Assignment-7 Networking Problem Set II

Full Credit: 20 pts | Due: Sunday 5/15

Q1. Please answer the following questions on TCP in a detailed narrative

1) What do TCP and UDP stand for? What are commonalities and differences between TCP and UDP?

[References: Book 4 Sections 1.12, 17.1, and videos: "UDP and TCP: Comparison of Transport Protocols" [11m] https://www.youtube.com/watch?v=Vdc8TCESIg8 "TCP vs UDP Compari-son|Cisco CCNA 200-301" [7m] https://www.youtube.com/watch?v=cA9ZJdqzOoU]

TCP & UDP is Transport layer. User Datagram Protocol - small packet size. UDP header is 8 bytes and TCP is 20 bytes, connect less. If it lost packet during transportation it does not care and does not care about order of packet in receiver end and does not care about congestion. So it does not reliable.

Transmission Control Protocol based on 3 way handshake (establish connection). So sender send request to establish connection and if it is fine with receiver it send back OK respond and sender acknowledge connection. Now when connection is establish we can have delivery acknowledgement. So when data sent from sender to receiver now receiver sent back ack with #, that is tcp has those #. Another feature it has retransmission so if packet get lost and after curtain period of time aka timeout sender did not receive ack it resent the same packet. It will assemble in order on receiver end. Congestion control delay transmission when network is busy, but it also downside because data does not sent immediately. With all those ack it take longer time to load video so it where udp is shine, no need all those ack and if you packets are lost it is no problem.

So when creating application for sending text messages we need to use tcp because every character will be delivered unlike with udp can be lost few character and can be out of order words assemble. So in 99% you want that all data can be deliver to you.

2) In TCP, how does the connection between a client and a server is established via the 3-way handshake? How does the connection is torn down (closed)?
[References: Book 4 Section 17.3 and video: "TCP connection walkthrough | Networking tutorial (13 of 13)" [10m], https://www.youtube.com/watch?v=F27PLin3TV0]
Transmission Control Protocol based on 3 way handshake (establish connection). So sender send request to establish connection and if it is fine with receiver it send back OK respond and sender acknowledge connection. Now when connection is establish we can have delivery acknowledgement. So when data sent from sender to receiver now receiver sent back ack with #, that is tcp has those #. After data was sent server sent flag FIN to indicate close connection and client ack that and also sent FIN flag to server and server ack this and connection is closed.

3) How does TCP identify an application? What is a port number? What is a TCP socket?
Analogy post is data packet and mailbox is port. Where smart idea to assign every port in server number. And each this number deal with different protocols, e.g. when browser request html from server it goes to port: 80 which deal with html, when sent email SMTP it is port: 25 and dealing with files FTP it is port: 21. Because it is standard all computes know who port who. So when we make http request it adds destination port: 80 to tcp header. It send ip: 80 (ip + destination port #). Server look at destination port # and server understand that is web request and then server is respond. IP indicate which computer and port indicate which application. There are about 65k port #, only 1023 are important, other randomly generated to identify your local port when server sent respond back to your.

client socket is ip and randomly generated port number on local computer. Server socket is ip and standard port # which depends on type of requested application. Together they create socket pair.

[References: Book 4 Section 1.12 and videos: "Port Numbers Explained | Cisco CCNA 200-301" [6m] https://www.youtube.com/watch?v=RDotMcs0Erg "TCP and UDP: Sockets" [4m] https://www.youtube.com/watch?v=QLvDf3o7BpE]

4) What is a TCP SYN flood attack? [Extra point: How to prevent / mitigate this attack?]

This is attack target to take down a server based on 3 hand shake connection, where hacker changes ip and port # and sent to server syn flag and server respond with ack but it does not it is fake ip & port. Then hacker sent many syn requests from fake ips: ports and it drain server's memory because those connections not closed one because client does not send back ack to server.

[References: Book 4 Section 17.3, and video "SYN Flood Attack Explained" [7m] https://www.youtube.com/watch?v=tClcCMrXzek]

Q2. Internet Checksum

References: Book-4 Section 7.4, video "Error Detection and Correction 1: Internet Checksum" [9m], https://www.youtube.com/watch?v=EmUuFRMJbss

1) What is Internet checksum? How to calculate Internet checksum on the sender side? How to use it on the receiver side to detect errors?

It is error detection. Name speak for itself it check the sum, so sender create message and it is going calculate checksum and it will attach this checksum with message. On sender side checksum is created and on

receiver is validated. After validation receiver finds out there is no errors, then packet is accepted, othewise data is rejected.
On sender side break data into k amount of block with n amount of bits, then sum k blocks (binary sum), then add carry to the sum (move it all the way to right and sum), then do checksum (1's compliment - flip bits), then this checksum is added to the message.
Receiver collects all k blocks and checksum and sum it and if result is 1's it is accept it, otherwise rejected it.

2) Consider the following four-bit numbers, with decimal values in parentheses:

1000 (8) 1011 (11) 1101 (13) 1110 (14)

Find their Internet checksum, i.e., the ones-complement sum via three 4-bit ones-complement additions. To get started, note that the (exact) sum of 1000 and 1011 is 1|0011, and adding the carry bit to the low-order 4 bits gives a ones-complement sum of the first pair of 0100.
0100
1101
10001
0010
1110
10000
0001
1110 - 1's compliment = checksum

3) Consider the following 16-bit numbers in hexadecimal, with decimal values in parentheses:

4500 (17664) b861 (47201) c0a8 (49320) 8180 (33152)
4500 = 0100 0101 0000 0000 and then sum them up like above and do 1's compliment then convert them to hex $C074_{16}$

Find their Internet checksum, i.e., the ones-complement sum via three 16-bit ones-complement additions.

Q3. Cyclic Redundancy Check

References: Book-4 Section 7.4.1, video "Error Detection and Correction 2: Cyclic Redundancy Check" [12m], https://www.youtube.com/watch?v=6gbkoFciryA

1) What is CRC code? How to calculate the CRC code on the sender side? How to use it on the receiver side to detect errors?

Cyclic Redundancy Check is one of error detection technic.
On sender end: find length of divisor L, then append L-1 (0)bits to original message, perform binary division operation, then remainder of division is CRC, then xor operation and result add to original message.
On receiver side: it received message then it does same way as receiver it divide by divisor and if result will be all 0 then no errors were detected.

2) Suppose a message is 110010101. Calculate the CRC-3 checksum using the generator polynomial x^3 + 1, that is, find the 3-bit remainder using divisor 1001.

Binary form: 110010101 divided by 1001

x**8+x**7+x**4+x**2+1 message is 110010101

x**3+1 divisor = 1001 (1.x^3 + 0.x^2 + 0.x + 1)

append 3 zeros to the message to add it at the end because divisor is of n digits we have to take add n-1 0's to the message

Binary form (added zeros): 110010101000 divided by 1001

1001) 1 1 1 0 0 0 1 1 0 0 0 (1 1 1 1 1 1 0 0

1 0 0 1

1110

1 0 0 1

1110

1 0 0 1

1111

1 0 0 1

1101

1 0 0 1

1000

1 0 0 1

0010

0100

100 - remainder or crc code which be appended to original message

Data transmitted: 110010101100

3) Suppose a message is a two-letter string “Hi”. Represent it with ASCII hex value then to binary format, then calculate the CRC-5 checksum using generator polynomial x^5 + x^2 + 1, that is, find the 5-bit remainder using divisor 100101.

Hex value is 4869 to binary is 0100 1000 0110 1001

Because of diviser adding 5 0s to message:

0100 1000 0110 1001 00000 : 100101=010000100011111

Remainer 00011. Append remainder to original message:

0100 1000 0110 1001 00011 : 100101= 00000 remainder no error

Q4. TCP connection establishment, data transfer, and connection close

References: Book-4 Section 17.3.

Suppose A and B create a TCP connection with ISN_A=20,000 and ISN_B=5,000. [ISN is Initial Sequence Number]. A sends three 1000-byte packets (Data1, Data2 and Data3 below), and B ACKs each. Then B sends a 1000-byte packet DataB to A and terminates the connection with a FIN. In the table below, fill in the SEQ and ACK fields for each packet shown.

A sends	B sends
SYN, ISN_A=20,000	
	SYN, ISN_B=5,000, ACK=_____
ACK, SEQ=_____, ACK=_____	
Data1, SEQ=_____, ACK=_____	
	ACK, SEQ=_____, ACK=_____
Data2, SEQ=_____, ACK=_____	
	ACK, SEQ=_____, ACK=_____
Data3, SEQ=_____, ACK=_____	
	ACK, SEQ=_____, ACK=_____
	DataB, SEQ=_____, ACK=_____
ACK, SEQ=_____, ACK=_____	
	FIN, SEQ=_____, ACK=_____

b 20001

A ack, seq = 20001, ack = 5001

Data 1 , seq = 20001, ack = 5001 — s 5001, a=21001;

Data 2, s=21001, ack = 5002 — s = 5002, a=22001;

Data 3, s=22001, ack = 5002 — s = 5003, a=23001;

Ack ,s = 23001, a=6003 — fin s = 6003;a=23002

Q5. TCP segment transfers

Host A and B are communicating over a TCP connection, and Host B has already received from A all bytes up through byte 126. Suppose Host A then sends two segments to Host B back-to-back. The first and second segments contain 80 and 40 bytes of data, respectively. In the first segment, the sequence number is 127, the source port number is 302, and the destination port number is 80. Host B sends an acknowledgment whenever it receives a segment from Host A.

1) In the second segment sent from Host A to B, what are the sequence number, source port number, and destination port number?

SEQUENCE NUMBER = FIRST SEGMENT OF SEQUENCE NUMBER+ DESTINATION PORT NUMBER

=127+80

=207

So, SEQUENCE NUMBER=207

SOURCE PORT NUMBER = 302

DESTINATION PORT NUMBER= 80

2) If the first segment arrives before the second segment, in the acknowledgment of the first arriving segment, what is the acknowledgment number, the source port number, and the destination port number?

Acknowledgement number= 207

Source port number = 80

Destination port number= 302

3) If the second segment arrives before the first segment, in the acknowledgment of the first arriving segment, what is the acknowledgment number?

If the second segment arrives before the first segment, in the acknowledgement of the first arriving segment, the acknowledgement number will be 127

Hence, Acknowledgement number=127

Submission Instructions: Place all your answers into a pdf file, name it as LastFirstInitial_a7.pdf, and then upload it through your blackboard account by the due day.