DNSH SIRR1
224089

Computer Networks
Paper - 1

A-1 a/(i) Route Determination
This function involves deciding the path that data packets should take from the source to the destination. The layer respon for the route is network layer [3] of OSI model. It finds the most efficient ro

(ii) Error Detection & Correction
Error Detection & correction involves identifying errors that occur during data transmisson, main data integrity & Accuracy. Layer Responsible is Data Link layer

(iii) Interface to Outside world
This function provides means for communicatio between the networks & devices external to the network. layer responsible is physical layer

(iv) Services as E-mail & Mail transfer.
This function involves providing higher-level services & application to network use The layer responsible is Application layer

(b) → DF (Don't Fragment) :- The DF bit in the IPv4 header indicates weather the packet should not be fragmented during transmission. If the DF bit is set to 1, it means that the packet should not be fragmented. If it encounters a router with an MTU smaller than the packet size, it will be discarded and an ICMP error message will be sent back to the source.

→ MF (More Fragments) :- The MF bit is used to indicate whether there are more fragments following the current fragment in the packet. If the MF bit set to 1, it means there are more fragments to come. If it is set to 0, it signifies that current fragment is the last one.

(c) (i) FTP → It operates at the Application Layer of the TCP/IP protocol stack, providing file transfer services.

(ii) ICMP → It functions primarily at the Network layer of the TCP/IP protocol stack, handling network management & error reporting functionalities.

(iii) DNS → It operates at the Application Layer of the TCP/IP protocol stack, resolving domain names to IP addresses.

(c) UDP → It operates at the Transport Layer of the TCP/IP protocol stack, providing a connection less & unreliable transport service

(d) Selective Repeat Advantages

(1) Efficiency → Selective Repeat retransmits only the lost or damaged packets, allowing for more efficient use of network resources

(2) Bandwidth Utilization → It minimizes the need for retransmissions, reducing the impact on network bandwidth & improving overall throughput.

(3) Flexibility → Selective Repeat allows the receiver to acknowledge packets individually, enabling the sender to resend only the necessary packets, leading to faster recovery from errors.

Go-Back-N Limitations

1) Higher Overhead → Go-Back-N requires the sender to retransmit all unacknowledged packets from the last correctly received packet, leading to higher overhead, especially in cases of multiple lost packets.

2) Lower Bandwidth utilization → It may result in unnecessary retransmission of packets that are already received correctly at the receiver, leading to lower bandwidth utilization.

(e) Maximum Bit Rate = $2 \times \text{Bandwidth} \times \log_2(1+S/N)$

$= 2 \times 1600 \times \log_2(1+20)$

$= 3200 \times \log_2(21)$

$= 3200 \times 4.392$

$= 14,054.4$ bits per sec

(f) Band Rate = $\frac{\text{Bit Rate}}{\text{No. of Symbols}}$

$= \frac{4800 \text{ bps}}{8}$

$= 600$ band

(g) The frame format of PPP typically consits of following fields:

1) Flag → A 1-byte field used to mark the beginning & End of frame.
2) Address → A 1-byte field, usually set to 11111111 in the case of broadcast.
3) Control → A 1-byte field used to indicate control info.
4) Protocol → A 2-byte field indicating the protocol type of encapsulated data
5) Data → Variable-length field containing the payload data
6) Padding → optional field used for byte alignment
7) Frame Check sequnce → A 2 or 4 byte field used for error detection

8) Flag → A-1 byte field marking the end of the frame.

These fields are arranged in the PPP format, allowing for the encapsulation of data packets for transmission over a point-to-point link.

(b) 1100110111111

C(1,3,5,7,9,11) → 1011011 (no error) = 0
Even 1's

C2(2,3,6,7,10,11) = 1010111 = Even 1's (no error)
= 0

C4(4,5,6,7) = 0110 = Even 1's (no error)
= 0

C1C2C4 = 000 = no error

original code set = 1100110111111

Q (i) Peer-to-Peer Connection → A P2P connection enables direct communication & resource sharing b/w devices without a centralized server, P2P networks allow each device to function as both client & server, facilitating decentralized data exchange. This architecture boosts scalability, fault tolerance, ensuring uninterrupted operation even if some nodes fail. P2P connections are widely used in file sharing, decentralized apps, & communication platforms.

(ii) Remote Procedure Call (RPC) → Remote Procedure call is a protocol for executing functions or procedures on remote system as if they were local. It simplifies network communication complexities, enabling seamless interaction in distributed applications. RPC facilitates interprocess communication across various devices & platforms, promoting efficient distributed computing. Popular implementations, including XML-RPC, SON-RPC, & gRFC, each with specific encoding formats & Transport protocols

Q2 ① Flow Control

→ Flow Control regulates the rate of data transmission b/w sender & receiver within a network to ensure that the sender doesn't overwhelm the receiver.

→ It primarily manages data rates at the receiver's end to avoid data loss or overflow

→ Eg: TCP's sliding window protocol is a form of flow control

② Congestion Control

→ Congestion Control manages the data traffic within the network to prevent network nodes from becoming overloaded.

→ It aims to ensure fair access to network resources for all users it prevent networks collapse due to excessive traffic

Eg → TCP's congestion avoidance mechanisms to adjust the transmission rate based on network conditions.

Reason of Occurrence of Congestion

Congestion occurs in a network when the volume of data packets being transmitted exceeds the capacity of network infrastructure to handle efficiently.

→ High demand for network resources

→ Limited Bandwidth

→ Network equipment failure or inefficiency

→ Lacking of congestion control, leading to unchecked data flow

(6) A Cyclic - Redundancy Check (CRC) is widely used for error-detecting code in digital networks. It verifies data integrity during transmission by generating checksum based on transmitted data.

⊙ Error Detection:- CRC helps identify error caused by noise, interfere, or data corruption during transmission

⊙ Reliability :- It enhances the reliability of data transmission by providing simple yet efficient method.

⊙ Efficiency :- CRC is computationally efficient, making it suitable for real time error detection.

⊙ Widespread Adoption :- CRC is widely used in various networking protocols.

Q3 a) In Ethernet networks, the Binary Exponential Backoff algorithm is used to handle collisions, when a collision occurs during data transmission. the involved nodes wait for a random amount of time before attempting to retransmit.

Reducing Collision Probability
It helps to reduce the prob of collisions by introducing randomness into the retransmission process. By waiting for a random period, the likelyhood of collisions decreases as nodes are less likely to transmit simultaneously

① In IPv4 datagram consists of 2 main Parts: The Header & the data payload. The header contains essential info for routing & delivery of the packet while the data payload carries actual user data.

i) Header → The header is 20 bytes long & contains various fields, including:

→ Version: Indicates the IP version (IPv4 or IPv6)
→ Header length: 32-bit words
→ Type of Service: Describes the quality of service required
→ Total length: Indicates Total length of datagram
→ Identification: Unique identifier for fragmented packets
→ Flags: Control Fragmentation Behaviour
→ Fragment offset: Position of fragment within the original datagram
→ Time to Live (TTL): Limits the lifespan of packet
→ Protocol: Specifies the protocol used in data payload
→ Header checksum: Ensure integrity of the header

② Data Payload → The Data Payload carries the actual user data, such as application data encapsulated within the IP Packet. Its length varies based on the size of the packet and the data being transmitted

Q4 (a) Distance vector routing is a type of algorithm used in CN to determine the best path for forwarding packets. Each router in the network maintains a table that contains info.

Steps :-

1) Initialization → Each router initializes its distance vector table with info about directly connected neigh
2) Exchang of Info → Routers exchange their dis vector tables with neighbouring routers.
3) Update → Based on received info, routers update their dis. vector tables.
4) Converged → The process continues until no further updates are made, indicating that the routing tables have converged.

→ Count to infinity Problem →

The count to infinity problem in dist. vector routing arises when routers disseminate inaccurate data about unreachable destinations, causing the cost to reach those destinations to increment until it hits infinity.

Q) The Transmission Control Protocol (TCO) connection establishment and release follows a standardized procedure.

Connection Establishment (Three-way handshake)

1) client sends a SYN Packet to the server
2) Server responds with SYN-ACK packet
3) Client acknowledges with an ACK packet to complete the connection

Data Transfer

→ After the connection establishment, data can be exchanged b/w the client & Server using TCP segments.

Connection Release (Four-way handshake)

1) Sender sends a FIN packet to initiate closure
2) Receiver acknowledges with an ACK packet.
3) Receiver sends its own FIN packet to close its side
4) Sender acknowledges the receivers FIN packet to complete closure

Q5 (a) Data Communication refers to the process of transferring data b/w 2 or more devices through a medium, such as cables, wires or wireless signals.

1) Delivery → Ensuring that data reaches the intended destination accurately & reliably.
2) Accuracy → Transmitting data without errors or loss maintaining its integrity
3) Timeliness → Delivering data within an acceptable timeframe, ensuring real time or timely connection
4) Jitter → Minimizing variations in the arrival time of data packet to maintain consistency & smooth communication flow

(6) (i) Unicasting → The data is transmitted from a single sender to a single recipient. It involves a one-to-one communication method, where sender addresses the data to specific recipient

(ii) Broadcasting - It is a communication mechanism where data is sent from one sender to all nodes or recipients in a network. It utilizes one to all communication

(iii) Multicasting :- It involves sending data from one sender to multiple specific recipients. It is a one-to-many communication method

Q6 (i) We borrow 3 bits from the host to create 119 subnets

With 3 borrow bits $2^3 = 8$

(1) 134.122.0.0119
(2) 134.122.32.0119
(3) 134.722.64.0119
(4) 134.122.96.0119
(5) 134.122.128.0119
(6) 134.122.160.0119
(7) 134.122.192.0119
(8) 134.122.224.0119

(ii) No of hosts per network $= 2^n - 2$

$= 2^3 - 2$

$= 32 - 2 = 30$ hosts

No. of host bits $- n = h$

$8 - 3 = 2$

$n = 2$

(iii) ~~Data diods stages~~ The IP address 134.122.67.124 belongs to 134.122.66.0 to 134.122.95.255 since 134.122.67.124 belongs within this range

it belongs to network 134.122.66.0/19