Evaluation Scheme for Q1: Correct answer (with justification) 2 Marks. Partial answer (answer without justification) 1 mark.

1 (a). For a p2p file-sharing application, do you agree with the statement, "There is no notion of client and server sides of a communication session"? <2 points> Why or why not?

No. All communication sessions have a client side and a server side. In a P2P file-sharing application, the peer that is receiving a file is typically the client and the peer that is sending the file is typically the server.

1(b). What is the Source and Destination IP address in a datagram that carries the ICMP message?

Source Address

The address of the gateway/router or host that composes the ICMP message.

Destination Address

The address of the gateway or host to which the message should be sent.

1(c) What are the use of Subnet mask in IP addressing?

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. It is used for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

1.(d). Mentioned the destination IP used in a packet for limited broadcast? Specify an application layer protocol that uses it?

Limited broadcast is the broadcast limited to a single LAN and which is to be received by all. It is sent to reserved Class E, IP address 255.255.255.255. DHCP packets uses Limited broadcast packets for its functionalities.

1(e). A system has n-layer…..

With n layers and h bytes added per layer, the total number of header bytes per message is **hn**, so the space wasted on headers is **hn**. The total message size is **M + nh**, so the fraction of bandwidth wasted on headers is **hn /(M + hn).**

1(f). If an IP packet has arrived with first 8 bits as 01000010 then whether it will be accepted or rejected? Why

There is an error in this packet. The 4 left-most bits (0100) show the version, which is correct. The next 4 bits (0010) show the header length; which means ($2 \times 4 = 8$), which is wrong. The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

1(g). The value o HLEN is 1010 how many options bytes are used?

Header length is scaled by a factor of 4. So, Actual header size $=10*4=40$B. Out of which 20B are necessary and remaining 40-20=20 bytes are for options.

1(h). How many sequence numbers are are consumed by SYN+ACK segments? Why

One. Server responds to the client request with SYN-ACK signal bits set. ACK signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with.

1(i) Explain way to do reassembling of IP fragments at the destinations?

Assuming an IP packet, a receiver assembling fragments has to

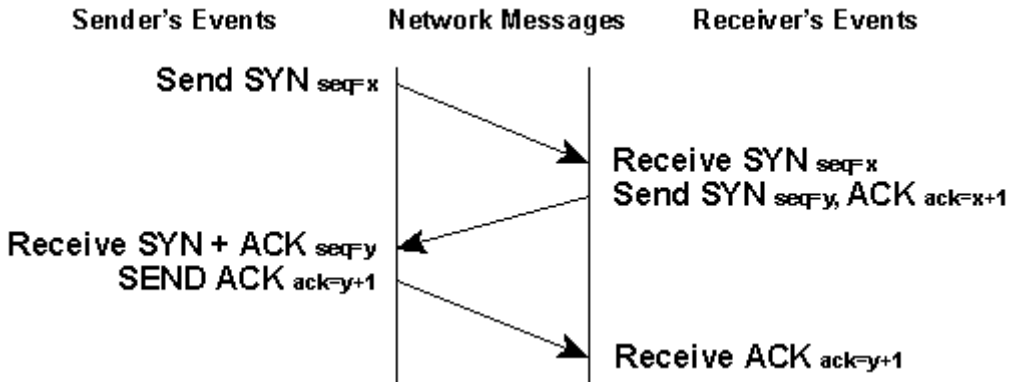
1) Intermediate nodes may not get all the fragments.

2) If assembled at intermediate node then there may be a need of fragmentation once which will be more costly as far as CPU and time is concerned.

1(j). One way of detecting errors is to transmit data as a block of n rows of k bits per row and adding parity bits to each row and each column. Will this scheme detect all single errors? Double errors? Triple errors?
Yes, it will detect all single errors, double errors, but NOT triple errors, as there is one case that three errors occur but none of the parity bits can detect. That is, when one message bit is flipped, and the corresponding row and column parity bits are flipped as well.

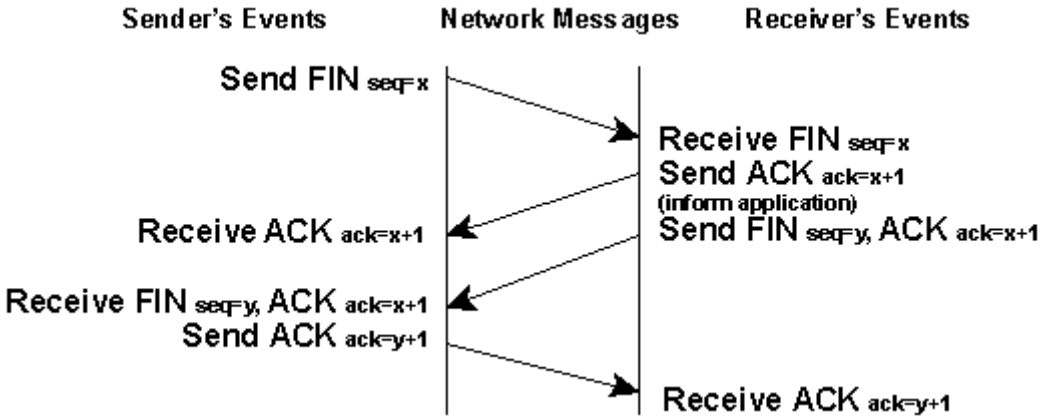
Evaluation Scheme for Q2:

a) Connection Establish



• The sender sends a SYN packet with sequence number say 'x'.
• The receiver on receiving SYN packet responds with SYN packet with sequence number 'y' and ACK with seq number 'x+1'
• On receiving both SYN and ACK packet, the sender responds with ACK packet with seq number 'y+1'
• The receiver when receives ACK packet, initiates the connection.

Connection Release



• The initiator sends a FIN with the current sequence and acknowledgement number.
• The responder on receiving this informs the application program that it will receive no more data and sends an acknowledgement of the packet. The connection is now closed from one side.
• Now the responder will follow similar steps to close the connection from its side. Once this is

done the connection will be fully closed.

b) **Channel efficiency= (t_{data}) / (t_{data} + t_{ACK} + 2 t_{prop})**

(t_{data} + t_{ACK} + 2 t_{prop})= (t_{data}) / Channel efficiency

2 t_{prop} = {(t_{data}) / Channel efficiency} - t_{data} - t_{ACK}

t_{prop} = [{(t_{data}) / Channel efficiency} - t_{data} - t_{ACK}] / 2

Evaluation Scheme for Q3:

a) Describing the NAT (2 Marks)
Working with example (2 Marks)
b) DNS functionalities (2 Marks)
Justification (2 Marks)

Evaluation Scheme for Q4:

a) <u>Limitations of Go-Back-N-ARQ are:</u>

- If error rate is high, it wastes a lot of bandwidth.
- Receiver do not store the frames received after the damaged frame until the damaged frame is retransmitted.
- Go Back N ARQ is inefficient for the noisy link.
- Retransmits all the frames that are sent after the frame which suspects to be damaged or lost.

<u>Selective Repeat ARQ overcomes these limitations.</u>

- Comparatively less bandwidth is wasted in retransmitting.
- Receiver stores the frames received after the damaged frame in the buffer until the damaged frame is replaced.
- Retransmits only those frames that are suspected to lost or damaged.

b) A CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. It a mechanism used in the half-duplex communication mode to help multiple PC/node to access the channel with a minimum delay time.

<u>Procedure of CSMA/CD</u>

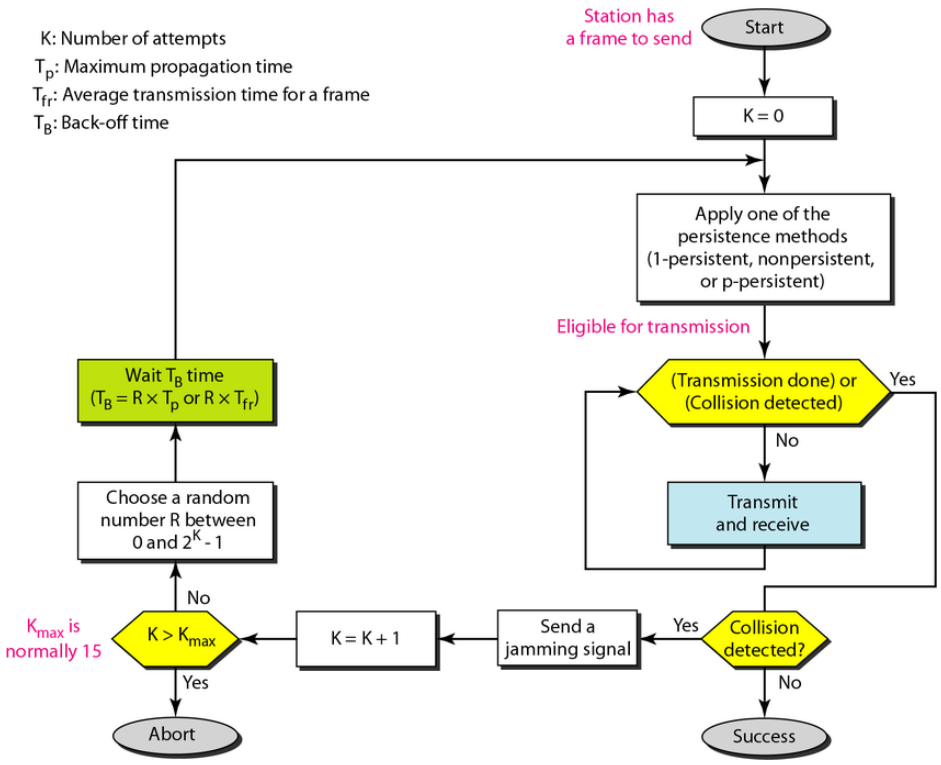
The following procedure is used to initiate a transmission. The procedure is complete when the frame is transmitted successfully or a collision is detected during transmission.

- Is a frame ready for transmission? If not, wait for a frame.
- Is medium idle? If not, wait until it becomes ready.
- Start transmitting and monitor for collision during transmission.
- Did a collision occur? If so, go to collision detected procedure.

- Reset retransmission counters and complete frame transmission.

The following procedure is used to resolve a detected collision. The procedure is complete when retransmission is initiated or the retransmission is aborted due to numerous collisions.

- Continue transmission (with a jam signal instead of frame header/data/CRC) until minimum packet time is reached to ensure that all receivers detect the collision.
- Increment retransmission counter.
- Was the maximum number of transmission attempts reached? If so, abort transmission.
- Calculate and wait the random backoff period based on number of collisions.
- Re-enter main procedure at stage 1.



Full duplex transmission is functionally much simpler than half-duplex transmission because it involves no media contention, no collisions and no need to schedule retransmissions. As communication is possible in both directions in full duplex mode, there is no chance of collision and no CSMA/CD mechanism is required to detect the same.

Evaluation Scheme for Q5:

a) $2^r >= m+r+1$ where m is no. of data bits, r is redundancy bits.

b) step-1: Initially, construct the routing table at node A with the local information.

Step-2: update the routing table at A after getting the distance vector information from B, D, &E.

Evaluation Scheme for Q6:

6.(a)(i) 192.53.00111000.7 → received IP (192.53.56.7)
255.255.11111110.0 → Subnet mask taken from routing table

192.53.56.0

None of the entries in routing table is matching, Hence the Default entry will be used by the router.

(ii) 192.53.00101000.7 → received IP (192.53.40.7)
255.255.11111110.0 →

192.53.40.0

Matching with the 3rd entry which will be used by the router to route the pkt.

(iii) 135.46.00111111.10 → received IP (135.46.63.10)
255.255.11111100.0

135.46.60.0

Matching with the 2nd entry which will be used by the router to route the pkt.

(iv) ~~135.46.57.14 → recei~~
135.46.00111001.14 → received IP (135.46.57.14)
255.255.11111100.0

135.46.56.0

Matching with the 1st entry which will be used by the router to route the pkt.

Note: Answer for every part will carry one mark each.

(b) Reason, for Layered Architecture will carry one mark.
Similarity between OSI and TCP/IP → Carries 1.5 marks
Distinction between OSI and TCP/IP – Carries 1.5 marks.

Evaluation Scheme for Q7:

a)

Evaluation Scheme:

- Correct answer with proper explanation : 4 Marks
- Some valid explanation with wrong answer: 1-3 marks

Answer:

The maximum size of data field in each fragment = 480 (20 bytes IP header).
Thus the number of required fragments is7
(3000-20)/480 = 7
Each fragment will have Identification number 422. Each fragment except the last one will be of size 500 bytes (including IP header). The last datagram will be of size 120 bytes (including IP header). The offsets of the 7 fragments will be 0, 60, 120, 180, 240, 300, 360. Each of the first 6 fragments will have flag=1; the last fragment will have flag=0.

b)

Evaluation Scheme:

- Correct comparison with explanation : 4 Marks
- Parial correct : 1-3 marks

Answer:

Comparison Chart
Distance Vector Routing Vs Link State Routing

SL. NO.	BASIS FOR COMPARISON	DISTANCE VECTOR ROUTING	LINK STATE ROUTING
1	Algorithm	Bellman ford	Dijsktra
2	Network view	Topology information from the neighbour point of view	Complete information on the network topology
3	Best path calculation	Based on the least number of hops	Based on the cost
4	Updates	Full routing table On broadcast	Link state updates On multicast
5	Updates frequency	Periodic updates	Triggered updates
6	CPU and memory	Low utilisation	Intensive
7	Simplicity	High simplicity	Requires a trained network administrator
8	Convergence time	Moderate	Fast
9	Hierarchical structure	No	Yes
10	Intermediate Nodes	No	Yes

Key Differences Between Distance Vector Routing and Link State Routing

- Bellman-Ford algorithm is used for performing distance vector routing whereas Dijsktra is used for performing the link state routing.
- In distance vector routing the routers receive the topological information from the neighbour point of view. On the contrary, in link state routing the router receive complete

information on the network topology.

- Distance vector routing calculates the best route based on the distance (fewest number of hops). As against, Link state routing calculates best route on the basis of least cost.
- Link state routing updates only the link state while Distance vector routing updates full routing table.
- The frequency of update in both routing technique is different distance vector update periodically whereas link state update frequency employs triggered updates.
- The utilization of CPU and memory in distance vector routing is lower than the link state routing.
- The distance vector routing is simple to implement and manage. In contrast, the link state routing is complex and requires trained network administrator.
- The convergence time in distance vector routing is slow, and it usually suffers from count to infinity problem. Conversely, the convergence time in link state routing is fast, and it is more reliable.
- Distance vector doesn't have hierarchical structure while in link state routing the nodes can have a hierarchical structure.

Evaluation Scheme for Q8:

a. Explanation of ICMP protocol with message format. 4 marks

b. Defining congestion control, explaining the Slow start phase, congestion avoidance phage and congestion detection phase. 4 Marks

c. Explanation of checksum techniques with example calculation. 4Marks