Computer Networks

Assignment (Paper-2)

(1) (a) Number of bits req. = $\frac{\text{Bandwidth} \times \text{Round trip time}}{\text{Frame\_Size}} \times U$

Number of bits req. = $\frac{1.5 \times 10^6 \times 0.05}{8 \times 10^3} \times 0.6$

$N \approx = \frac{1500 \times 5}{8 \times 100} \times \frac{6}{10^2}$

$= \frac{45}{8} = \boxed{5.625}$

5 bits are req.

(b) One significant diff. b/w port address, physical address, & logical address is their respective purposes & scopes.

→ Port Address: Identifies specific communication endpoints in a network & facilitates communication b/w processes at the transport layer. It distinguishes b/w different network services or applications.

→ Physical Address: Represents the hardware address assigned to network interfaces & operates at the data link layer. It is used for communication within a local network (LAN) & is unique to each network

interface card (NIC).

→ Logical Address: Refers to virtual addresses assigned to devices by network protocols, such as IP addresses. It operates at the network layer & is used for routing packets across networks.

(c) To transmit the character frame using byte stuff framing method, we insert an ESC byte before any FLAG or ESC occurences in the frame. The bit sequence transmitted in binary would be:

~~So, +~~

So the bit sequnce ~~transmitted~~ transmitted would be:

11010111 11101101 10100011 11011101
10100011 10100011 01111110.

(d) (i) 127.0.0.0 → This address range, specifically 127.0.0.1, is reserved for loopback purposes. When a device sends data to 127.0.0.1, it's looped back to the same device. It's commonly used for testing network interfaces & services locally without sending data over a physical network.

(ii) 255.255.255.255 → This address represents the broadcast address for IPv4 networks. When a packet is sent to this address, it is received by all devices on the

network segment. It's commonly used for broadcasting messages or requests to all devices within a local network.

(e) Circuit Switching → In Circuit Switching, a dedicated communication path is established before data transmission begins. Imagine a traditional telephone call where a physical circuit is established b/w the caller and receiver for the duration of the call. Until the call ends, this circuit remains exclusively reserved for the communication.

Packet Switching → Packet switching, on the other hand, divides data into packets & sends them independently through the network. Each packet is routed independently based on the network conditions. Think of sending an email where each packet travels independently across various routers & switches to reach the recipient, & packets may take diff. paths.

(f) To resolve an IP address from a given URL, the Domain Name System (DNS) is used:

① DNS Query:- When a user enters a URL into a web browser, the browser sends a DNS query to a DNS resolver.

② DNS Resolution:- The DNS resolver checks its cache for the corresponding IP address. If not found, it sends requests to multiple DNS servers hierarchically until it finds the authoritative DNS server for the domain.

(3) Authoritative DNS Server:- The authoritative DNS server holds the mapping of the URL to its IP address. It responds with the IP address to the resolver.

(4) Response to User:- The resolver returns the IP address to the user's device, allowing it to establish a connection with the desired server.

This process enables users to access websites using human-readable domain names while the underlying internet infrastructure communicates using IP addresses.

(9) Total Bandwidth of channels = $5 \times 100KHz$
$= \boxed{500KHz}$

Bandwidth of Guard Band = $10KHz$

Total Bandwidth Req. = $500KHz + 10KHz$
$= \boxed{510KHz}$

(10) (i) Number of bits per baud (r) = $\frac{N}{\log_2(M)}$

N = bit rate = 72 Kbps
M = Total no. of symbols = $4 \times 16 = 64$

$r = \frac{72 \text{ Kbps}}{\log_2(64)} = \frac{72 \text{ Kbps}}{12 \text{ Kbps}} = \boxed{6 \text{ baud}}$

$= \frac{72\text{Kbps}}{6} = \boxed{12\text{ Kbps}}$

(ii) Baud Rate (S) $= \frac{N}{r}$

$= \frac{72\text{ Kbps}}{12\text{ Kbps}} = \boxed{6\text{ baud}}$

(i) (i) True
(ii) False

(j) The twisting in twisted-pair cables provides several benefits:-

1. Reduced Electromagnetic Interference (EMI)
2. Improved Signal Strength
3. Noise Immunity
4. Compact Design

(K) 1. PSH (Push) Flag → It instructs the receiving host to deliver the data immediately to the application without buffering.

2. SYN (Synchronize) Flag → It initiates a connection establishment process b/w 2 hosts by synchronizing the Sequence nos.

(l) Well-known ports are reserved port nos. assigned by the Internet Corporation for Assigned Names & Nos. (ICANN) for specific services. These ports are standardized across systems, as they serve as entry points for common network services.

(1) HTTP (Hypertext Transfer Protocol) →
Port 80 is the well-known port assigned to HTTP.

(2) SMTP (Simple Mail Transfer Protocol) →
Port 25 is the well-known port assigned to SMTP.

(m) Ports needed per device in mesh topology
$= n-1$
$= 6-1 =$ **5 ports**

Total no. of links req. $= \frac{n(n-1)}{2}$

$= \frac{6(6-1)}{2} = \frac{6 \times 5}{2} =$ **15 links**

(n) (o) (1) Route determination → This corresponds to the **Network Layer** of the OSI model

(2) Interface to transmission media → This aligns with the **Physical Layer** of the OSI model.

(3) Provides Access to the end user → This relates to the **Application Layer** of the OSI model.

(2) (i) (a) 01010
: 10101
11111 → (5) 1's

Hamming Dist. = 5

(b) 2 bit errors can be detected by this code.

(c) 1 bit error can be corrected by this code.

(ii) Received Code → 111 00100 1111

C_1 = (1, 3, 5, 7, 9, 11)

= 1 1 0 0 1 1 = even 1's = 0

C_2 = (2, 3, 6, 7, 10, 11)

= 1 1 1 0 1 1 = odd 1's = 1

C_4 = (4, 5, 6, 7, 12)

= 0 0 1 0 1 = even 1's = 0

C_8 = (8, 9, 10, 11, 12)

= 0 1 1 1 1 = even 1's = 0

Code = 0 1 0 0 = 4

Corrected code = 1111 0100 1111

(iii) It consists of 12 basic fields :-

(1) Version (4 bits) → Indicates the IP protocol version being used, typically IPV4.

(2) Header length (4 bits) → Specifies the length of the header in 32 bit.

(3) TOS (8 bits) → Determines the priority & handling for the packet.

(4) Total Length (16 bits) → Indicates the total length of the packet, + header + data

(5) Identification (16 bits) → Helps in fragmenting & reassembling packets.

(6) Flag (3 bits) → Used for fragmentation control, including flags for fragmentation & reassembly.

(7) Fragment offset (13 bits) → Specifies the position of the fragment in the original packet.

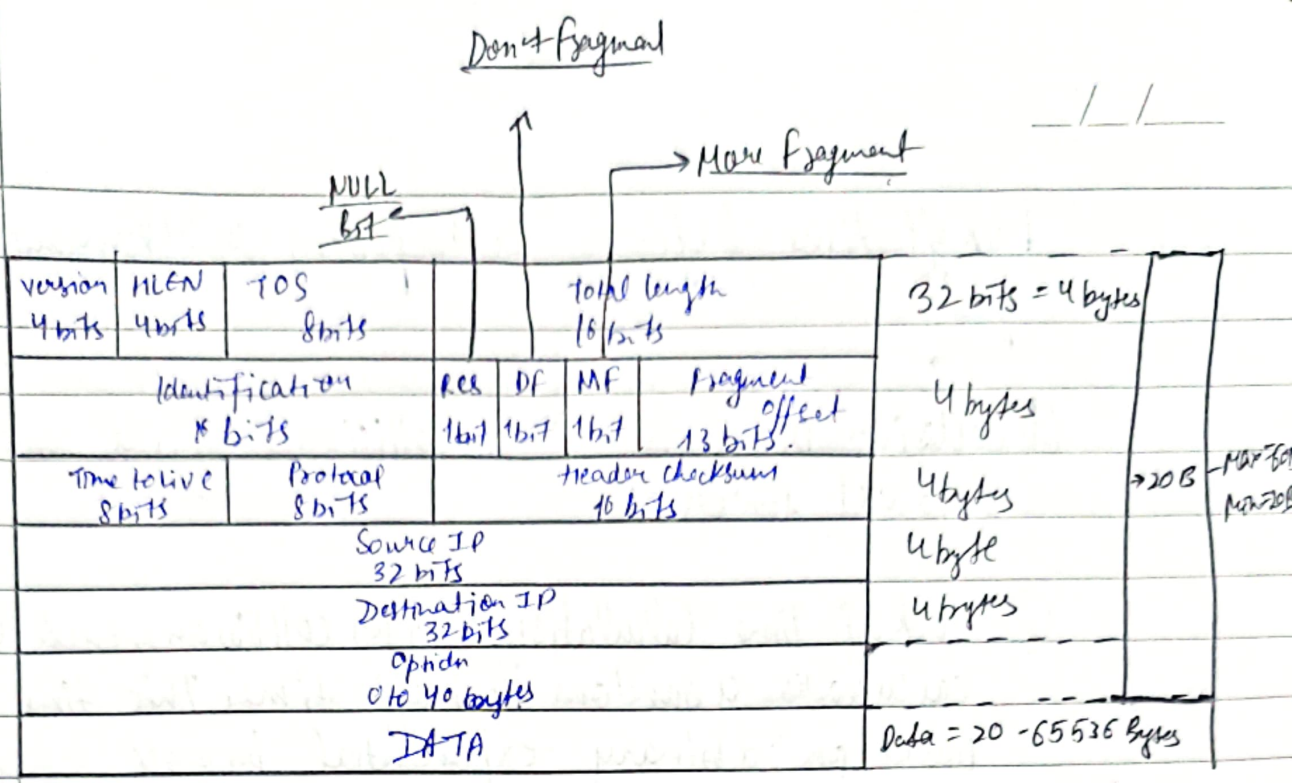
(8) Time to live (8 bits) → limits the lifetime of the packet, prevent indefinite looping.

(9) Protocol (8 bits) → Specifies the higher-layer protocol used after IP.

(10) Header Checksum (16 bits) → Ensures the integrity of header during transmission

(11) Source IP (32 bits) → Identifies the sender of the packet.

(12) Destination IP (32 bits) → Identifies the intended recipient of the packet.



(3) (i) It is a stateless protocol because each request is handled independently by the server without any knowledge of previous requests. It means that each request from a client to the server is treated as a new request, without any memory of past interaction. This design simplifies implementation & enhances scalability but requires additional mechanisms like cookies or sessions to maintain user state across multiple requests.

(ii) (a) 135.46.63.10

Taking the first 22 bits of it as network address we have. 135.46.60.0.

(b) 192.53.56.7

Taking the first 22 bits as network address we have 192.53.56.0

(iii) In CSMA/CD, the binary exponential back off algorithm is employed when collisions occur. After each frame transmission, if a collision is detected, the stations wait for a random

backoff time before attempting to retransmit the frame.

① Collision Detection → If a collision occurs, each station involved detects it.

② Backoff Time Calculation → After collision, each station calculates a random backoff time. This time is based on a binary exponential backoff scheme, where the backoff time doubles with each collision attempt.

③ Randomization → The backoff time is randomized to avoid synchronization issues. Stations select a random time within their calculated backoff window.

④ Retransmission Attempt → After waiting for the backoff time, stations attempt to retransmit their frames. If another collision occurs, the process repeats.

⑤ Increasing Backoff → With each unsuccessful transmission attempt, the backoff time increases exponentially, giving higher priority to stations with fewer collision attempts.

iv ⓐ Connection:

TCP, a connection-oriented protocol, establishes a connection b/w sender & receiver before transmitting data. (communication is reliable & ensures that data is delivered in

the correct order.

UDP, a connectionless protocal, doesn't establish a connection before sending data. Communication is unreliable, & there is no guarantee of data delivery or order.

(b) Sequence of Data Packets at the Receiver:

TCP ensures that the data packets arrive at the receiver in the same order they were sent, as it uses sequence nos. & acknowledgments to manage packet flow.

UDP doesn't guarantee the order of data packets at the receiver, as packets may arrive out of order.

(c) Acknowledgement of Received Packets:

TCP, Utilizes acknowledgements to confirm the receipt of data packets. If a packet is not acknowledged, TCP will retransmit it to ensure reliable data delivery.

UDP, Doesn't use acknowledgements, so there is no confirmation of packet receipt. This can result in faster transmission but lacks reliability.

(1) (i) Nyquist sampling rate = 2x highest frequency component

Highest Frequency Component = $200KH_2$

Nyquist rate = $2 \times 200KH_2 = \boxed{400KH_2}$ Hz

(ii) ① Static Routing →

→ The routes are manually configured & don't change unless modified by an administrator.

→ Example :- Configuring a router to send all traffic for a specific destination network through a particular interface.

② Dynamic Routing →

→ Dynamic Routing protocols automatically update routing tables based on network changes such as topology changes or link failures.

→ Example :- Routing Info. Protocol (RIP) dynamically updates routing tables by exchanging routing info. b/w routers.

(iii) (a) Message: 1101101101.
Generator: x^3+1 → 1001

```
1001 | 1101101101000 | 1100001100
     1001↓
     ----
      1001
      1001↓
      ----
       0000
       0000↓
       ----
        0001
        0000↓
        ----
         0011
         0000↓
         ----
          0110
          0000
```

```
1101
1001
----
1000
1001
----
 0010
 0000
 ----
  0100
  0000
  ----
   100
```

~~Re~~ Transmitted ~~string~~ String → 1101101101100

(b) Received message → 1101001101100

```
1001 | 1101001101100 | 1100|0|000
     1001
     ----
     1000
     1001
     ----
      0010
      0000
      ----
       0101
       0000
       ----
        1011
        1001
        ----
         0100
         0000
         ----
          1001
          1001
          ----
           0010
           0000
           ----
            0100
            0000
            ----
             100
```

Since Remainder is not 0 error is

(5) (i) No. of fragments = $\left\lceil \frac{\text{IP Packet size}}{\text{MTU Size}} \right\rceil$

$= \left\lceil \frac{9000}{1500} \right\rceil = \boxed{6 \text{ fragments}}$

The first 5 fragments payload = MTU size - IP header size

= 1500 - 20 bytes

= **1480 bytes**

The payload of last fragment = 9000 - (5 * 1480)

= 9000 - 7400

= **1600 bytes**

(ii) A machine can have multiple IP addresses associated with a single DNS name through a mechanism called DNS Round Robin. Essentially, when a DNS query is made for a certain hostname, the DNS server can respond with multiple IP addresses in a rotating order. This allows for load distribution & fault tolerance among multiple servers or network interfaces associated with the same DNS name.

(iii) (a) IP 184.86.92.182 belongs to class B, i.e., 128.00.0 to 191.255.255.255.

(b)

(6) (i) Flow control is crucial in network communication to prevent overwhelming receivers with data, ensuring smooth transition. One technique to manage flow control is the use of sliding window protocol, allowing senders to transmit multiple data packets before requiring acknowledgement from the receiver, optimizing network efficiency.

(ii) Multiplexing is a technique in telecommunications that combines multiple signals into a single transmission medium, optimizing bandwidth usage. Here's the diff. b/w Time Division Multiplexing (TDM) & frequency division multiplexing (FDM).

① Time Division Multiplexing (TDM):

→ Divides time into slots, with each slot assigned to a diff. signal.
→ Suitable for digital signals & analog signals.
→ Utilizes time slices for each signal.
→ Example: Phone calls in a cell phone network.

② Frequency Division Multiplexing (FDM):

→ Shares the frequency spectrum among multiple

signals.
→ Works primarily with analog signals.
→ Each signal operates at a distinct frequency.
→ Example: Radio broadcasting.

(7) (i) The header checksum of an IP packet is recalculated at every hop to ensure the integrity of the packet's header. As the packet traverses diff. routers & networks, there's a chance of corruption or alteration in the header due to noise, errors, or malicious attacks. By recalculating the checksum at each hop, routers can verify that the header remains intact & hasn't been tampered with, ensuring reliable delivery to the destination.

(ii) Yes, the loss of DNS packets with UDP can lead to delays in hostname resolution or failed queries. DNS resolvers tackle this by employing timeout & retry strategies. If no response is received within a set time, resolvers retry the query, potentially using different DNS servers. In cases of UDP failure, some apps & servers may switch to TCP for DNS queries due to its reliability via ack & retransmission.

(iii) The optimality principle in networks asserts that each router in a network should have complete & accurate info. about the topology of the entire network,

& each router should make routing decisions based solely on this global info. This principle ensures that each router forwards packets along the shortest or most optimal path towards their destination, leading to efficient & reliable network communication. By adhering to the optimality Principle, routers can dynamically adapt to changes in network conditions & topology, optimizing the overall network performance.

(iv) Transmission impairment refers to the degradation or alteration of a signal as it travels through a transmission medium. This impairment can occur due to various factors such as attenuation, distortion, noise & interference.

① Distortion → It refers to changes in the shape or form of the signal waveform during transmission. It occurs when the signal waveform at the receiver differs from the original waveform. It can result from factors like interference, reflections, & nonlinearities in the transmission medium or components.

② Attenuation → It is the reduction in signal strength as it propagates through the medium. It leads to the weakening of the signal over distance, primarily due to resistance, absorption, & dispersion in the medium. Unlike distortion, it doesn't alter the waveform shape but decreases its magnitude.