G – 16792

Register No. | | | | | | | | |

BE Degree Examination November 2024

Fifth Semester

Computer Science and Engineering

22CST52 – COMPUTER NETWORKS

(Regulations 2022)

Time: Three hours Maximum: 100 marks

Answer all Questions

Part – A (10 × 2 = 20 marks)

1. Show the transmission delay for a 100 KB message is sending over the network, if the bandwidth of the network is 1 Gbps. 0.8ms [CO1,K2]
2. Identify the message formats follows in five-layer internet protocol stack. [CO1,K3]
3. Select the appropriate application layer protocol for the following popular internet application. [CO2,K3]
   a) E-mail (Ex. Gmail) SMTP / POP3 / IMAP
   b) Streaming multimedia (Ex.YouTube) HTTP / RTP
   c) Internet Telephony (Ex. Whatsapp) SIP / RTP
   d) Remote Terminal Access (Ex. PuTTY) Telnet / SSH
4. Illustrate file distribution problem. [CO2,K2]
5. Show the TCP Header format. [CO3,K2]
6. Compare connection oriented and connection less protocol service. [CO3,K2]
7. Choose the appropriate classes (A, B, C, D, E) of the following IP address. [CO4,K3]
   a) 208.34.54.12 – C
   b) 129.14.6.8 – B
   c) 11110111 11110011 10000111 11011101 – E
   d) 10.0.0.10 – A
8. Outline the Dijkstra's algorithm. [CO4,K2]
9. Identify the type of MAC address. [CO5,K3]
   a) A3 : 34 : 45 : 11 : 92 : F1 – Multi
   b) A2 : 84 : 95 : 22 : 92 : E7 – uni
   c) FF : FF : FF : FF : FF : FF – broad
   d) 4A : 30 : 10 : 21 : 10 : 1A – uni
10. Build an institutional network connected together by four switches. Use the following data to build the network. [CO5,K3]
    1) The network should have external internet connection, one web server, one mail server.
    2) EEE department has 5 computers, CSE department has 10 computer, ECE department has 15 computers.

Part – B (5 × 16 = 80 marks)

11. a. i) Illustrate packet switching and principle used in it. (8) [CO1,K2]

ii) Estimate the nodal delay and end-to-end delay for a frame of size 5 million bits that is being sent on a link with 10 routers each having a queuing time of 20 ms and processing time of 100 ms, the length of the link is 2000 km. the speed of light inside the link is 2×10^8 m/s. The link has a bandwidth of 5 mbps. (8) [CO1,K3]

dtrans = 1s dprop = 10ms dnodal = 1130ms

dend-to-end = 12.43 s

(OR)

b. i) Explain briefly about five-layer internet protocol stack with neat sketch. (8) [CO1,K2]

ii) Consider a source host wants to send a message to a destination host. The message size is 64 KB in between source and destination host, there is a link-layer switch and a router is attached. Assume the sender is sending an e-mail message (i.e reliable data transfer protocol used in transport layer), sender using IPV4 address in Network layer, the entire network is connected by using Ethernet cable (i.e., Ethernet protocol used in data link layer) and 32-bit CRC as trailer portion for error detection and correction. (8) [CO1,K3]

Answer the following questions.

msg size = 65536 + 20

1) What will be the message size after adding transport layer header (H_t).
2) What will be the message size after adding network layer header (H_n)? 65556+20
3) What will be the message size after adding link layer heading and trailer (HT_l)? 65576 + 4 + 14 = 65594
4) How many layers the message has travelled over a network? 4 layers

12. a. Illustrate the following E-mail scenario's with neat diagrams. (16) [CO2,K2]

1) A high-level view of the internet e-mail system
2) Alice sends a message to Bob
3) E-mail protocols and their communicating entities.

(OR)

b. Outline the client-server application using TCP socket programming. (16) [CO2,K2]

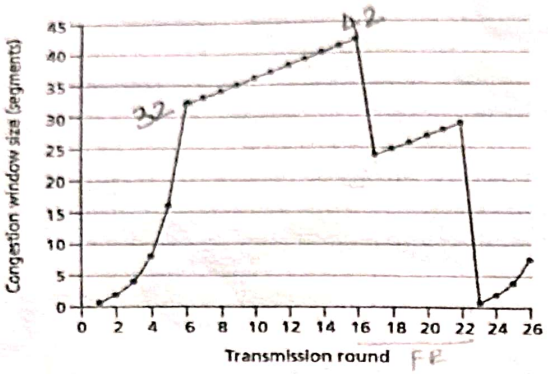
13. a. Develop a pipelined data transfer between sender and receiver by using the following protocol methods. (16) [CO3,K3]

1) Go-Back-N (GBN)
2) Selective Repeat (SR)

(OR)

b. Assuming TCP Reno is the protocol experiencing the behaviour shown below, answer the following Questions. In all cases, you should provide a short discussion to justify your answer. (16) [CO3,K3]

(*ssthresh* = slow start threshold)



1) Identify the internals of time when TCP slow start is operating
2) Identify the intervals of time when TCP congestion avoidance is operating.
3) After the 16th transmission round, is segment loss detected by a triple duplicate ACK (or) by a time out?
4) What is the value of *sstresh* at the 18th transmission round?
5) During what transmission round in the 70th segment sent?
6) 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 *sstresh*?
7) Suppose TCP Tahoe is used (instead of TCP Reno), and assume the triple duplicate ACKs are received at the 16th round. What are the *sstresh* and the congestion window size at the 19th round?
8) Again suppose TCP Tahoe is used, and there is a timeout event at 22nd round. How many packets have been sent out from 17th round till 22nd round, inclusive?

14. a. i) Explain IPV4 Header format. (8) [CO4,K2]

ii) And ISP in granted a block of address starting with 190.100.0.0/16 (65, 536 address) the ISP needs to distribute these addresses to three group of customers as follows: (8) [CO4,K3]

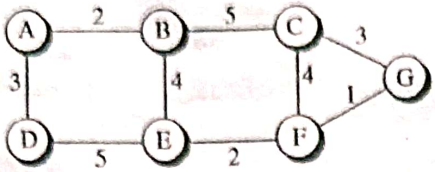
1) The first group has 64 customer; each needs 256 addresses.
2) The second group has 128 customers; each needs 128 addresses.
3) The third group has 128 customers; each needs 64 addresses.

Organize the sub blocks and find out how many addresses are still available after these allocations.

(OR)

b. i) Explain distance vector algorithm. (8) [CO4,K2]

ii) Apply distance vector algorithm and construct the least cost tree for the given network. (8) [CO4,K3]



15. a. i) Explain parity check and checksum error detection technique. (6) [CO5,K2]

ii) Make use of cyclic Redundancy check (CRC) algorithm and generate the CRC codeword at the sender side and also verify at the receiver side without error and with single-bit error. (Assume dataword = 1001 and divisor = 1011) (10) [CO5,K3]

(OR)

b. i) Illustrate the principles of network security and cryptography. (6) [CO5,K2]

ii) Assume Alice wants to send a message to Bob. Alice's message in its original form (for Example, "Bob, I love you. Alice") is known as plaintext. If Alice encrypts her plaintext message by using the following symmetric key encryption algorithms, then what will be the encrypted message, known as ciphertext? (10) [CO5,K3]

1) Caesar cipher (if k = 3)
2) Mono alphabetic cipher
3) Poly alphabetic encryption. (with k = 5 and k = 19)

Bloom's Taxonomy Level	Remembering (K1)	Understanding (K2)	Applying (K3)	Analysing (K4)	Evaluating (K5)	Creating (K6)
Percentage	–	48	52	–	–	–

B.E Degree Examination November-2024

V Semester - CSE

22CST52 - COMPUTER NETWORKS (R2022)

PART-A

1) Calculate transmission delay. (2M)

Message - 100 KB

Bandwidth - 1 Gbps.

Transmission delay $T_d = \frac{\text{Message size}}{\text{Bandwidth}} = \frac{100\,KB}{1\,Gbps} = \frac{100 \times 8\,Kb}{1\,Gbps}$

$T_d = 0.8\,ms$

2) Message format (2M)

Application layer - Data - message

Transport layer - Segment | Transport layer Header | Data |

N/w layer - packet | N/w layer Header | Segment |

Data link layer - Frame | Data link layer header & trailer | packet |

physical layer - Bits (frame converted into binary signal)

3) Application layer protocol. (2M)

a) E-mail → Sending mail - SMTP
Receiving mail - POP3 / IMAP

b) Streaming multimedia → HTTP / RTP

c) Internet Telephony → SIP / RTP.

d) Remote Terminal Access → Telnet / SSH

4) Illustrate file distribution problem. (2M)

Client-Server ⇒ Server directly sends the file to all clients

minimum distribution time $D_{cs} = \text{Max}\left(\frac{NF}{U_s}, \frac{F}{d_{min}}\right)$

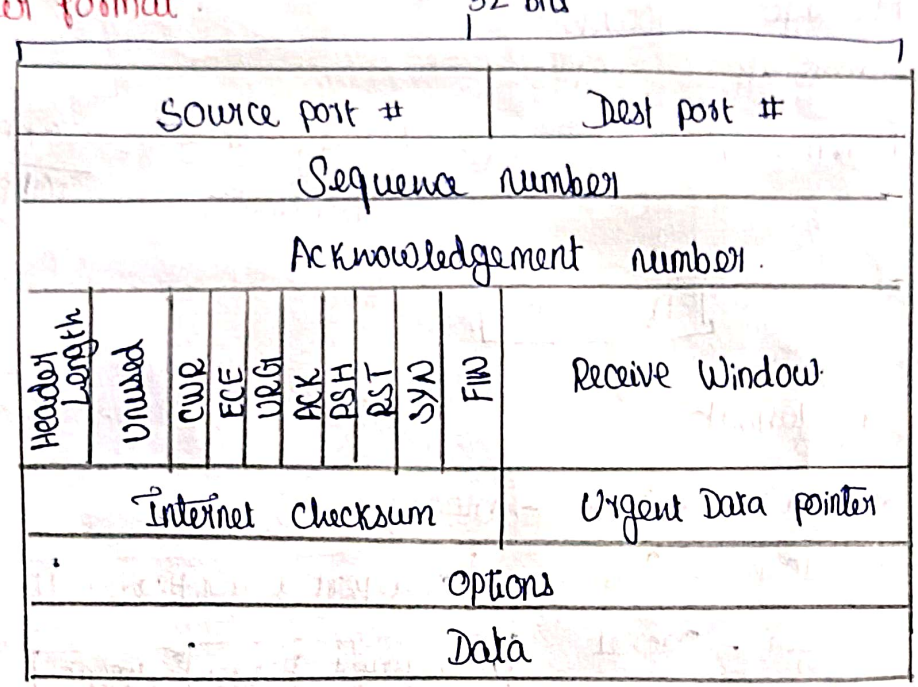
D_{cs} Yes as peers ↑es.

Peer-to-peer → One peer obtain file from server. Peer distribute to other peers.

$$D_{P2P} = \max\left\{ \frac{F}{U_S}, \frac{F}{d_{min}}, \frac{NF}{U_S + \sum_{i=1}^{N} U_i} \right\}$$

$D_{P2P} < D_{CS}$

5) TCP Header format.



6) (2M)

Connection Oriented	Connectionless protocol.
i) It gives the guarantee of reliability	It does not give a guarantee of reliability
ii) It requires authentication	Does not require authentication.
iii) Packets follow same route	Packets donot follow same route
iv) Require bandwidth of high range	Require BW of low range.
v) TCP	UDP.

7) Classes of IP address (4 × 1/2 = 2M)

208.34.54.12 → Class C

129.144.6.8 → Class B

11110111 11110011 10000111 11011101 → Class D

100.0.10 → class A.

8) Dijkstra's algorithm.

- Find the shortest paths from the source to all other vertices.

Algorithm

* declare two arrays

distance[] - to store the distances from source vertex to other vertices in graph.

Visited[] - to store visited vertices.

* Set distance[S] = 0 distance[V] = ∞, V → all other vertices in the graph.

* Add S to the visited[] array & find the adjacent vertices of S with the minimum distance.

* adjacent to S, say A has minimum distance and is not in visited array. A is added to visited array & the distance A is changed from ∞ to assigned distance of A.

9) Identify MAC address. (4 × 1/2 = 2M)

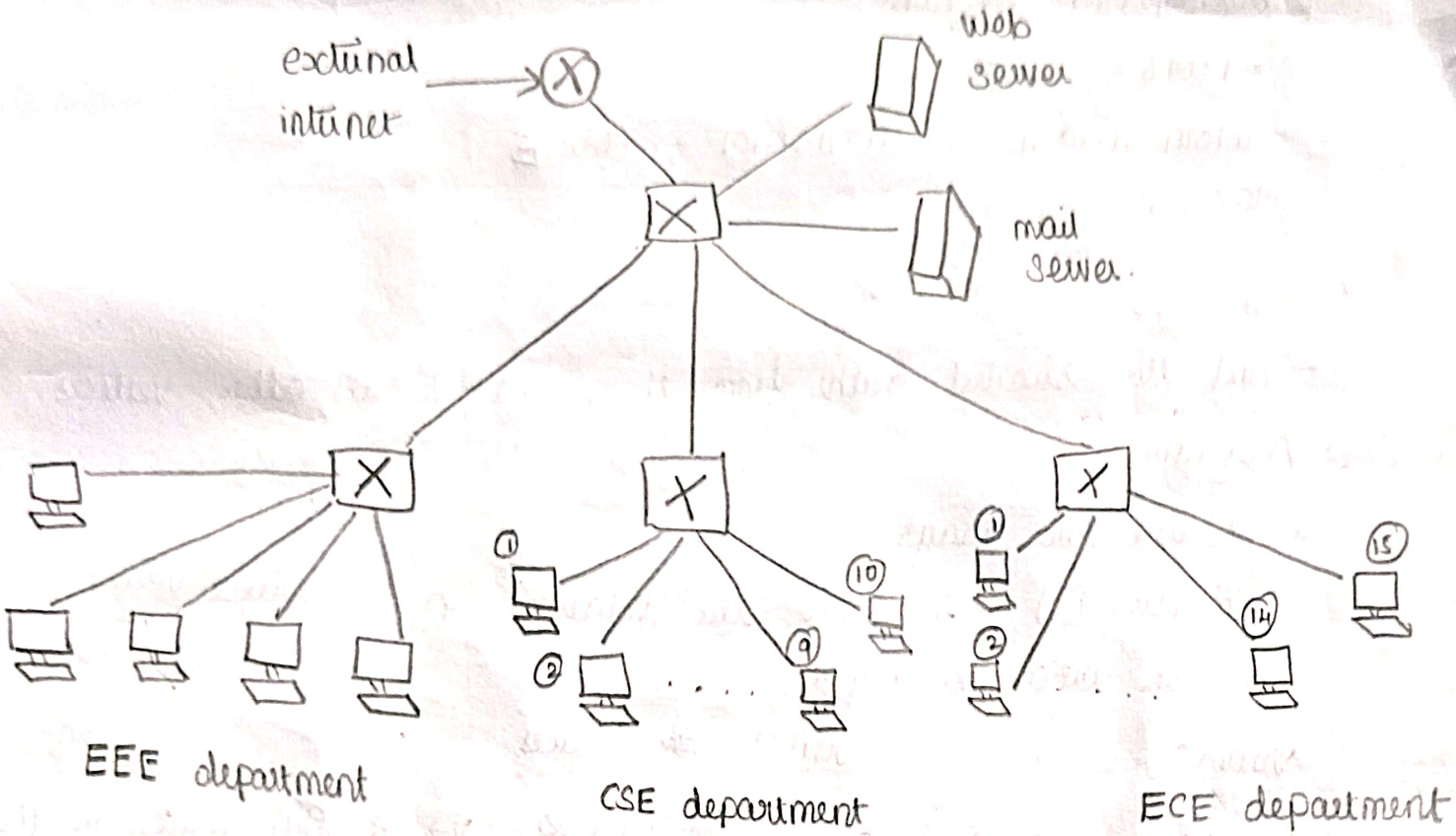
A3:34:45:11:92:F1 → Multicast

A2:34:95:22:92:E7 → Unicast.

FF:FF:FF:FF:FF:FF → Broadcast

4A:30:10:21:10:1A → Unicast.

10) Institutional network.



PART-B

11) a) Packet Switching. (2M)

→ To send message from source to destination, the source breaks long messages into smaller chunks of data known as packets.

⇒ packets travel through communication link & switches.

⇒ packets transmitted at a rate of L/R seconds.

L → Length of packets.

R → Transmission rate.

(2M)

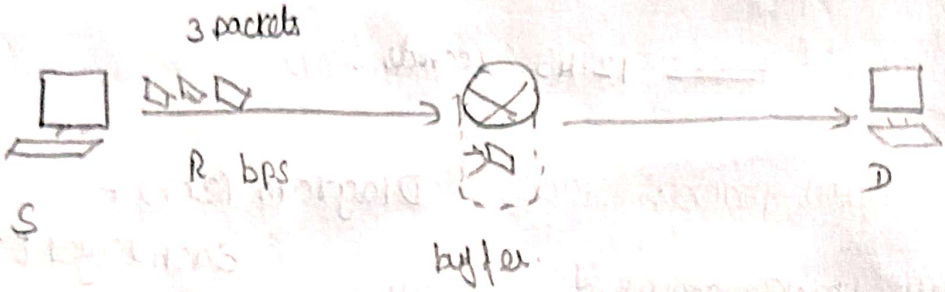
Store and Forward transmission.

→ packet switch must receive the entire packet before it transmit the first bit of the packet to outbound link.

eg. source has 3 packets each of L bits. (1M)

→ source transmitted some of packet 1 & the front of packet 1 has arrived the router

→ Router (buffer) stores data until all the packet's bit are received & it begin to transmit.



→ source begins to transmit at t=0.

→ At L/R it reaches Router. At L/R second packet start transmitting from source.

→ At 2L/R destination has received first packet. Router receives second packet.

→ At 3L/R destination received first two packets & router received 3rd packet.

→ At 4L/R destination received all four packets.

ii) Nodal delay

$$d_{trans} = \frac{\text{Frame size}}{\text{Link B.W}} = \frac{5\times10^6 \text{ bit}}{5\times10^6 \text{ bps}} = 1 \text{ second.} \quad (1M)$$

$$d_{prop} = \frac{\text{Distance}}{\text{propagation speed}} = \frac{2\times10^6}{2\times10^8} = 10 \text{ ms.} \quad (1M)$$

$d_{queue} = 20 \text{ ms.}$

$d_{proc} = 100 \text{ ms.}$

$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$ (3M)

$= 100\text{ms} + 20\text{ms} + 1000\text{ ms} + 10\text{ms} = 1130 \text{ ms}$

$d_{end\text{-}to\text{-}end} = N(d_{proc} + d_{trans} + d_{prop} + d_{que})$ (3M)

$= 11(100\,ms + 1000\,ms + 10\,ms + 20\,ms)$

$= 11(1130\,ms)$

$= 11 \times 1$ Second.

$= 12.43$ Seconds.

b) i) Five layer internet protocol stack. Diagram (3M) + Each layer (5M)

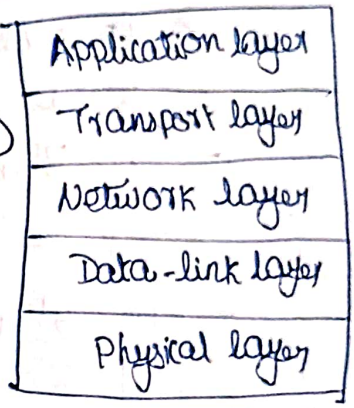
Internet protocol stack consist of five layers

Application layer:

→ provide n/w services directly to end-user applications. (end-to-end application)

→ information referred as message

→ protocols → HTTP (HyperText Transfer protocol)
FTP (File Transfer protocol)
SMTP (Simple Mail Transfer protocol)
DNS (Domain Name System)



Transport layer

→ ensures reliable data transfer.
→ provides end-to-end communication between hosts.
→ transport layer packet referred to as segment.
→ two protocols TCP & UDP
→ TCP - provides connection oriented service
- ensures guaranteed delivery of application-layer messages to the destination & flow control.

UDP - provides connectionless service

Network layer

⇒ Network layer packet known as datagrams.

⇒ responsible for routing data packets across different networks.

- responsible for i) routing & forwarding data
  ii) Logical addressing & packet fragmentation
  iii) Error reporting (ICMP protocol)
- routing packets using IPV4 & IPV6. - 128-bit addressing.
  32-bit addressing
  ARP - Resolve MAC address to IP address.

Link layer

- move packets from one node to next node in the route
- ⇒ link layer packets referred to as frames.
- Sub layers - logical link control & media access control
- Protocol - Ethernet, Wi-Fi

Physical layer

- physical transmission of raw binary data over physical medium.
- Transmission media - copper cables, fiber optics, wireless.
- Transmission mode - simplex, half-duplex, full-duplex.

ii) Given:

Message size = 64KB (2M)

1) Transport layer is TCP ⇒ header size - 20 bytes

Message size = 64 x 1024 = 65536 bytes.

Total size after Transport layer header = 65536 + 20

= 65556 bytes.

2) Network layer header size (IPV4) - 20 bytes (2M)

Total message size = 65536 + 20 = 65576 bytes.

3) Link layer protocol - ethernet (2M)

header - 14 bytes trailer (CRC) - 4 bytes

Total message size = 65576 + 24 + 14 = 65594 bytes

4) 4 layers. (2M)

12) a) i) A high-level view of internet e-mail system Diagram - 3M
Explanation - 3M

User agent - mail reader.

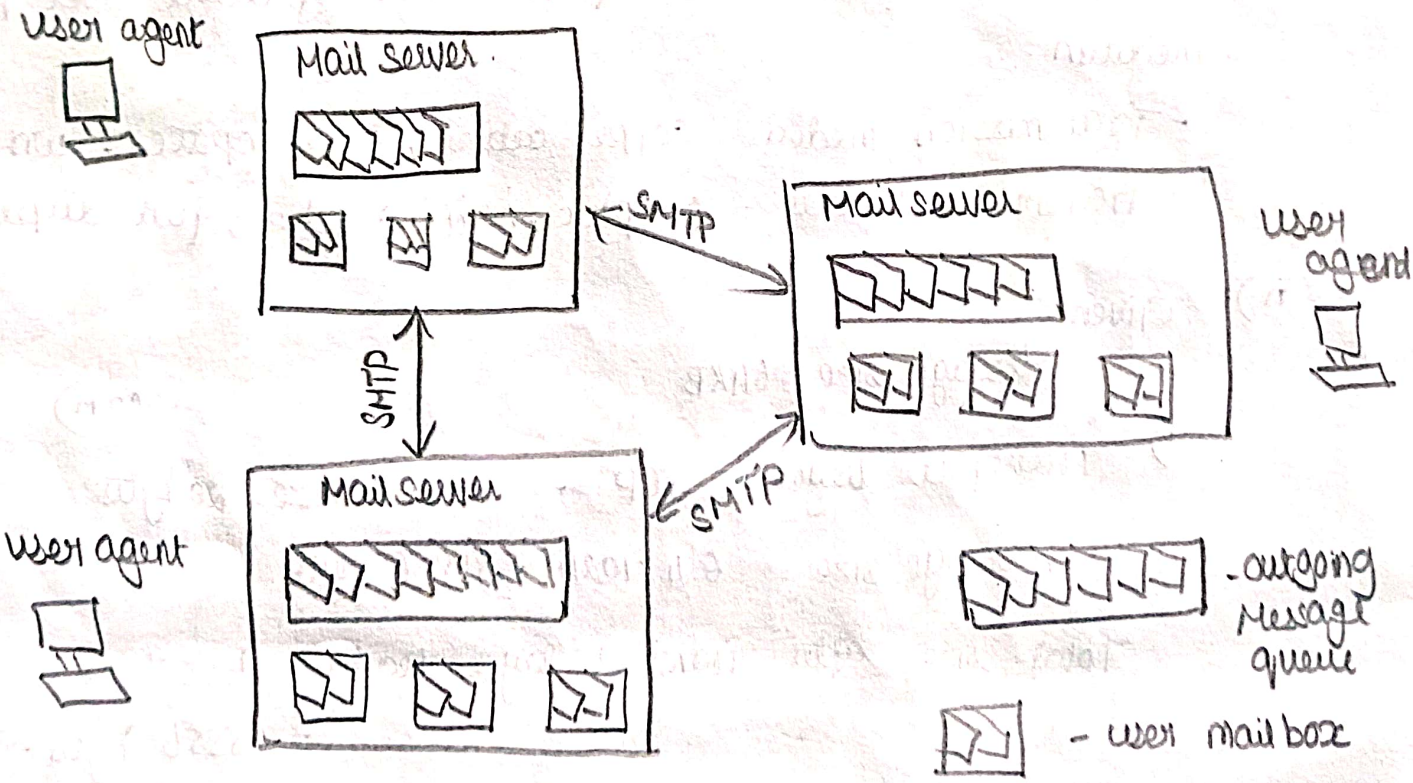
- allows users to read, reply to, forward, save and compose messages.

eg: Microsoft outlook / Apple mail

Mail server → Mailbox - contains incoming messages for user.

Message queue - contain outgoing mail messages.

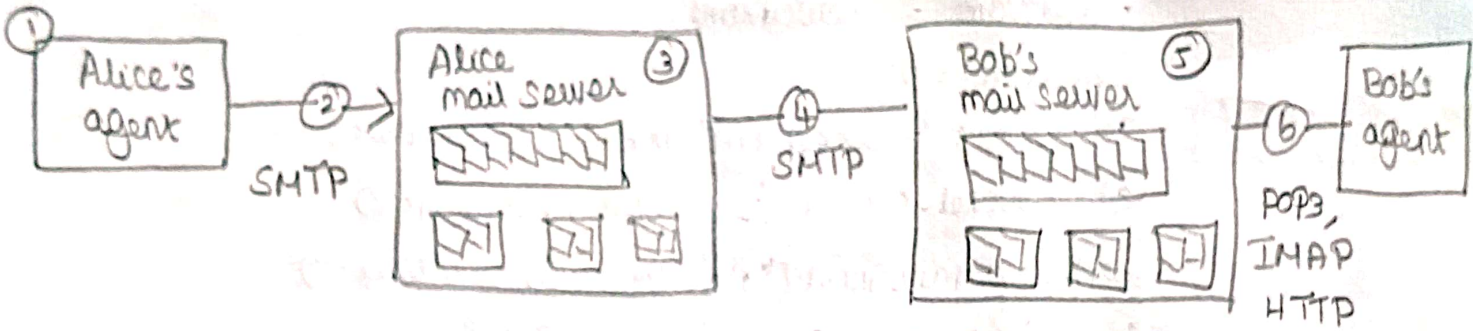
SMTP protocol → Transfer mail from sender's mail server (client side) to recipients mail server. (server side)



2) Alice sends a message to Bob

Diagram - 2M
Explanation - 2M.

* Alice uses user agent to compose e-mail message to Bob.
* Alice user agent sends message to her mail server using SMTP; message placed in message queue.
* Client side of SMTP at mail server opens TCP connection with Bob's mail server.
* SMTP client sends Alice's message over TCP connection.
* Bob's mail server places the message in Bob's mailbox.
* Bob invokes his user agent to read message.



3) E-mail protocols and their communication entities. (2M)

- email message need to be deposited in Bob's mail server.

SMTP - used to push email message from Alice user agent to her mail server & from Alice Mail server (SMTP client) to Bob's mail server.

- Bob's user agent has to pull message from mail server - uses POP3, IMAP & HTTP.

b) Client-Server application using TCP Socket programming. (4M)

Socket - door between application process & end to end Transport protocol.

Socket programming

⇒ Server - Server process must be running first.
Socket must be created to contact client.

Client - Create TCP socket specifying IP address, port number of Server process.

Client TCP establishes connection to server TCP.

Server - Server creates socket for each client to allow server to talk with multiple client.

Client source number & IP address distinguish clients

TCP Client.py (6M)

```
from socket import *
ServerName = 'servername'
ServerPort = 12000
clientSocket = socket(AF_INET, SOCK_STREAM)
clientSocket.connect((ServerName, ServerPort))
sentence = raw_input("I/P lowercase sentence: ")
clientSocket.send(sentence.encode())
newsentence = clientSocket.recv(1024)
Print('New sentence: ', newsentence.decode())
clientSocket.close()
```

TCP Server.py (6M)

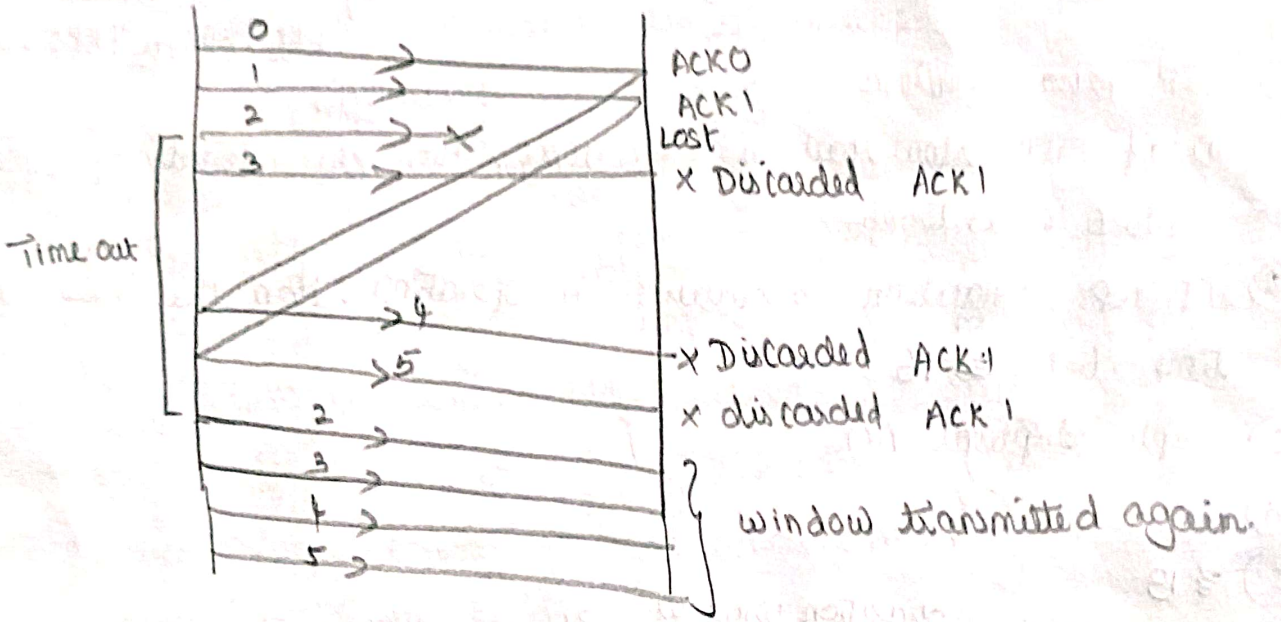
```
from socket import *
ServerPort = 12000
serverSocket = socket(AF_INET, SOCK_STREAM)
serverSocket.bind(('', serverPort))
serverSocket.listen(1)
While True:
    connectionSocket, addr = serverSocket.accept()
    lowerc = connectionSocket.recv(1024).decode()
    upperc = lowerc.upper()
    connectionSocket.send(upperc.encode())
    connectionSocket.close()
```

13) a) 1) Go Back N (GBN) (2M)

- Sender can send multiple data packets without waiting for an acknowledgement for each one.
- If one packet is lost or not acknowledged, sender must go back and resend that packet and all the packets that follow it.

window size - determines no. of packets sender can transmit without acknowledgement.

eg: Assume window size = 4, packets = 0 to 5, (6M)
suppose packet 2 is lost.



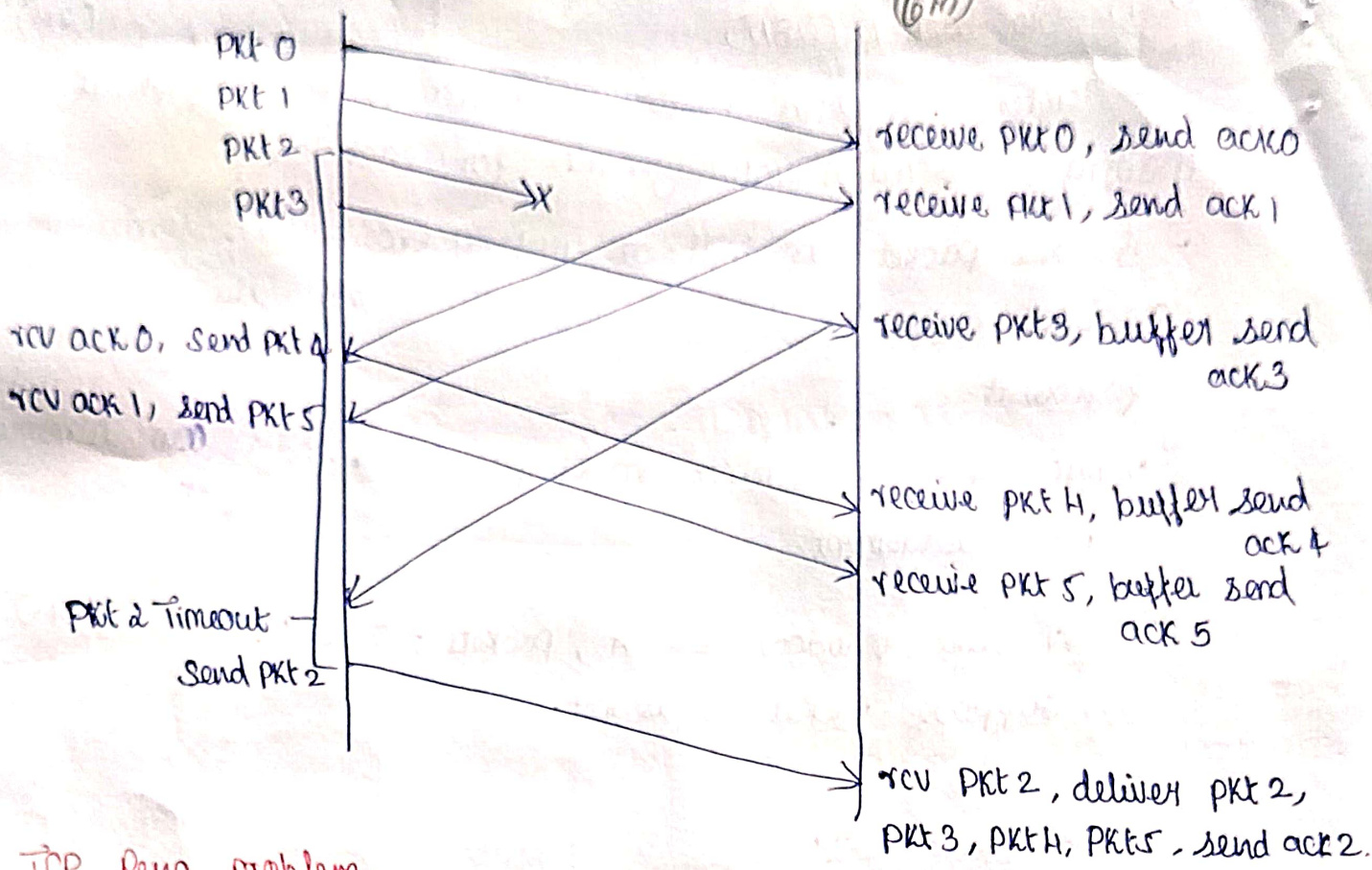
2) Selective Repeat (SR) (2M)

GBN - bandwidth wasted in retransmitting frames.

Selective repeat - allow the receiver to accept & buffer the frames following a damaged or lost one.

eg: Assume window size = 4 packets = 0 to 5. Suppose packet 2 is lost.

(6m)



b) TCP Reno problem.

(8x2 = 16M)

1) If TCP slow start is operating, then the intervals of time 1 to 6 & 23 to 26.

2) If TCP congestion avoidance is operating, then the intervals of time 6 to 16.

3) triple duplicate ACK

4) 21

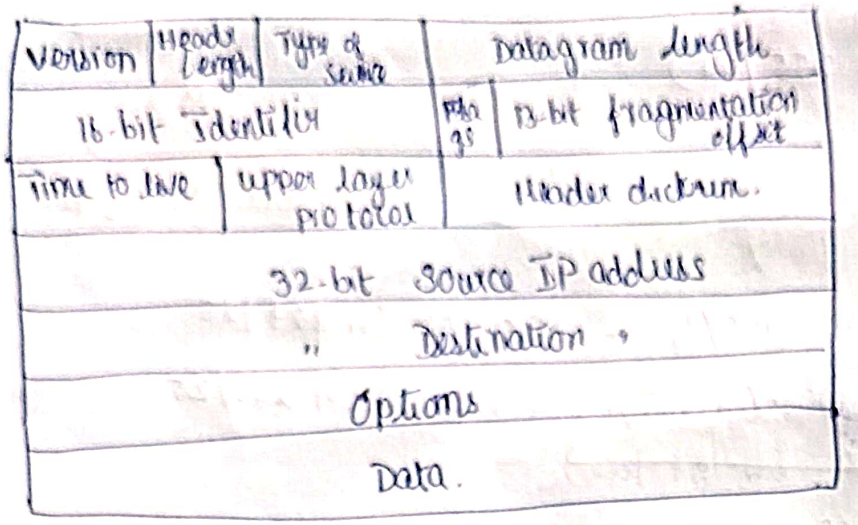
5) 13

6) 4 sthresh = $\frac{\text{congestion window}}{2}$ = 8/2 = 4.

7) ssthresh = 1 congestion window size is 21

8) 48.

14) a i) IPV4 Header Format. (4+4M)



Version - IP version (IPV4=4) (size = 4 bits)
Header length - Length of the header in 32-bit words (4 bit)
Type of service - used for QoS, now part of differentiated services (8 bit)
Datagram length - Header + data (16 bit)
Identifier - unique ID for packet fragments (16 bit)
flags - control flags (DF, MF) (3 bit)
fragmentation offset - offset for fragmented packets (13-bit)
TTL - maximum hops allowed before packet is discarded (8 bit)
protocol - protocol used in upper layer TCP, UDP (8-bit)
checksum - Error checking for IP header. (16-bit)
options - optional fields for additional settings.
padding - To ensure header is 32-bit aligned.

(ii) Group 1 (8M)

Each customer need 256 addresses ie 8 bits ($\log_2 256$)
The prefix length 32-8 = 24 (2M)

1st customer
2nd customer
192.100.0.0/24 (192.100.0.0 - 192.100.0.255)
192.100.1.0/24 (192.100.1.0 - 192.100.1.255)

64th customer 190.100.63.0/24 Total = 64 × 256 = 16394.

[190.100.63.255/24.

- 190.100.63.255/24)

Group 2 (2M)

each customer needs 128 addresses · 7 bits ($\log_2 128$)

Prefix length 32-7 = 25

1st customer - 190.100.64.0/25 - 190.100.64.127/25

2nd - 190.100.64.128/25 - 190.100.64.255/25.

~~190.100.64.127/25)~~

~~190.100.64.255/25)~~

128th - 190.100.127.128/25 to 190.100.127.255/25.

Total = 127 × 128 = 16384.

Groups - needs 64 addresses. (2M) customer 1 - [190.100.128.0/26 - 190.100.128.63/26]

6 bits needed. ($\log 64$) 128 × 64 = 8192.

no.of granted addresses to the ISP → 65,536 (2M) customer 128 - [190.100.159.192/26 - 190.100.159.255/26]

allocated → 40,960.

available → 24576.

b) i) Distance vector algorithm. (8M)

- used to determine the best path to forward packets through an internetwork.
- each router maintains routing table that stores the distance to reach each destination & next hop router.

Algorithm

1) Initialization - Initialize routing table with direct neighbors cost = 1 & others cost = ∞

2) Routing table exchange - exchange routing table to all of its directly connected neighbors.

3) update mechanism.

→ when a router receives a routing table from a neighbor, it compares the cost of the route via that neighbor to the existing route in its own table.

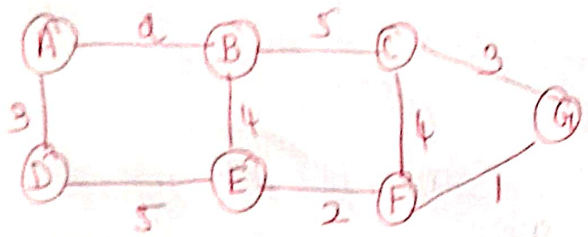
→ If the received route offers a better path to any destination, the router updates its table with new cost & next hop.

→ algorithm follows Bellman-Ford equation

$$cost(A \to D) = \min(cost(A \to B) + cost(B \to D))$$

4) The algorithm continues to update & exchange tables until no update.

ii)



Initialization

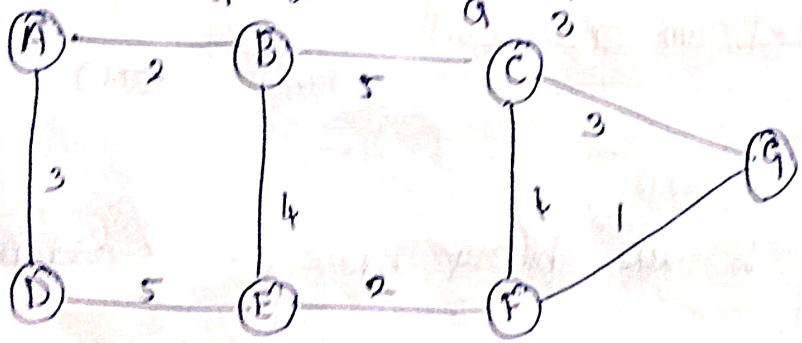
A	0
B	2
C	∞
D	3
E	∞
F	∞
G	∞

A	2
B	0
C	5
D	∞
E	4
F	∞
G	∞

A	∞
B	5
C	0
D	∞
E	∞
F	4
G	3

(1+4)

A	∞
B	∞
C	3
D	∞
E	∞
F	1
G	0



A	3
B	∞
C	∞
D	0
E	5
F	∞
G	∞

A	∞
B	4
C	∞
D	3
E	0
F	2
G	∞

A	∞
B	∞
C	4
D	∞
E	2
F	0
G	1

Receive distance from neighbors B, D (2M)

	B	D	old A	New A
A	2	3	0	A 0
B	0	5	2	B 2
C	5	∞	∞	C 7
D	5	0	3	D 3
E	4	5	∞	E 6
F	∞	∞	∞	F ∞
G	∞	∞	∞	G ∞

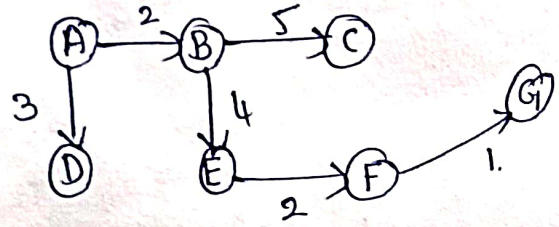
Receive update from E

	New A
A	0
B	2
C	7
D	3
E	6
F	8
G	∞

Receive update from F

	New A
A	0
B	2
C	7
D	3
E	6
F	8
G	9.

(2M)



15) a) Parity check & checksum error detection.

(3M)

Parity check

- to detect single bit error
- parity bit added to make binary representation odd parity/ even parity.
- at receiver parity of received data is checked, if parity doesn't match error is detected.

Checksum (3M)

- Sender divides the data into fixed size segment & adds them using binary addition.
- Sum complemented to form checksum
- data & checksum sent together
- at receiver data segments & checksum added
- result all 1's ⇒ error free otherwise error

ii) CRC

Sender (5M)

Append (4-1) zeros

```
      101
   ------
1011 | 1001000
     | 1011
     ------
       1000
       1011
       ----
        110
```

CRC code word = 1001110

Receiver without error (2M)

```
      1010
   ------
1011 | 1001110
     | 1011
     ------
       1011
       1011
       ----
          0
```

With single bit error (3M)

```
      1011
   ------
1011 | 1000110
     | 1011
     ------
       1111
       1011
       ----
       1000
       1011
       ----
         11
```

Non zero ⇒ error in data.

b) i) Network security & cryptography.

(3M)

Network security

→ ensures sensitive information is only accessible to authorized users. (encryption technique)

→ data remains unchanged during transmission.

→ Verifies identity of user attempting to access.

Cryptography

→ converts plaintext into ciphertext (encryption) to ensure confidentiality

→ Decrypts ciphertext back to plaintext with correct key

→ Symmetric encryption - Same Key is used for encryption & decryption

→ Asymmetric encryption - public & private Key are used

→ converts data into a fixed length hash value to ensure integrity

→ Hashes are irreversible & used in digital signatures.

ii) Symmetric Key Encryption

1) Caesar Cipher K=3 (3M)

Plaintext - Bob, I love you. Alice

Ciphertext - Ere, L oryh brz. Dolfh.

2) Mono alphabetic Cipher (3M)

Substitution table

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V

X	Y	Z
B	N	M

Ciphertext - WQW, O SGCT NGIX. QSOET. (4M)

3) Poly alphabetic encryption

Ciphertext with K=5 ⇒ Gtg, N qtaj dtz. Fqnhj

K=19 ⇒ whw, z ehox rhn. Tezvx

Pattern (any pattern can be accepted) eg: $C_1C_2C_1C_2$.

Faculty

(Dr. S SUDHA AP/ECE)