Lab Exercise 4: Exploring TCP

Exercise 1: Understanding TCP using Wireshark

Question 1: What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection? 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?

gaia.cs.umass.edu
IP address: `128.119.245.12`
port number : `80`

client computer
IP address: `192.168.1.102`
port number: `1161`

Question 2: What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

Sequence Number (raw): 232129013

Question3: 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) sent from the client to the web server (Do not consider the ACKs received from the server as part of these six segments)? 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 (see relevant parts of Section 3.5 or lecture slides) after the receipt of each ACK? Assume that the initial value of EstimatedRTT is equal to the measured RTT (SampleRTT) for the first segment, and then is computed using the EstimatedRTT equation for all subsequent segments. Set alpha to 0.125.

Using `EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT` to get EstimatedRTT

Sequence number	time sent	time received	RTT	EstimatedRTT
232129013	0.026477	0.053937	0.02746	0.02746
232129578	0.041737	0.077294	0.035557	0.028472125
232131038	0.054026	0.124085	0.070059	0.03367048438
232132498	0.054690	0.169118	0.114428	0.04376517383
232133958	0.077405	0.217299	0.139894	0.0557812771
232135418	0.078157	0.267802	0.189645	0.07254167996

Question 4. What is the length of each of the first six TCP segments? (same six segments as Q3)

First segment is `565`
Other : `1460`

Question 5. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

`5840` bytes, get answer from No2. [SYN, ACK] segment.

The lack of receiver buffer space does not throttle the sender. Even in the minimum buffer space condition, the receiver does not throttle the sender.

Question 6. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

Using Wireshark and input 'tcp.analysis.retransmission' in filter display, it doesn't show any capture packet in the list.

Or there are not same sequence number, thus no retransmitted segments in the trace file.

Question 7. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (recall the discussion about delayed acks from the lecture notes or Section 3.5 of the text).

`acknowledge data: 1460`

At No.60. It misses ACK=36509. No.60 's acknowledge number(raw) is `232166981` and No.50 is `232164061`, the two difference is exactly two ack data.

Question 8. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

the first tcp segement is No.4 and the last tcp segment is No.202

Total bytes = `232293103 - 232129013 = 16409` or we can use ACK `164091 - 1 = 164090`

Time = `5.455830 - 0.026477 = 5.42936`

`Throughtput = Total bytes / Time = 164090 / 5.42936 = 30220.87318 bytes/s`

Exercise 2: TCP Connection Management

Question 1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and server?

sequence number: `2818463618`

Question 2. What is the sequence number of the SYNACK segment sent by the server to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did the server determine that value?

sequence number sent by server: `1247095790`

Value of Ack field: `2818463619`

The client sequence number plus 1 to get this value.

Question 3 . What is the sequence number of the ACK segment sent by the client computer in response to the SYNACK? What is the value of the Acknowledgment field in this ACK segment? Does this segment contain any data?

sequence number: `2818463619`

ack: `1247095791`

No, because this is three way handshake to establish tcp connection, it doesn't contain any data.

Question 4 . Who has done the active close? client or the server? how you have determined this? What type of closure has been performed? 3 Segment (FIN/FINACK/ACK), 4 Segment (FIN/ACK/FIN/ACK) or Simultaneous close?

Client done the active close.

The Client send [FIN] to server.

Simultaneous close.