COMP3331 Computer Networks and Applications
Lab Exercise 04: Exploring TCP

HyoJoo Kwon
z5222646
W12A

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?

- IP address:128.119.245.12
- Port number: 80
- Client's IP address: 192.168.1.102 / TCP 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: 232129013

Question 3. 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.

EstimatedRTT = (1 - a) * (EstimatedRTT) + a * (SampleRTT)				
Sequence Number	Sent(sec)	ACK received (sec)	RTT (sec)	EstimatedRTT (sec)
232129013 (#4)	0.026477	0.053937 (#6)	0.02746	0.02746
232129578 (#5)	0.041737	0.077294 (#9)	0.035557	0.0285
232131038 (#7)	0.054026	0.124085 (#12)	0.070059	0.0337
232132498 (#8)	0.054690	0.169118 (#14)	0.11443	0.0438
232133958 (#10)	0.077405	0.217299 (#15)	0.13989	0.0558
232135418 (#11)	0.078157	0.267802 (#16)	0.18964	0.0725

Question 4. What is the length of each of the first six TCP segments?

- seg1: 565 bytes
- seg2: 1460 bytes
- seg3: 1460 bytes
- seg4: 1460 bytes
- seg5: 1460 bytes
- seg6: 1460 bytes

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?

- Minimum available buffer space: 5840 bytes.
  No, it 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?

- There are no retransmitted segments. We can know this by comparing the sequence numbers. If there is a retransmitted segment, the sequence number will be less than the previous segment sequence number.

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).

- It typically acks 1460 bytes of data.
  There are cases where the receiver acks every other segment. This is happens when more than one ack occurs right after.

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

Total data transmitted
= (ack sequence number of the last segment) - (sequence number of the first segment)
= 232293103 - 232129012
= 164091 bytes
Transmission time
= 5.455830(seg #202) - 0.026377(seg #4) = 5.42492 seconds

Throughput
= total data transmitted / transmission time
= 164091 bytes / 5.2494 seconds
= 30223bps

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: 1247095790
- ACK field: 2818463619
- Seq = previous ACK field
- Ack = previous seq + 1.

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?

- Seq: 2818463619
- Ack: 1247095791

No this segment does not 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 have done the active close. Client, who has the ip 10.9.16.201 sent the FIN segment first. It is performing simultaneous close, since it is sending FIN without receiving FIN (crossing each other).

Question 5 . How many data bytes have been transferred from the client to the server and from the server to the client during the whole duration of the connection? What relationship does this have with the Initial Sequence Number and the final ACK received from the other side?

- Client -> Server: 2818463653 - 2818463618 - 2 = 33
- Server -> Client: 1247095832 - 1247095790 - 2 = 40
- Final ACK - Initial seq - 2 (-2 is for SYN and FIN which does not contain any data)