Computer Networks

Assignment (Paper-1)

Q1 (a) (i) Route Determination is performed by Network Layer:- This Layer is responsible for routing packets across diff. networks, determining the optimal path for data transmission.

(ii) Error Detection & Correction is primarily handled by Transport layer. This Layer ensures the reliable delivery of data by implementing error-checking mechanisms & retransmitting data if errors occurs during transmission.

(iii) Interface to outside world is managed by the Physical Layer. This layer deals with the physical transmission of data over the network medium, including connection establishment, maintenance, & termination.

(iv) Services such as email and file transfer are facilitated by the Application layer. This layer provides network services directly to end-users & applications, including email protocols (e.g., SMTP) & file transfer protocols (e.g., FTP).

(b) → DF (Don't Fragment) :- The DF bit in the IPv4 header indicates whether the packet should not be fragmented during transmission. If the DF bit is set to 1, it means that the packet ~~is~~ should not be fragmented, & if it encounters a router ~~or~~ with an MTU smaller than the packet size, it will be

discarded, & 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 is set to 1, it means there are more fragments to come. If it is set to 0, it signifies that the 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.

(iv) UDP → It operates at the Transport Layer of the TCP/IP protocol stack, providing a connectionless & unreliable transport service.

8.

(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~~ 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 retransmissions of packets that are already received correctly at the receiver, leading to lower bandwidth utilization.

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

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

$= 3200 \times \log_2(21)$

$= 3200 \times 4.392$

$\approx$ **14,054.4 bits per sec**

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

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

Baud Rate = 600 baud

(g) The frame format of PPP typically consists of the 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 the encapsulated data.
5. Data → Variable-length field containing the payload

data.

(6) Padding → Optional field used for byte alignment

(7) Frame check Sequence → 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.

(9) 11001101111

$C_1(1,3,5,7,9,11)$ 101011

~~$C_1(1,2,3,4)$ = 1010 = Even 1's (no error) = 0~~

~~$C_2(2,3,6,7)$ = 1010 = Even 1's (no error)~~

$C_2(2,3,6,7,10,11)$ = 101011 = Even 1's (no error) = 0

$C_4(4,5,6,7)$ = 0110 = Even 1's (no error) = 0

$C_1C_2C_4$ = 000 = no error

∴ Original code sent = 11001101111

(i) The Components of a URL (uniform Resource Locator) are:-

① Scheme or Protocol :- It specifies how the resource is accessed. Common schemes include HTTP, HTTPS, FTP & ftc.

② Domain :- It identifies the location of the resource on the internet. It can include subdomains, such as "www" or "blog", followed by the main domain name.

③ Top-Level Domain :- It indicates the type or purpose of the website, such as .com, .org, .net, .edu, or country-specific codes like .uk, .in, etc.

④ Port no. :- It specifies the communication endpoint on the server. Most web traffic uses default ports (HTTP: 80, HTTPS: 443), but other services may use diff. ports.

⑤ Path :- It identifies the specific resource or page on the server. It comes after the domain & may include directories & folders.

⑥ Query String :- It provides additional parameters or data to be sent to the server, typically in key-value pairs separated by "&".

⑦ Fragment or Anchor :- It specifies a specific section within a webpage where the browser should scroll to.

(K) (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 func^n as both the client & server, facilitating decentralized data exchange. This architecture boosts scalability, fault tolerance, & resilience, 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 systems as if they were local. It simplifies network communication complexities, enabling seamless interaction in distributed applications. RPC facilitates inter-process communication across various devices & platforms, promoting efficient distributed computing. Popular implementations include XML-RPC, JSON-RPC, & gRPC, each with specific encoding formats & transport protocols.

(2) (a) (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 data traffic within the network to prevent network nodes from becoming overloaded.

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

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

Reason for Occurrence of Congestion in a Network:-

Congestion occurs in a network when the volume of data packets being transmitted exceeds the capacity of the network infrastructure to handle them efficiently. This can happen due to various reasons such as:

→ High demand for network resources.
→ Limited bandwidth
→ Network equipment failure or inefficiency
→ Routing issues leading to suboptimal paths.
→ Bursty traffic patterns or sudden spikes in data transmission.
→ Lack of congestion control mechanisms, leading to unchecked data flow.

(b) A Cyclic - Redundancy Check (CRC) is a widely-used error-detecting code in digital networks. It verifies data integrity during transmission by generating a ~~check~~ checksum based on the transmitted data. This checksum is appended to the data packet. Upon receipt, the receiving device recalculates the CRC value & compares it with the received checksum. A match indicates likely intact data, while a mismatch suggests errors during transmission.

Uses & Benefits in Networks :-

(i) Error Detection :- CRC helps identify errors caused by noise, interference, or data corruption during transmission.

(ii) Reliability :- It enhances the reliability of data transmission by providing a simple yet effective method for error detection.

(iii) Efficiency :- CRC is computationally efficient, making it suitable for real-time error detection in high-speed networks.

(iv) Widespread Adoption :- CRC is widely used in various networking protocols & technologies, including Ethernet, Wi-Fi, Bluetooth, & others, ensuring interoperability & compatibility.

__/__/__

(3) (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. The waiting time is determined using a binary exponential backoff strategy, where the waiting time doubles with each collision.

→ **Reducing Collision Probability:-** This algorithm helps reduce the probability of collisions by introducing randomness into the retransmission process. By waiting for a random period, the likelihood of collisions decreases as nodes are less likely to retransmit simultaneously. Additionally, the exponential increase in waiting time ensures that collisions are resolved more efficiently as the network becomes less congested over time. As a result, the Binary Exponential Backoff algorithm contributes to the overall Efficiency & reliability of Ethernet Networks.

(b) An 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 the actual user data. Here's a breakdown of the IPv4 datagram format:-

(1) ~~Header~~ **Header** → The header is 20 bytes long & contains various fields, including:

→ **Version**: Indicates the IP version (IPv4 or IPv6)

→ **Header Length** :- Specifies the length of the header in 32-bit words.

→ **Type of Service (ToS)** :- Describes the quality of service requested.

→ ~~Total~~ **Total Length** :- Indicates the total length of the 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 the packet.

→ **Protocol** :- Specifies the protocol used in the data payload (e.g., TCP, UDP).

→ **Header** ~~Checksum~~ :- Ensures integrity of the header.

→ **Source & Destination IP addresses** :- Identifies the sender & recipient.

→ **Options** :- Additional Info. or control data (optional).

(2) **Data Payload** → ~~The~~ 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.

(4) (a) Distance vector routing is a type of algorithm used in Computer Networks to determine the best path for forwarding packets. Each router in the network maintains a table that contains info. about the distance (cost) to reach each destination & the next-hop router to reach that destination. This table is periodically updated based on info. received from neighboring routers.

→ Steps:-

1) Initialization → Each router initializes its distance vector table with information about directly connected neighbours.

2) Exchange of Info. → Routers exchange their dist. vector tables with neighbouring routers.

3) Update → Based on received info, routers update their dist. vector tables.

4) Convergence → 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.

This can lead to erroneous routing decisions & network instability. Mitigation strategies like route poisoning & split horizon prevent routers from propagating unreachable routes or advertise them with infinite cost, addressing this issue.

(b) The Transmission Control Protocol (TCP) connection establishment and release follow 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 receiver's **FIN** packet to complete closure.

5 (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. It involves the exchange of digital info, instructions, or messages.

The effectiveness of a data communication systems depends on the following characteristics.

① Delivery → Ensuring that data reaches the intended destination accurately & reliability.

② Accuracy → Transmitting data without errors or loss, maintaining its integrity during transmission.

③ Timeliness → Delivering data within an acceptable timeframe, ensuring real-time or timely communication.

④ Jitter → Minimizing variations in the arrival time of data packets to maintain consistency and smooth communication flow.

(b) (i) Unicasting → The data is transmitted from a single sender to a single recipient. It involves a one-to-one communication method, where the sender addresses the data to a 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 a one-to-all communication method, transmitting data to all devices within the network.

(iii) Multicasting → Multicasting involves sending data from one sender to multiple specific recipients. It is a one-to-many communication method, where the sender addresses the data a selected group of recipients who have expressed interest in receiving it.

(c) The World Wide Web (WWW), or simply the web, is a global info. system enabling content sharing over the internet through user-friendly interfaces. It consists of interconnected websites & web pages hosted on servers, invented by Tim Berners-Lee in 1980. Users navigate b/w web pages via hyperlinks, impacting modern life by facilitating communication, collaboration, & access to resources.

(6) (i) We borrow 3 bits from the host to create /19 subnets.

With 3 borrowed bits, we have $2^3 = 8$ subnets.

1. 134.122.0.0/19
2. 134.122.32.0/19
3. 134.122.64.0/19
4. 134.122.96.0/19
5. 134.122.128.0/19
6. 134.122.160.0/19
7. 134.122.192.0/19
8. 134.122.224.0/19

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

$= 2^3 - 2$

$= 32 - 2 =$ **30 hosts**

No. of host bits - $n = h$

$8 - 3 = 2$

$\boxed{h = 2}$

(iii) The IP address 134.122.67.124 belongs to 134.122.64.0 to 134.122.95.255. Since 134.122.67.124 belongs within this range,

∴ It belongs to the network **134.122.64.0/19**

(b) Data Link layer :-

(1) Link Establishment & Termination :- It establishes, maintains, & terminates connections b/w nodes on a network, ensuring reliable data transfer within the same network segment.

(2) Framing :- It divides data into frames for transmission, enabling error detection & correction.

(3) Error Detection & Correction :- Utilizes techniques like checksums to detect & correct errors that

occur during data transmission.

Transport Layer :-

(1) End-to-End Communication :- Provides communication services b/w 2 processes running on diff. hosts, ensuring data delivery with reliability & integrity.

(2) Segmentation & Reassembly :- Breaks data into smaller segments for efficient transmission & reassembles them at the receiver end.

(3) Flow Control & Error Recovery :- Manages the flow of data b/w hosts & implements mechanisms for error detection, retransmission & recovery.