value of the acknowledgement field is 0+1=1.
* The segment that identifies the segment as SYNACK is the SYN and ACK flag in the Transmission Control Protocol which are both set to SET, whereas all the others are set to NOT SET.

**6. What is the sequence number of the TCP segment containing the HTTP POST command?**

* The sequence number of the TCP segment containing the HTTP POST command is 1. This is the first segment with the PUSH flag set to SET. This is the segment which contains POST in the data field.

**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? 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 on page 242 for all subsequent segments.**

* Considering HTTP POST as the first segment in the TCP connection, the first six segments which were sent and their acknowledgments, along with their sequence numbers, time at which they were sent/received and their RTT values are as follows.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sent | | | | | Received | | | | RTT | Estimated RTT |
| Segment Number | Length | Sequence Number | Ack Number | Sent Time | Segment Number | Sequence Number | Ack Number | Received Time | = Received Time - Sent Time | = 0.875 • EstimatedRTT + 0.125 • SampleRTT |
| 4 | 565 | 1 | 1 | 0.026477 | 6 | 1 | 566 | 0.053937 | 0.02746 | 0.02746 |
| 5 | 1460 | 566 | 1 | 0.041737 | 9 | 1 | 2026 | 0.077294 | 0.035557 | 0.028472125 |
| 7 | 1460 | 2026 | 1 | 0.054026 | 12 | 1 | 3486 | 0.124085 | 0.070059 | 0.033670484 |
| 8 | 1460 | 3486 | 1 | 0.05469 | 14 | 1 | 4964 | 0.169118 | 0.114428 | 0.043765174 |
| 10 | 1460 | 4946 | 1 | 0.077405 | 15 | 1 | 6406 | 0.217299 | 0.139894 | 0.055781277 |
| 11 | 1460 | 6406 | 1 | 0.078157 | 16 | 1 | 7866 | 0.267802 | 0.189645 | 0.072514242 |

EstimatedRTT = 0.875 • EstimatedRTT + 0.125 • SampleRTT

EstimatedRTT:

Segment 1 is 0.02746 (Given EstimatedRTT = Measured RTT for Segment 1)

Segment 2 is (0.875 \* 0.02746000 + (0.125 \* 0.035557) 0.028472125

Segment 3 is (0.875 \* 0.028472125 + (0.125 \* 0.070059) 0.033670484

Segment 4 is (0.875 \* 0.033670484 + (0.125 \* 0.114428) 0.043765174

Segment 5 is (0.875 \* 0.043765174 + (0.125 \* 0.139894) 0.055781277

Segment 6 is (0.875 \* 0.055781277 + (0.125 \* 0.189645) 0.072514242

**8. What is the length of each of the first six TCP segments?**

As shown in the above table, the length of the first six TCP segments are 565 Bytes (1st segment) and 1460 Bytes (2nd till 6th segment)

**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?**

* On analyzing the entire trace, we can see that the minimum amount of the available buffer space advertised is 5840 Bytes.
* The trace also shows that the receiver buffer space never throttled the sender in any segment. We can see that the window size was always greater than the size of the data which was being transmitted.

**10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?**

On filtering the segments using **tcp.analysis.retransmission** or **tcp.analysis.fast\_retransmission**, there are no results displayed. This confirms that there were no retransmitted segments in the trace file. Moreover, from the Time Sequence (Stevens) graph we can see that the sequence numbers are continuously increasing throughout the trace.

**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?**

* 1460 Bytes of data is used to acknowledge in an ACK.
* No. There are no cases where the receiver is ACKing every other received segment.

**12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.**

Throughput = Bytes Transferred / Unit Time

Size of the file which was transmitted = 155648 Bytes

Total Time Taken = Last Segment – First Segment = 7.595557 – 0.0 = 7.595557 Seconds

Hence the throughput is 155648/7.595557 = 20491.98 Bytes/Second or 163935.8 bits/second

**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.**

* TCP’s Slow Start phase begins at 0 and ends at 0.15 second (Approximately 0.2 Seconds).
* Congestion avoidance takes over the slow start from 0.15 seconds (Approximately 0.2 Seconds).

**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?**

* **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?** 
  + The sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.ucmass.edu is 0.
  + The segment number is 190 which is the first segment related to this session of uploading the file from local machine to gaia.cs.umass.edu.
  + The segment that identifies the segment as a SYN segment is the SYN flag in the Transmission Control Protocol which is set to SET, whereas all the others are set to NOT SET.
* **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?**
* The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.
* Related segment number is 192
* The value of the acknowledgement field in the SYNACK segment is 1.
* This value of the acknowledgement field is determined by adding 1 to the initial sequence number. The initial sequence number here is 0. Hence the value of the acknowledgement field is 0+1=1.
* The segment that identifies the segment as SYNACK is the SYN and ACK flag in the Transmission Control Protocol which are both set to SET, whereas all the others are set to NOT SET.
* **What is the sequence number of the TCP segment containing the HTTP POST command?**
* The sequence number of the TCP segment containing the HTTP POST command is 1. This is the first segment with the PUSH flag set to SET. This is the segment which contains POST in the data field.
* Related segment number is 194.