19-20

8(a)

(a) Describe the sift cipher and Transposition ~~chi~~ ciphers with example. [4]

Shift Cipher:

A shift cipher (Additive cipher or caesar cipher) is a substitution cipher where each letter in the plaintext is moved forward by a fixed number in the alphabet. Encryption is performed using the

Formula:- $c = (p+k) \bmod 26$

c = ciphertext letter

p = plaintext letter (0-25)

k = shift value

Example: Encrypting "HELLO" with k=3:

H→K, E→H, L→O, L→O, O→R

Result: KHOOR

The letters change, but their positions stay the same.

Transposition cipher :-

A Transposition cipher does not change the letter ; it only changes their order by using a pattern or rule.

Example: plaintext "NETWORK", using a transposition key (say, reversing every two letters).

original : NE TW OR K

transposed: EN WT RO K

Result: ENWTROK

It keeps the same letters but hides the message by rearranging them.

19-20

8(b)

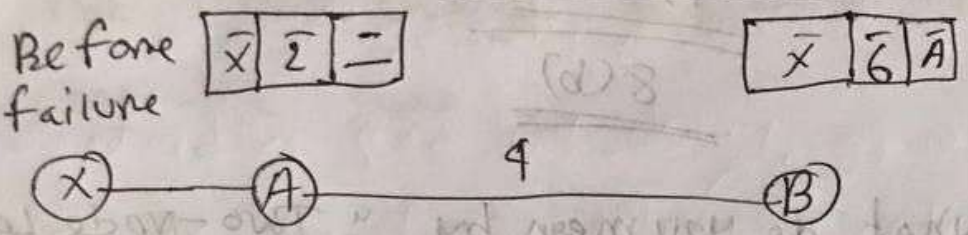
(b) what do you mean by "Two-Node Loop Instability" problem with distance vector routing? Explain with necessary diagram. Also, provide a solution to the problem. [4]

The Two-Node Loop Instability happens in distance vector routing when two routers keep sending wrong distance information to each other after a link fails.

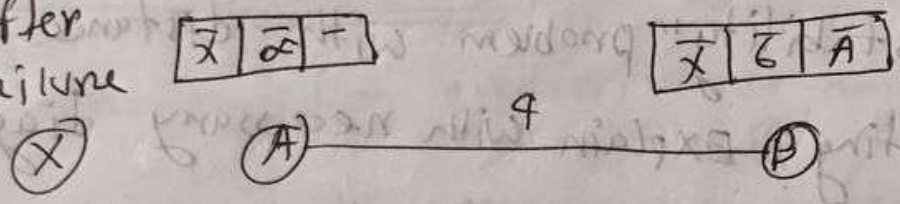
Both routers (A and B) think the other has a valid route to network X, so they keep increasing the hop count again and again. This creates a loop and causes the count-to-infinity problem.

Two-node Instability

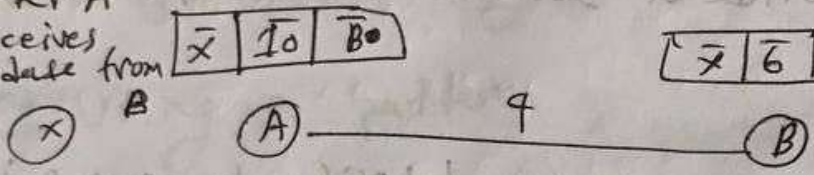
Before failure



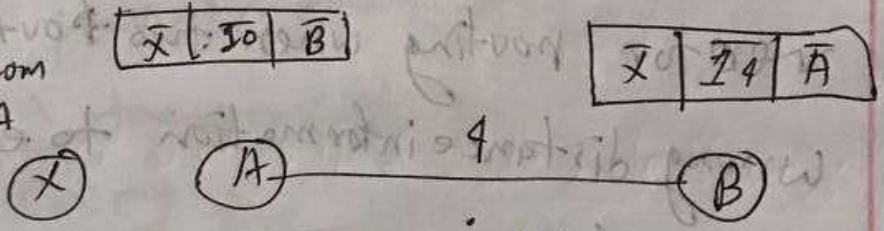
After failure



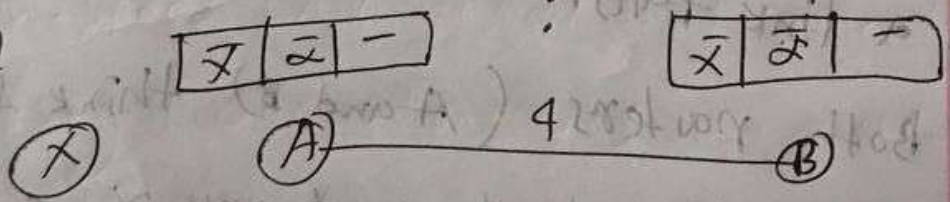
After A receives update from B



After B receives update from A



Finally



Soution: The solution is poisoned Reverse.

A router tells its neighbor that the distance to a network is infinity if it uses that neighbor to reach the network. This stops the loop and prevents wrong updates.

19-20

8(c)

(c) i) packet switching
ii) circuit switching
iii) HTTP
iv) FDDI [4]

short notes on :

i) Packet switching: packet switching is a method of data communication where information is broken into small packets, each sent independently through the network. It uses a store-and-forward mechanism and allows efficient use of bandwidth.

ii) circuit switching: circuit switching is a communication method where a dedicated path is established between sender and receiver for

the entire session. It provide guaranteed bandwidth and low delay. It is commonly used in traditional telephone networks.

iii) HTTP (Hypertext transfer protocol): HTTP is an application layer protocol that clients (like browsers) to request resources from servers on the web. It is stateless and uses TCP, while HTTPS ensures secure, encrypted communication.

iv) FDDI (Fiber Distributed Data Interface): FDDI is a high-speed LAN protocol that connects devices using fiber optic cables in a dual-ring topology. It uses token passing for access and provides high reliability and fault tolerance, mainly used in backbone networks.

20-21

1 (a)

(a) Define ICMP and explain how it is used in error reporting and diagnostics? [5]

ICMP (Internet control message protocol):

ICMP is a network-layer protocol used by devices to send error message and operational information, supporting IP communication.

Uses:

Error Reporting: ICMP notifies the sender of delivery issues. common messages:

- Destination Unreachable: target cannot be reached.
- Time Exceeded: TTL expired before reaching destination.
- Redirect: Suggests a better route.
- Parameter problem: Invalid IP header field detected.

Network Diagnostics: supports tools like:

- Ping: sends Echo ~~Req~~ Request/Reply to check connectivity and round-trip time.
- Traceroute: maps packet path using time Exceeded messages to identify delays or routing issues.

Extra

ICMP and Network performance: ICMP helps in error reporting and diagnostics but can hurt networks if abused:-

- Flood: overloads CPU/bandwidth with many Echo Requests.
- Smurf: the Attack spoofed requests flood victim with replies.
- Ping of Death: oversized packets can crash systems (historical)

ICPM ⇒ 3 uses

i) Error Reporting
ii) Diagnostics
iii) Hurt Network Performance

20-21

1(b)

(b) what is the difference between IPV6 link-local and unique-local address? provide examples: [4]

Feature	IPV6 Link-Local Address	IPV6 unique-Local Address
(i) scope	single link (local Network)	with organization or site
ii) prefix	FE80::/10	FC00::/7 (usually FD00::/8)
iii) purpose	Local communication; required for routing	private internal use; not for internet.
iv) Routable	No routable beyond link	Not routable on the global internet

v) Assignment	Automatically assigned to interface	Manually or internally planned
vi) Lifetime	Exists as long as interface is active	Exists as long as assigned internally
vii) Required for protocols	Yes, e.g., Neighbor Discovery routing	optional for internal communication
viii) Example	FE80::1	FD12:3456:789A::1

2020-21

1(c)

(c) Define Bandwidth, Ping, Jitter

Bandwidth: Bandwidth is the maximum data transfer rate of a network or channel. It determines how much data can be sent in a given time.

Ping : Ping is a network tool that tests connectivity and measures round-trip time. It uses ICMP Echo Request and Reply messages.

Jitter: Jitter is the variation in packet arrival times. It affects the quality of real-time communications like VoIP or video calls.

18-19

1 (a)

(a) Determine one or more layers of the OSI model to perform the following task: [5]

i) Format and code conversion services

ii) Establishes, manages, and terminates sessi

iii) Ensures reliable transmission of data

iv) Log-in and log-out procedures

v) provides independence from differences in data representation.

Ans: i) presentation Layer (Layer 6)

ii) Session Layer (Layer 5)

iii) Transport Layer (Layer 4) and Data Link Layer (Layer 2)

iv) session Layer (Layer 5) and Application Layer (Layer 7)

v) presentation Layer (Layer 6)

18-19

1(b)

(b) what is port address?

A port address is a numerical identifier used at the transport layer (TCP/UDP) to distinguish different applications or services on a hos

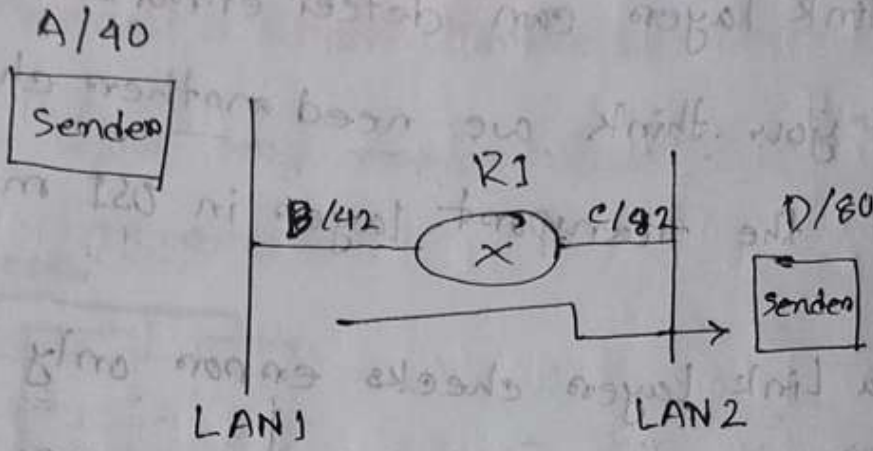
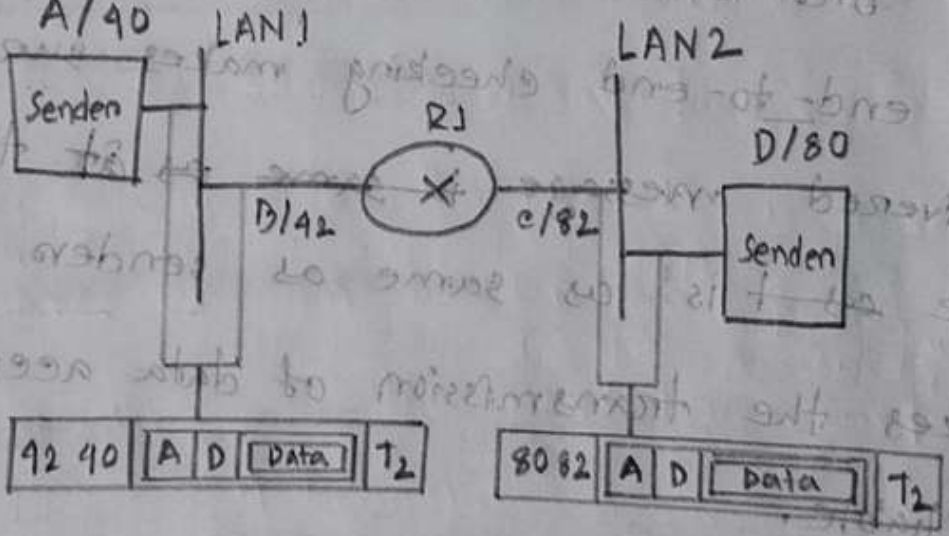


Fig: 1

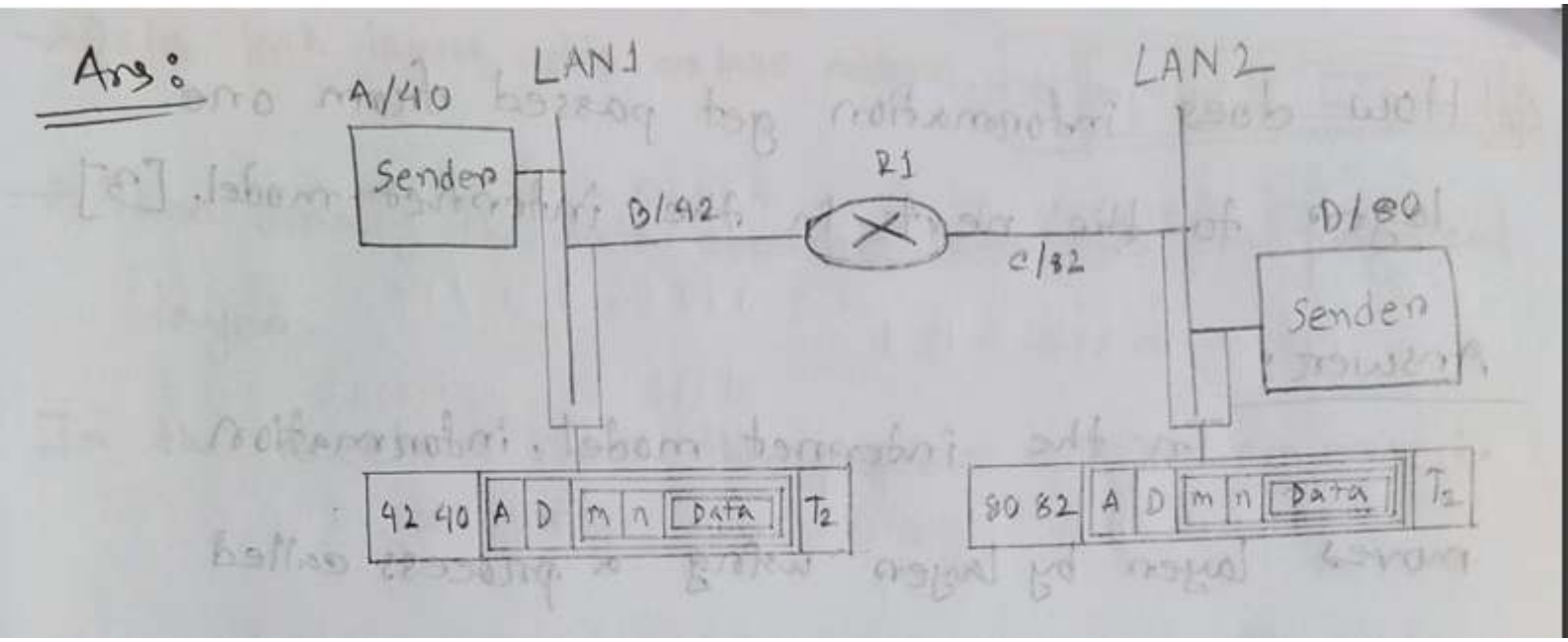
In Fig: 1 Computer A sends a message to computer D via L Router R1 and LAN2. Show the contents of the packet and frames at the network and data link layer for each hop interface.

Ans:



In fig: 1 assume that the communication is betw a process running at computer A with port address m at computer D with port address n. Show the content of packeets and frames at the network, data link an transport layer for each hop.

Ans:



If the data link layer can detect errors between hops, why do you think we need another checking mechanism at the transport layer in OSI model? [3]

Ans: The Data Link layer checks error only between two directly connected nodes, but errors may still happen on later hops.

To solve this Transport layer adds an another level of checking where ~~data~~ verifying the data from sender ~~and~~ to the final receiver.

This end-to-end checking makes sure the delivered message ~~is same as~~ at the receiver side ~~as t~~ is as same as sender side. This makes the transmission of data accurate and reliable.

(d) What are the responsibilities of the network and transport layer in the Internet model. [4]

Ans:

The Network layer and the Transport layer both are the layers of OSI model. They have some specific responsibilities. Such as,

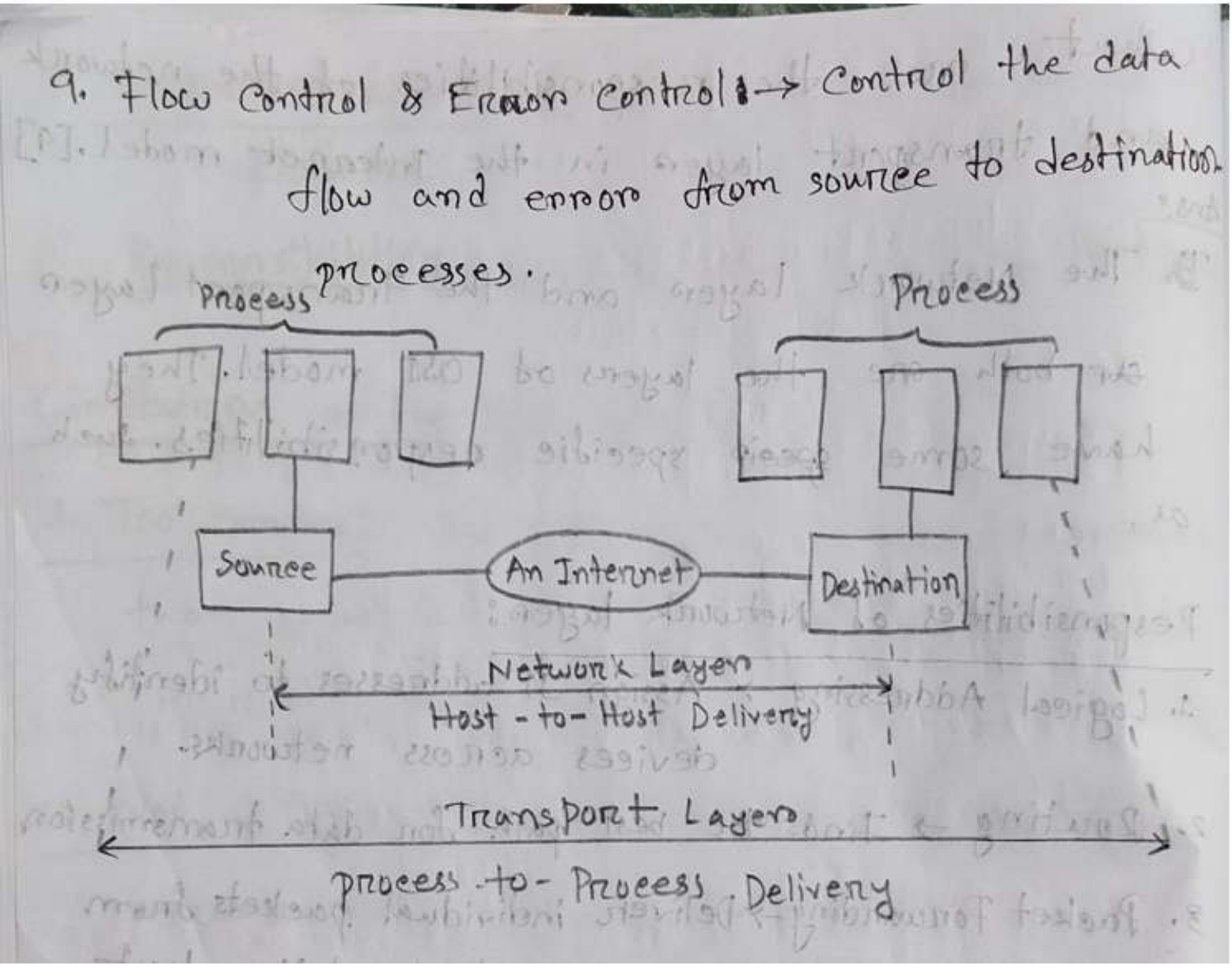
Responsibilities of Network layer:

1. Logical Addressing → Assign IP addresses to identify devices across networks.
2. Routing → Finds the best path for data transmission.
3. Packet Forwarding → Deliver individual packets from source host to destination host.

Responsibilities of Transport layer:

1. Port Addressing → Uses port number to deliver data.
2. Segmentation and Reassembly → Breaks data into segments at sender side and reassembly at receive side
3. Message Forwarding → Delivers a message from process to process.

9. Flow Control & Error Control :→ Control the data flow and error from source to destination processes.



18-19

2 (b)

(b) Explain the advantages of IPV6 when comapred to IPV4. In which transition strategy do we need to encapsulate IPV6 packets in the IPV4 packets? [4]

Advantages of IPV6 over IPV4:

i) Larger address space:- 128-bit address allow more unique devices then IPV4's 32-bit space.

ii) simplified header:- Reduces processing overhead and improves network performance.

iii) Better support for quality of service (QOS):- Flow label field helps prioritize high-priority packets.

N) Improved Security:- Built-in IPSec support ensures encryption, authentication and integrity.

Transition strategy:-

- tunneling: When IPV6 packets need to pass through and IPV4-only network, they are encapsulated inside IPV4 packets. The protocol value is set to 41 to indicate the payload is an IPV6 packet. This allows IPV6 communication across IPV4 networks.

19-20

2(a)

(a) In the Go-Back-N protocol, the size of the send window can be $2^m - 1$, while the size of the receive window

is only 1. How can flow control be accomplished when there is a big difference between the size of the send and receive window? Briefly Explain? [5]

Go-Back-N protocol Flow control :-

i) Sender window size; $2^m - 1$ frames, sender can send multiple frames without waiting for Ack.

ii) Receiver ~~control mechan~~; window size: 1 frame; receiver accepts only the next expected frame in order.

Why this work :-

- sender is limited by its window, so proper flow control is maintained.

• Receiver accepts only one frame, but the large sender window keeps the pipeline efficient.

• Lost or erroneous frames cause all later frames to be retransmitted, ensuring reliability.

conclusion: Small receiver window gives simplicity; large sender window increases throughput.

19-20

2 (b)

(b) what is socket address? compare between TCP and UDP protocols? [9]

A socket address is a combination of an IP address and a port number that uniquely identifies a process on a host in a network.

Socket Address = IP Address + port Number

Comparison between TCP and UDP:

Feature	TCP	UDP
i) connection type	connection-oriented	connectionless
ii) Reliability	Reliable (Ack + retransmission)	Not reliable (best + effort)
iii) order	ordered delivery	No order guarantee
iv) Flow and congestion control	Yes (windowing, slow start)	No control
v) overhead	Higher	lower
vi) use cases	HTTP, FTP, Email	DNS, streaming, VoIP

TCP is suited for applications that require reliability, while UDP is used where speed and low overhead are prioritized over guaranteed delivery.