COMP3331

Lab 4

Dean So (z5204873)

Exercise 1: Understanding TCP using Wireshark

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 is 128.119.245.12

Destination Port number is 80

Source IP Address is 192.168.1.102 and port number 1161

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.*

Seq number with POST is 232129013

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.* ***Note:*** *Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph>Round Trip Time Graph . However, do not use this graph to answer the above question.*

Estimated RTT = (1-a)*EstimatedRTT + a*SampleRTT

Segment Number	Seq Number	Sent Time (s)	ACK Recv Time (s)	RTT (ms)	Estimated RTT (ms)

1	232129013	0.026477	0.053937	0.02746	0.02746
2	232129578	0.041737	0.077294	0.035557	0.0285
3	232131038	0.054026	0.127085	0.070059	0.0337
4	232132498	0.054690	0.169118	0.11443	0.0438
5	232133958	0.077405	0.217288	0.13989	0.0558
6	232135418	0.078157	0.267802	0.18964	0.0725

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

Segment Number	Size (bytes)
1	565
2	1460
3	1460
4	1460
5	1460
6	1460

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?*

The minimum buffer is 5480 bytes which can reach a maximum of 62780 bytes. The lack of receiver buffer space does not throttle the sender.

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

No retransmission occurred. I checked the sequence numbers of each of the TCP segments and the sequence numbers always increase.

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).*

The receiver typically acknowledges 1460 bytes of data. In the case below

```
14 0.169118    128.119.245.12    192.168.1.102    TCP    60 80 → 1161 [ACK] Seq=883061786 Ack=232133958 Win=14600 Len=0
15 0.217299    128.119.245.12    192.168.1.102    TCP    60 80 → 1161 [ACK] Seq=883061786 Ack=232135418 Win=17520 Len=0
16 0.267802    128.119.245.12    192.168.1.102    TCP    60 80 → 1161 [ACK] Seq=883061786 Ack=232136878 Win=20440 Len=0
17 0.304807    128.119.245.12    192.168.1.102    TCP    60 80 → 1161 [ACK] Seq=883061786 Ack=232138025 Win=23360 Len=0
```

The receiver begins ACKing every other received segment and starts doing it in groups.

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

Total data = seq no. of last – seq no. of 1st

= 883061786 – 232129013 = 650932773

Total time = time of last – time of 1st

= 5.455830 (seg #202) – 0.026477 (seg #4) = 5.42494

Throughput = 650932773/5.42494 = 119988934.993

Exercise 2: TCP Connection Management

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 281846318

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 of SYNACK is 1247095790 ACK number is +1 of Q1, 281846319

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, ACK contains 0 bytes of data.

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?*

Both parties have done the active close as it is simultaneous closure.

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?*

Data sent = final ACK - ISN

Client to server data = 1247095831-1247095790 = 41

Server to Client data = 2818463653-2818463618-2 = 33