FORMAT-1

Semester: 5th.
Programme: B. Tech
Branch/Specialization: CSE,IT,CSCE,CSSE

AUTUMN END SEMESTER EXAMINATION-2023

5th Semester, B. Tech (Programme)

SUBJECT COMPUTER NETWORKS

CODE IT 3009

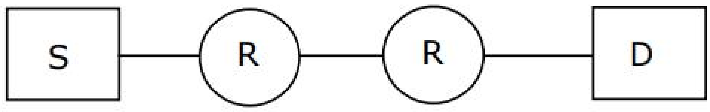
(For 2021Admitted Batches)

Time: 3 Hours **Full Marks: 50**

Answer any SIX questions.
Question paper consists of four SECTIONS i.e. A, B, C and D.
Section A is compulsory.
Attempt minimum one question each from Sections B, C, D.
The figures in the margin indicate full marks.
Candidates are required to give their answers in their own words as far as practicable and all parts of a question should be answered at one place only.

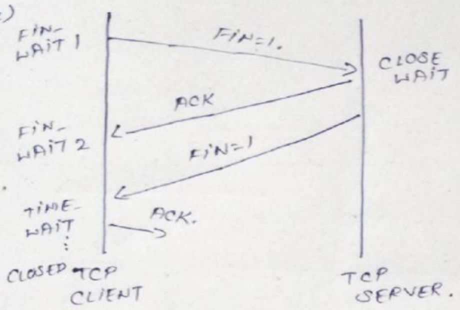
1.		Answer the following questions.	[1×10]
	(a)	Suppose you wanted to do a transaction from a remote client to a server as fast as possible. Would you use UDP or TCP? Why? Ans: If the primary concern is speed and minimizing latency, UDP (User Datagram Protocol) would be the preferred choice over TCP (Transmission Control Protocol) for a transaction from a remote client to a server. Reduced Overhead: UDP has minimal overhead compared to TCP. No Handshaking: TCP requires a connection establishment process (the three-way handshake) before data transfer begins, which adds to the initial latency. UDP doesn't have this overhead, allowing for immediate data transmission. Suitability for Real-Time Applications: UDP is often favored in scenarios where real-time data transmission is crucial, such as video streaming, online gaming, or VoIP (Voice over Internet Protocol).	
	(b)	Assume a sender sends 6 packets: packets 0, 1, 2, 3, 4, and 5. The sender receives an ACK with ackNo = 3. What is the interpretation if the system is using GBN or SR? Ans: In the context of networking protocols like Go-Back-N (GBN) or Selective Repeat (SR), the ACK number received by the sender indicates the acknowledgment of the next expected packet by the receiver. Go-Back-N (GBN): In GBN, the receiver acknowledges correctly received packets cumulatively, meaning it acknowledges the highest in-order packet it has received. If the sender receives an ACK with ackNo = 3, it implies that all packets up to packet number 2 have been received successfully and acknowledged. Packets 0, 1, and 2 are acknowledged successfully, and the sender can now send packets starting from 3.	

		Selective Repeat (SR): Unlike GBN, SR allows the receiver to acknowledge individual packets rather than just the highest in-order packet. An ACK with ackNo = 3 means the receiver has received and correctly acknowledged packet number 3. However, this acknowledgment doesn’t necessarily mean that the earlier packets (0, 1, and 2) have been received or acknowledged by the receiver.	
	(c)	Consider four components that constitute delay for a packet network: queueing delay, processing delay, propagation delay, and transmission delay. Describe circumstances where the processing delay for one packet type varies significantly from the mean processing delay of a packet. Ans: There are several scenarios in networking or computing where the processing delay for one packet type can significantly vary from the mean processing delay of other packets. Here are a few examples: Packet Size Differences: If packets of different sizes are being processed, the processing delay can vary. Priority or QoS (Quality of Service): Some packets might be marked with higher priority or QoS requirements. Packet Content or Type: Certain packet types might require more complex processing due to their content or the protocol they belong to. Congestion or Network Conditions: During periods of congestion or network instability, certain packets might face delays due to retransmissions, packet drops, or queuing in network devices. Packet Error or Corruption: Packets that are corrupted or contain errors might incur additional processing time due to error detection, retransmission requests, or other error handling mechanisms.	
	(d)	In the transfer of file between PC and server, if the transmission rates along the path is 15Mbps, 50Mbps, and 16Mbps. Calculate the traffic of the network. Ans: The traffic of the network is typically constrained by the slowest link in the path. Here, the transmission rates are 15Mbps, 50Mbps, and 16Mbps. The slowest rate is 15Mbps, so this will be the maximum rate at which the file can be transferred. Thus, the traffic of the network is constrained to 15Mbps.	
	(e)	Discuss the impact of a stable end-to-end latency by explaining the difference between flow control and congestion control. Ans: Flow Control: It is a technique used to prevent the sender from overwhelming the receiver. It ensures that the sender does not send more data than the receiver can process. Congestion Control: It is used to prevent too much data from being injected into the network. This is necessary because too much data can lead to network congestion, leading to packet loss and increased	

		latency. Stable end-to-end latency is important for efficient network performance. With effective flow and congestion control, the network can avoid situations where buffer overflow or data packet loss occur, thus maintaining a stable latency.	
	(f)	Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during transmission from S to D.  Ans: Network Layer Visits: Each time a packet reaches a new router or the destination, it interacts with the network layer. For a packet going from S to D via two routers, there will be 1 (source) + 2 (routers) + 1 (destination) = 4 visits to the network layer. Data Link Layer Visits: Each hop (from source to router, router to router, and router to destination) involves the data link layer. So, there will be 1 (S to R1) + 1 (R1 to R2) + 1 (R2 to D) = 3 visits to the data link layer. Therefore, each packet will visit the network layer 4 times and the data link layer 3 times during its transmission from S to D.	
	(g)	Identify the correct sequence (sequence are- HTTP GET request, DNS query, TCP SYN) in which the following packets are transmitted on the network by a host when a browser requests a web page from a remote server, assuming that the host has just been restarted.	
	(h)	Consider a TCP client and a TCP server running on two different machines. After completing data transfer, the TCP client calls close to terminate the connection and a FIN segment is sent to the TCP server. Server-side TCP responds by sending an ACK which is received by the client-side TCP. As per the TCP connections state diagram (RFC 793), in which state does the client-side TCP connection wait for the FIN from the server-side TCP?	
	(i)	Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header and a 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0. The fragmentation offset value stored in the third fragment is ________.	
	(j)	What are the disadvantages of Stop and wait protocol. Ans: (Q 1. g, h, I, j)	

(g) DNS QUERY → TCP SYN → HTTP GET.
(CORRECT SEQUENCE)

(h)



FIN-WAIT-2 STATE.

(i) PACKET LENGTH = 4500 BYTES.
MTU = 600 BYTES.
MTU PAYLOAD = 600 - 20 = 580 BYTES.
IT SHOULD BE ANY MULTIPLE OF 8, IF NOT FIND JUST A NEAREST SMALLER NO. i.e 576
FRAGMENT SIZE = 576 BYTES.

I OFFSET = 0
II OFFSET = $\frac{0+576}{8} = 72$
III OFFSET = $\frac{0+576+576}{8} = \boxed{144}$

(j). 1. RECIEVER IS WAITING FOR DATA FOR A LONG TIME.
2. ITS MEANT FOR ONLY NON-NOISY CHANNEL BUT IN REALITY, NON-NOISY CHANNEL DON'T ~~OCCUR~~. EXISTS.
3. INEFFICIENT FOR LONG DISTANCE COMMUNICATION.
4. INCREASES LATENCY

SECTION-B (Learning levels 1,2, and 3)

2.	(a)	What is the formula to calculate the number of redundancy bits required to correct a bit error in a given number of data bits? Explain an error correction technique on the following data: Data send 1001101 and data received 1000101. Ans:	[4]

Data : 1001101

Number of data bits = 7
minimum no of redundancy bits (r)
$2^r \geq m + r + 1$

So minimum of r bits should be 4
as $2^4 \geq 7 + 4 + 1$ (formula)
$16 \geq 12$

We know the redundancy bits are placed at the powers of 2
no of bits in code word $= r + m = 7 + 4 = 11$

So,

R_1	R_2	D_1	R_3	D_2	D_3	D_4	R_4	D_5	D_6	D_7
R_1	R_2	1	R_3	0	0	1	R_4	1	0	1
1	2	3	4	5	6	7	8	9	10	11
0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011

Now calculate the value of redundant bit by taking parity from the array values

R_1 =
no of ones = 4
so parity = 0 $\qquad R1 = 0$

R_2: ~~no of~~ no of ones = 3
so parity = 1 $\qquad R2 = 1$

R3: no of ones = 1
so parity = 1 $\qquad R3 = 1$

R4: no of ones = 2 $\qquad R4 = 0$
so parity = 0

code word : 01110010101 ~ data sent

After receiving the data was changed to 1000101

So, code word that was received was ~~0110~~
01110000101
corrupted bit

So when the redundancy bit will checked for:

R1 0111 0000 101 parity = 1

R2 0111 0000 101 parity = 1

R3 0111 0000 101 parity = 1

R4 0111 0000 101 parity = 0

Since the parity for all was not 0 error was detected

and the error was at 111 = 7th bit
So it was corrected by reversing the bit

(b) In a Stop-and-Wait system, the bandwidth of the line is 1 Mbps, and 1 bit takes 20 milliseconds to make a round trip. What is the bandwidth-delay product? If the system data packets are 1,000 bits in length, [4]

(1) What is the utilization percentage of the link?
(2) What is the utilization percentage of the link in (1) if we have a protocol that can send up to 15 packets before stopping and worrying about the acknowledgments?

Ans:

The bandwidth-delay product (BDP) is a measure of the amount of data that can be in transit in the network at any point in time. It is calculated by multiplying the bandwidth of the line by the round-trip time (RTT). The formula is:

BDP=Bandwidth×Round-Trip Time (RTT)

Given that the bandwidth is 1 Mbps and the round-trip time is 20 milliseconds:

BDP=1 Mbps×(20 milliseconds×2)=40 kilobits

Now, lets move on to the utilization percentage.

(1) Utilization Percentage with Stop-and-Wait:

The utilization (U) can be calculated using the formula:

U = (BDP/Packet Size)

Given that the packet size is 1,000 bits, plug in the values:

U = 1000 bits / 40 Kilobits = 0.04

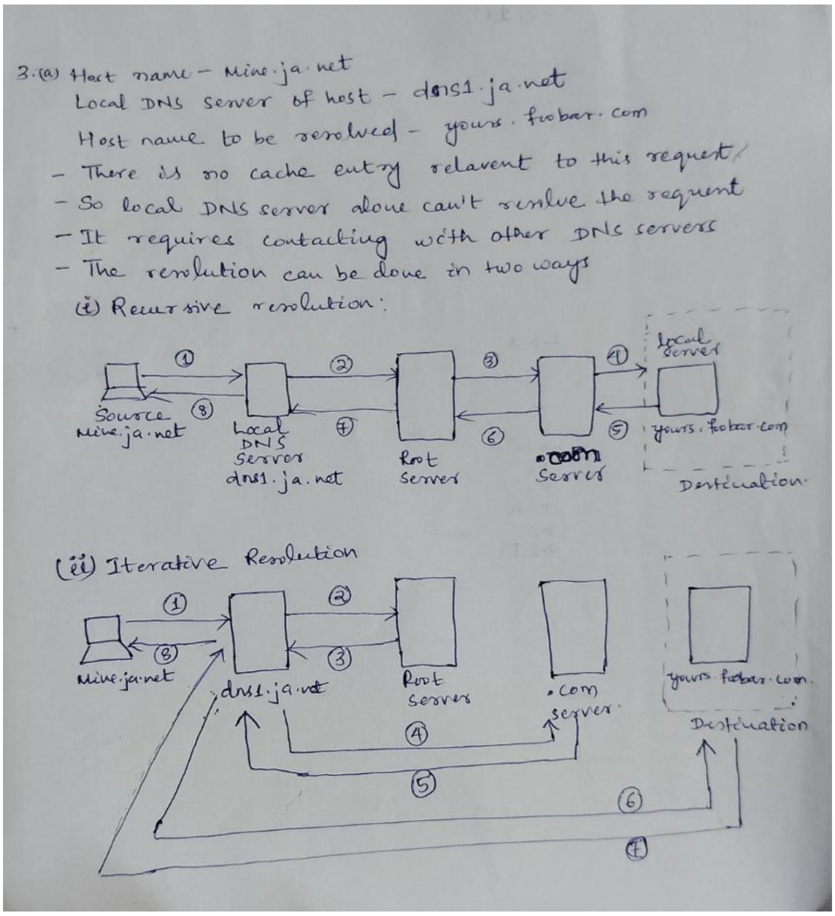
This is the utilization per packet. To get the percentage, multiply by 100

U% = 0.04×100=4%

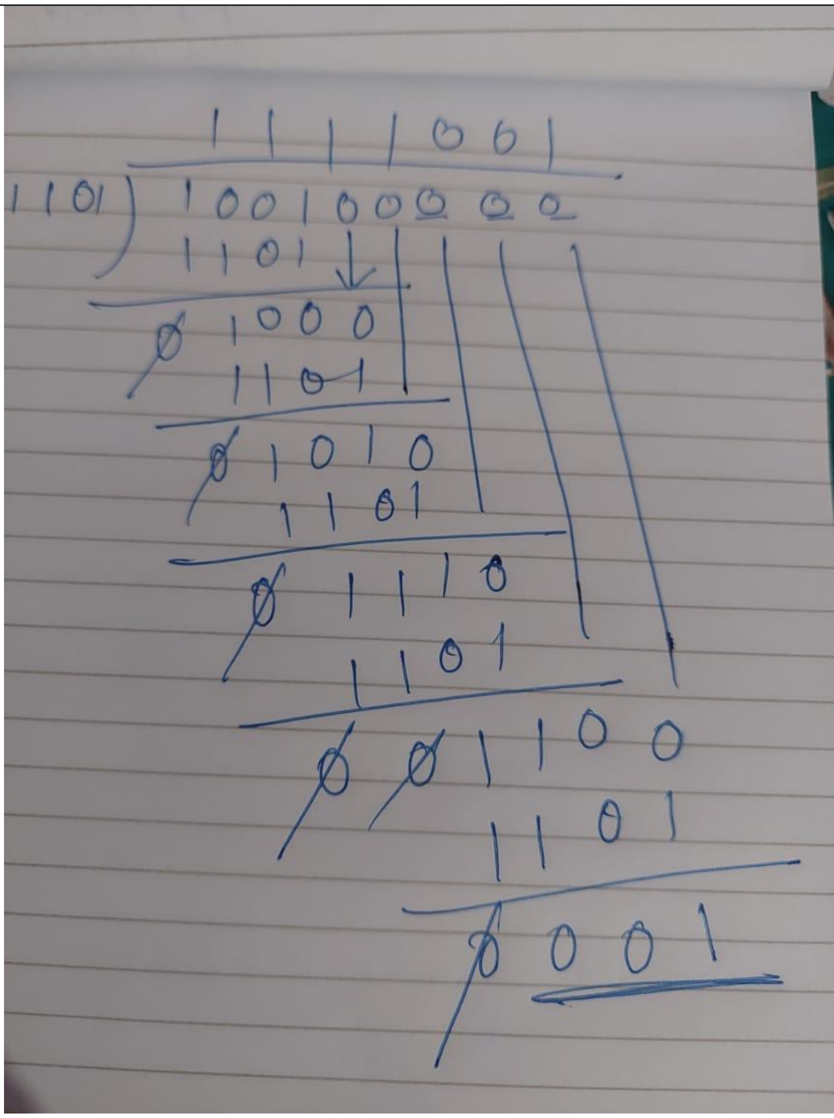
So, the utilization percentage of the link with the Stop-and-Wait protocol is 4%

(2) Utilization Percentage with a Protocol Allowing 15 Packets:

		If the protocol can send up to 15 packets before worrying about acknowledgments, it means that there can be up to 15 packets in transit simultaneously. The new utilization (U') is given by: U =(BDP/Number of Packets in Transit×Packet Size) Given that the number of packets in transit is 15 and the packet size is still 1,000 bits 1,000 bits, plug in the values: U′=40 kilobits / 15×1,000 bits U'=40 kilobits/15×1,000 bits U′=(40/15)×0.04 U' = 0.1067 So, the utilization percentage of the link with the protocol allowing 15 packets is 10.67%.	
3.	(a)	Consider the host mine.ja.net, with a local DNS server dns1.ja.net. (i) Host mine.ja.net asks server dns1.ja.net to resolve the hostname yours.foobar.com. Assume there are no cached entries relevant to this request. Write down the steps taken to resolve yours.foobar.com and respond to mine.ja.net. Ans:	[4]



	(b)	What is the CRC obtained by dividing Data word 100100 by the generator polynomial x3 +x2+ 1? Ans:	[4]



CRC 0001.

Deriving the CRC with correct answer - 4 marks. Partial answer or derivation with incorrect answer - 2 marks.

SECTION-C (Learning Levels 3 and 4)

4. (a) Here are four options for improving web page performance. [4]

Option 1: HTTP Caching with a Forward Proxy

Option 2: CDN using DNS

Option 3: CDN using anycast

Option 4: CDN based on rewriting HTML URLs

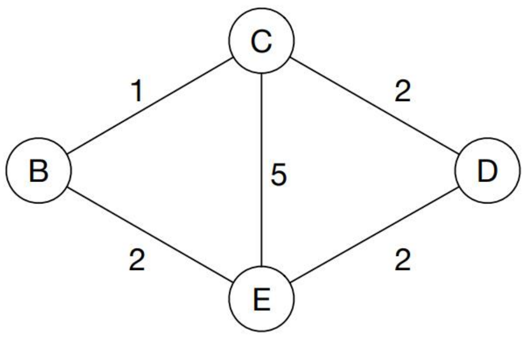
You have been asked to help reduce the costs for networking at KIIT University.

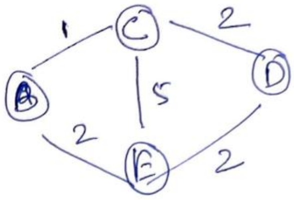
The delivery of online courses has become a tremendous success – but this has led to a significant increase in network costs for the University.

You must select one of the options above to minimize server load. Compare the operation of each option and justify a selection that provides the finest granularity of control over load to the content servers and a selection that will serve each customer from the closest CDN server.

Ans: "... network costs for the University. You must select one of the options above to minimize server load...."

		Option 2: CDN using DNS: Explanation ------ 2 marks "... Compare the operation of each option and justify a selection that provides the finest granularity of control over load…" -------- Explanation and comparison (2 marks)	
	(b)	Consider different activities related to email. m1: Send an email from a mail client to a mail server m2: Download an email from the mailbox server to a mail client m3: Checking email in a web browser Explain the application-level protocol used in each activity. Ans: Each of the mentioned activities related to email involves specific application-level protocols that facilitate communication between different components. Here's an explanation of the application-level protocols associated with each activity: Sending an Email (m1: Send an email from a mail client to a mail server): Application-Level Protocol: SMTP (Simple Mail Transfer Protocol) Explanation: SMTP is the standard protocol used for sending emails. When a user sends an email from a mail client (like Outlook or Thunderbird) to a mail server, the client establishes a connection to the server using SMTP. The client then sends the email, including sender and recipient information, subject, and message content, to the mail server using SMTP commands. Downloading an Email (m2: Download an email from the mailbox server to a mail client): Application-Level Protocol: POP3 (Post Office Protocol version 3) or IMAP (Internet Message Access Protocol) Explanation: To download emails from a mailbox server to a mail client, two commonly used protocols are POP3 and IMAP. POP3 is a simple protocol that downloads emails to the client's device, removing them from the server. IMAP, on the other hand, allows the client to access emails directly on the server without downloading them. IMAP is more suitable for users who want to access their emails from multiple devices and keep them synchronized. Checking Email in a Web Browser (m3: Checking email in a web browser): Application-Level Protocol: HTTP/HTTPS (Hypertext Transfer Protocol/Secure) Explanation: When a user checks their email through a web browser, the interaction typically involves HTTP or its secure variant, HTTPS. The email service provider's web application uses HTTP(S) to communicate between the user's browser and the server. User actions, such as logging in, viewing emails, and composing messages, trigger corresponding HTTP requests and responses. In modern email services, HTTPS is increasingly preferred over HTTP for secure communication, especially when handling sensitive information such as login credentials and email content. This ensures that the data transmitted between the user's browser and the email server is encrypted for privacy and security.	[4]

5.	(a)	ARP provides a service to the network layer, so it is part of the data link layer. Whether he is correct or not explain. Ans: Data link layer does not understand the concept of IP address so it cannot provide such service to the Network layer. ARP is part of the network layer: Given an IP address, a host will reply (in an IP packet) with MAC address if the requested IP address matches its IP, that way the requesting host will learn which MAC address (host) has an specific IP address. ARP uses IP address of network layer to find the MAC address. This ARP is being encapsulated in frame so the source MAC and destination MAC address will be there in outer header of frame. However inner ARP data like source IP and destination IP will be encapsulated in frame. ARP request will be broadcast at the data link layer level source MAC and destination MAC (all 1's) and inner ARP data will be source IP and destination IP and source MAC and destination Mac (all 0's).	[4]
	(b)	An Internet Service Provider (ISP) has the following chunk of CIDR-based IP addresses available with it: 245.248.128.0/20. The ISP wants to give half of this chunk of addresses to Organization A and a quarter to Organization B while retaining the remaining with itself. Explain the process to find out a valid allocation of address to A and B. Ans:Correct IP address assignment to organization A, B [4]	[4]
6.	(a)	Consider the network shown in the figure below with four nodes. Cost links are shown in the diagram. Give the distance-vector routing tables for node C in the following two consecutive steps.  Step 0: C knows the distances to its immediate neighbours and Step 1: information from step 0 is exchanged as per the distance-vector algorithm. ANS:	[4]



STEP 0:
Distance Vector tables for C

B	1
C	0
D	2
E	5

STEP 1: On receiving Distance vector from node B

D.V for B

B	0
C	1
D	∞
E	2

updated C

B	1
C	0
D	2
E	3

STEP 2: On receiving Distance vector from node D

D.V for D

B	∞
C	2
D	0
E	2

update C

B	1
C	0
D	2
E	3

STEP 3: On receiving Distance vector from node E

DV for E

B	2
C	5
D	2
E	0

updated C

B	1
C	0
D	2
E	3

	(b)	An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks. Ans:	[4]

1st subblock with 120 addresses.

out of 8 host bits available in the original granted block address, for the 1st block only 7 host bits are required.

14.24.74.$\underset{\text{subnet bit}}{0}\underbrace{0000000}_{\text{host bits}}$

Subnet address – 14.24.74.0
broadcast address – 14.24.74.127
Subnet mask – 255.255.255.128

2nd subblock with 60 addresses

The remaining available block for use is

14.24.74.10000000

out of 7 host bits available here, for the 2nd block only 6 host bits are required.

14.24.74.1$\underset{\text{subnet bit}}{0}\underbrace{000000}_{\text{host bits}}$

Subnet address – 14.24.74.128
broadcast address – 14.24.74.191
Subnet mask – 255.255.255.192

3rd Subblock with 10 address

The remaining available block for use is, 14.24.74.11000000
one may use this block for the 3rd subblock or may prepare subnets out of it as no. of available host bits are 6, where as required no. of host bits for this block is 4 ~~bits~~.

without any further subblock	with further subblocks
Subnet address – 14.24.74.192	Subnet address – 14.24.74.192
broadcast address – 14.24.74.255	broadcast address – 14.24.74.207
Subnet mask – 255.255.255.192	Subnet mask – 255.255.255.240

SECTION-D (Learning levels 4,5,6)

7. (a) Consider an instance of TCP's Additive Increase Multiplicative decrease (AIMD) algorithm where the window size at the start of the slow start phase is 2 MSS and the threshold at the start of the first transmission is 8 MSS. Assume that a timeout occurs during the fifth transmission. Find the congestion window size at the end of the tenth transmission. Explain the answer systematically. [4]

Ans:

Initial window size or window size for first transmission: cwnd = 2 MSS

For 2nd transmission → cwnd = 22 = 4 MSS

For 3rd transmission → cwnd = 23 = 8 MSS

When threshold is reached then additive increase

For 4th transmission → cwnd = 8 + 1 = 9 MSS

For 5th transmission → cwnd = 9+ 1 = 10 MSS(fails)

Now window size reduced to 10/2 =5 MSS

For 6th transmission → cwnd = 1 MSS

For 7rd transmission → cwnd = 21 = 2 MSS

For 8th transmission → cwnd = 22 = 4 MSS

Threshold reached now additive increase

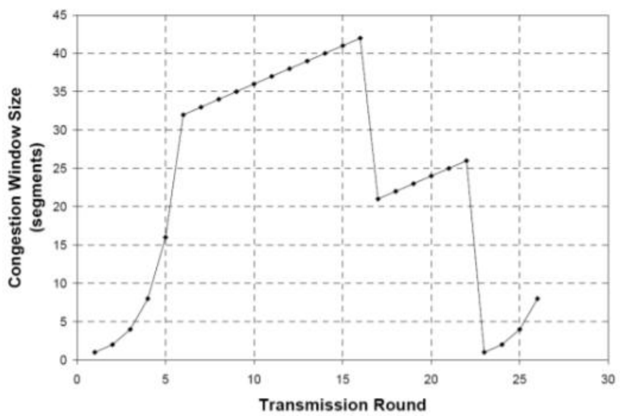
For 9th transmission → cwnd = 4 + 1 = 5 MSS

For 10th transmission → cwnd = 5 + 1 =6 MSS

So, at the end of 10th successful transmission

The congestion window size will be 6 + 1 = 7 MSS

(b) Consider the following plot of TCP window size as a function of time. [4]



Assuming TCP Reno is the protocol experiencing the behavior shown above, answer the following questions. In all cases, you should provide a short discussion justifying your answer.

(i) What is the initial value of Threshold at the first transmission round?

Ans: 32

(ii) Identify the intervals of time when TCP congestion avoidance is operating.

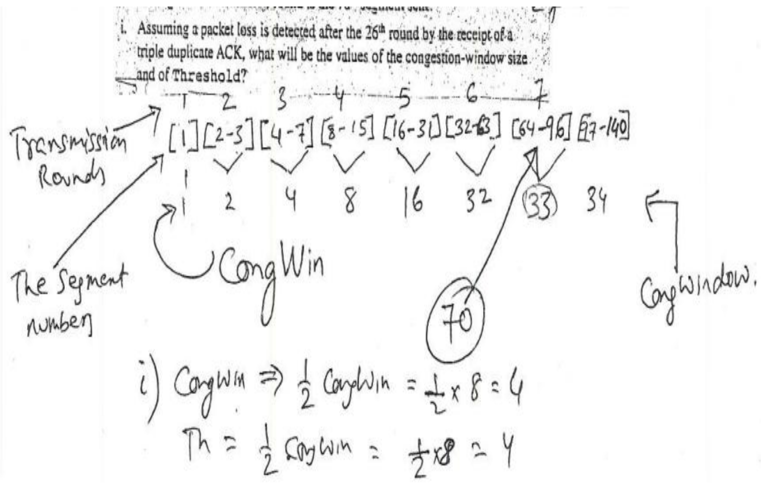
Ans: [6-16] and [17-22]

(iii) After the 16th transmission round, is segment loss detected by a triple duplicate ACK or by a timeout?

Ans: Triple duplicate

(iv) Assuming a packet loss is detected after the 26th round by the receipt of a triple duplicate ACK, what will be the values of the congestion-window size and of Threshold?

ANS:


i. Assuming a packet loss is detected after the 26th round by the receipt of a triple duplicate ACK, what will be the values of the congestion-window size and of Threshold?

8.	(a)	(i) Explain the single-bit parity error-detection code using a single byte of data. How many bit errors can this code detect? (ii) Based on the single-bit parity error-detection code devise a new code to detect and correct a single 1-bit error in 4 bytes of data. How many parity bits do you require? You may assume that parity bits are error-free. Ans: Bit (i) - 2 Marks Bit(ii) - 2Marks	[4]
	(b)	Write short notes on any 2 of the followings: i) Piggybacking. ii) Checksumming technique. iii) Congestion control. iv) RIP and OSPF.	[4]
		*****	