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?

Solution 1 :

As stated that in the 4th segment of the trace being sent from the host in MIT to gaia.cs.umass.edu. So, destination is gaia.cs.umass.edu and host is MIT. So,

The IP address as observed from the Wireshark output is 128.119.245.12.

The TCP segments are sent and received on port number 80.

The IP address of the source is 192.168.1.102 and port number is 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 Ethereal window, looking for a segment with a "POST" within its DATA field.

Solution 2 :

Sequence number = 232293013

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.

Solution 3 :

EstimatedRTT = (1 – alpha) • EstimatedRTT + alpha• SampleRTT

#1 = (1 - 0.125) x 0.02746 + 0.125 x 0.02746 = 0.02746

#2 = (1 - 0.125) x 0.02746 + 0.125 x 0.035557 = 0.02847212 =~ 0.02847

#3 = (1 - 0.125) x 0.02847 + 0.125 x 0.070059 = 0.03366862 =~ 0.03367

#4 = (1 - 0.125) x 0.03367 + 0.125 x 0.114428 = 0.0436475 =~ 0.04376

#5 = (1 - 0.125) x 0.04376 + 0.125 x 0.139894 = 0.05577675 =~ 0.05578

#6 = (1 - 0.125) x 0.05578 + 0.125 x 0.189645 = 0.07251312 =~ 0.07251

No.	Sequence Number	Time(sent)	Time(ACK)	Difference	EstimatedRTT
1	232293013	0.026477	0.053937	0.02746	0.02746
2	232129578	0.041737	0.077294	0.035557	0.02847
3	232131038	0.054026	0.124085	0.070059	0.03367
4	232132498	0.054690	0.169118	0.114428	0.04376
5	232133958	0.077405	0.217299	0.139894	0.05578
6	232135418	0.078157	0.267802	0.189645	0.07251

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

Solution 4 :

The lengths of the segments are as follows:

Length of first segment = 565

Length of second segment = 1460

Length of third segment = 1460

Length of fourth segment = 1460

Length of fifth segment = 1460

Length of sixth segment = 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?

Solution 5 :

The minimum amount of buffer space advertised at gaia.cs.umass.edu for the entire trace is 5840 bytes and no it doesn't 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?

Solution 6 :

There is no retransmitted segments in the trace file . This can be checked by looking at all the sequence numbers of the provided file and if there was one retransmitted segment then segment number would have been less than the previous one which is not the case.

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.

Solution 7 :

The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs. By inspecting the amount of acknowledged data by each ACK, there are cases where the receiver is ACKing every other segment. For example, segment of No. 80 acknowledged data with 2920 bytes = 1460*2 bytes.

	Seq's (end)	**Data Acknowledged**
ACK 1	0	565
ACK 2	578	1460
ACK 3	038	1460
ACK 4	498	1460
ACK 5	958	1460
ACK 6	418	1460
ACK 7	878	1460
ACK 8	025	1460
ACK 9	485	1460
ACK 10	945	1460
ACK 11	405	1460
ACK 12	865	1460

And so on….

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

Solution 8 :

Throughput = total data transmitted/transmission time

= (232293103 - 232129012) / (5.455 - 0.026)

= 30247.2 bits per second

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?

Solution 1 :

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?

Solution 2 :

Sequence number : 2818463619

Acknowledgement value : 1247095790

The value is extracted from the last Frame number + 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?

Solution 3 :

Acknowledgment value : 1247095791

Sequence number : 2818463619

No, the 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?

Solution 4 :

Client has done the active close with the FIN which has been initiated by the client and the closure has been performed by 3 Segment (FIN/FINACK/ ACK) with frames 304, 305 and 306 respectively.

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?

Solution 5 :

The relationship they share is that the number of bytes transferred between client to server is the difference between sequence number and the acknowledgement number.

Number of bytes transferred(client to server) = 2818463652 - 2818463619
= 33

Number of bytes transferred(server to client) = 2818463652 -

=