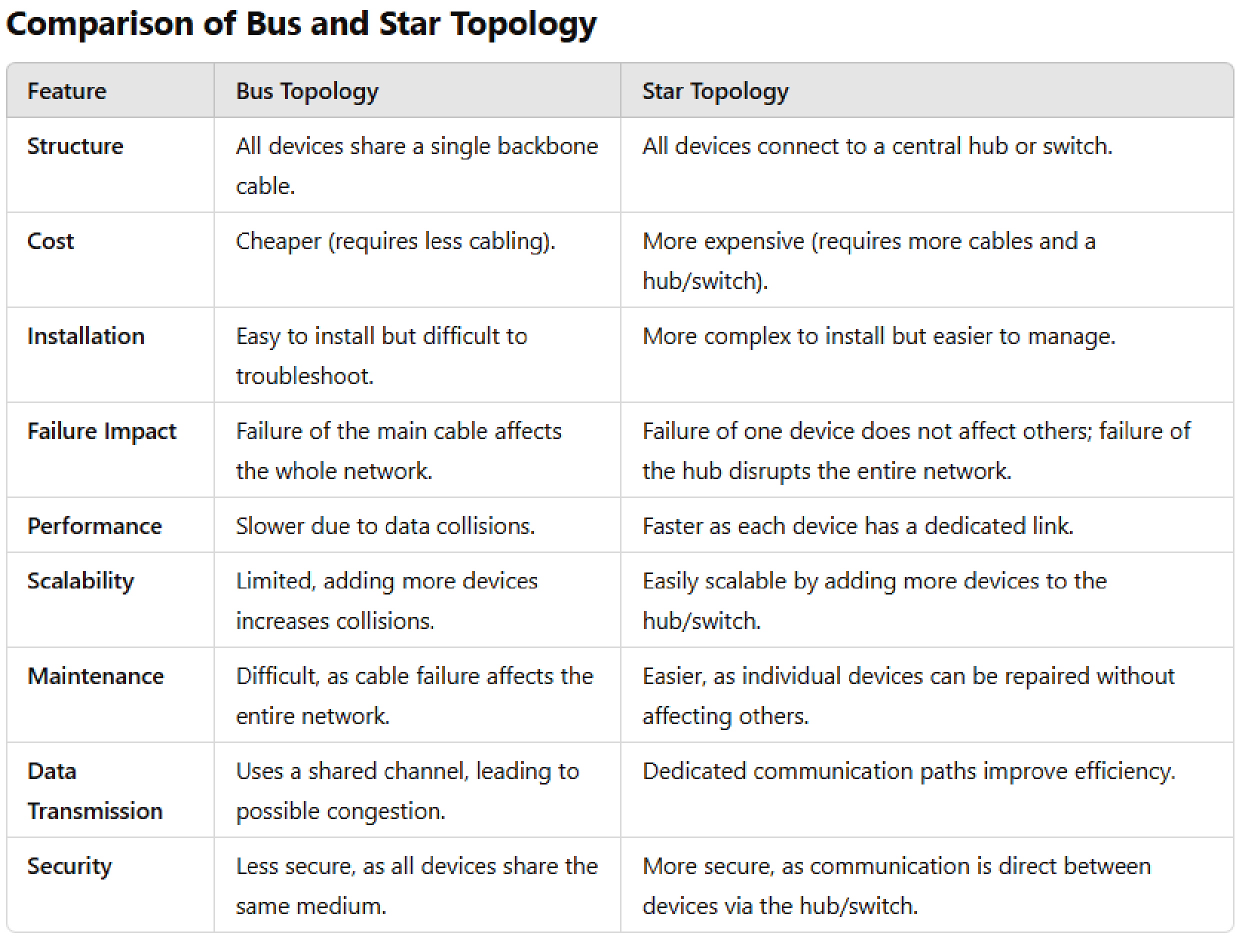
CNND DEC 2023 Answers

Q1

a) Compare Bus and Star topology



Comparison of Bus and Star Topology

Feature	Bus Topology	Star Topology
Structure	All devices share a single backbone cable.	All devices connect to a central hub or switch.
Cost	Cheaper (requires less cabling).	More expensive (requires more cables and a hub/switch).
Installation	Easy to install but difficult to troubleshoot.	More complex to install but easier to manage.
Failure Impact	Failure of the main cable affects the whole network.	Failure of one device does not affect others; failure of the hub disrupts the entire network.
Performance	Slower due to data collisions.	Faster as each device has a dedicated link.
Scalability	Limited, adding more devices increases collisions.	Easily scalable by adding more devices to the hub/switch.
Maintenance	Difficult, as cable failure affects the entire network.	Easier, as individual devices can be repaired without affecting others.
Data Transmission	Uses a shared channel, leading to possible congestion.	Dedicated communication paths improve efficiency.
Security	Less secure, as all devices share the same medium.	More secure, as communication is direct between devices via the hub/switch.

b) List the internetworking devices and explain any one

Internetworking Devices

Internetworking devices connect different networks to enable communication between them. The main devices are:

1. **Repeater**
2. **Hub**
3. **Bridge**
4. **Switch**
5. **Router**
6. **Gateway**
7. **Modem**

Explanation of Router

A **router** is a networking device that forwards data packets between different networks. It operates at the **Network Layer (Layer 3) of the OSI model** and uses **IP addresses** to determine the best path for data transmission.

Functions of a Router

Packet Forwarding: Routes data from one network to another based on destination IP addresses.
Path Selection: Uses routing algorithms (RIP, OSPF, BGP) to find the optimal path.
Traffic Management: Controls network congestion and improves efficiency.
Network Security: Can implement firewalls and filters to block unauthorized traffic.

Types of Routers

- **Wired Router**: Uses Ethernet cables for connectivity.
- **Wireless Router**: Provides Wi-Fi access for wireless devices.
- **Core Router**: Used in large networks for high-speed data transfer.
- **Edge Router**: Connects internal networks to external networks (e.g., ISP connections).

c) Explain RLE with an example

Run-Length Encoding (RLE) is a simple lossless compression technique used to reduce the size of repetitive data sequences. It works by replacing consecutive occurrences of the same data value with a single value and a count representing the number of repetitions.

How RLE Works

The idea behind RLE is to represent **runs** (continuous sequences) of repeated data efficiently. Instead of storing each repeated value individually, RLE stores:

1. The value.
2. The count of repetitions.

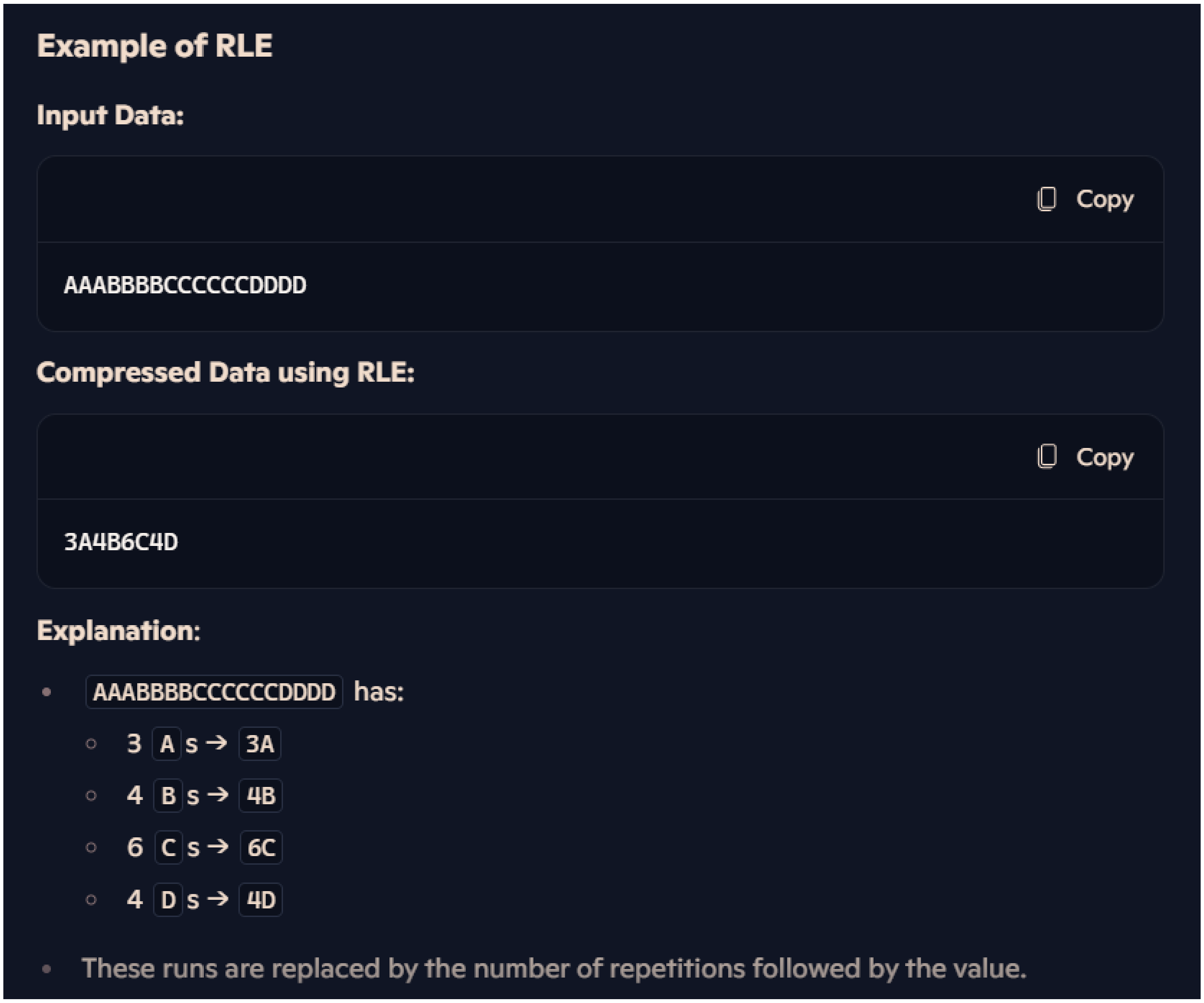
This method is most effective for data with many consecutive repeated values, such as images, text files, or binary sequences.

Advantages

1. **Efficient for Repeated Data**: Reduces file size significantly if the data has long runs of repetitions.
2. **Simple Implementation**: Easy to understand and use.

Disadvantages

1. **Inefficient for Random Data**: If the data has no repeated values, RLE can result in an increase in file size.



Example of RLE

Input Data:

```
AAABBBBCCCCCCDDDD
```

Compressed Data using RLE:

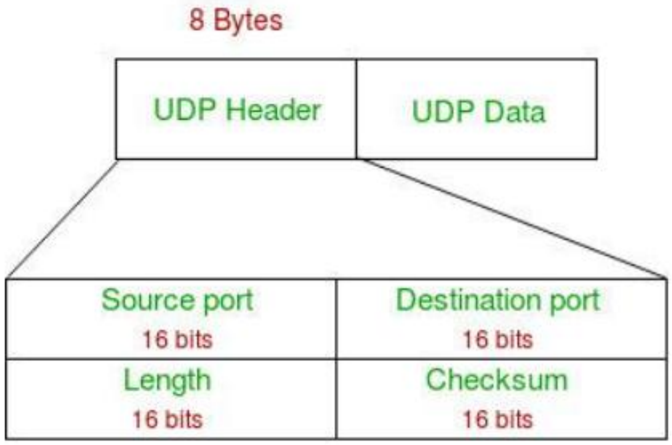
```
3A4B6C4D
```

Explanation:

- `AAABBBBCCCCCCDDDD` has:
  - 3 `A`s → `3A`
  - 4 `B`s → `4B`
  - 6 `C`s → `6C`
  - 4 `D`s → `4D`
- These runs are replaced by the number of repetitions followed by the value.

d) Draw the UDP Header with its fields.

UDP is a connectionless and lightweight transport layer protocol that is part of the Internet Protocol Suite. Unlike TCP, UDP focuses on providing fast, efficient communication without ensuring reliability, ordering, or error correction. Its header is compact, consisting of only **8 bytes**, making it ideal for applications like streaming and online gaming where speed is more critical than reliability.



UDP Header

Structure of the UDP Header

The UDP header consists of four fields, each 16 bits (2 bytes) long:

1. **Source Port (16 bits)**:
   - Identifies the port number of the application sending the data.
   - Optional in some cases; if not used, it can be set to 0.

2. **Destination Port (16 bits)**:
   - Specifies the port number of the receiving application.
   - Ensures the data is delivered to the appropriate service.

3. **Length (16 bits)**:
   - Indicates the total length of the UDP datagram (header + data), measured in bytes.
   - Minimum length is **8 bytes** (only the header).

4. **Checksum (16 bits)**:
   - Used for error-checking the header and data.
   - Optional in IPv4 but mandatory in IPv6.
   - If no checksum is calculated in IPv4, this field is set to 0.

Advantages of UDP Header Format

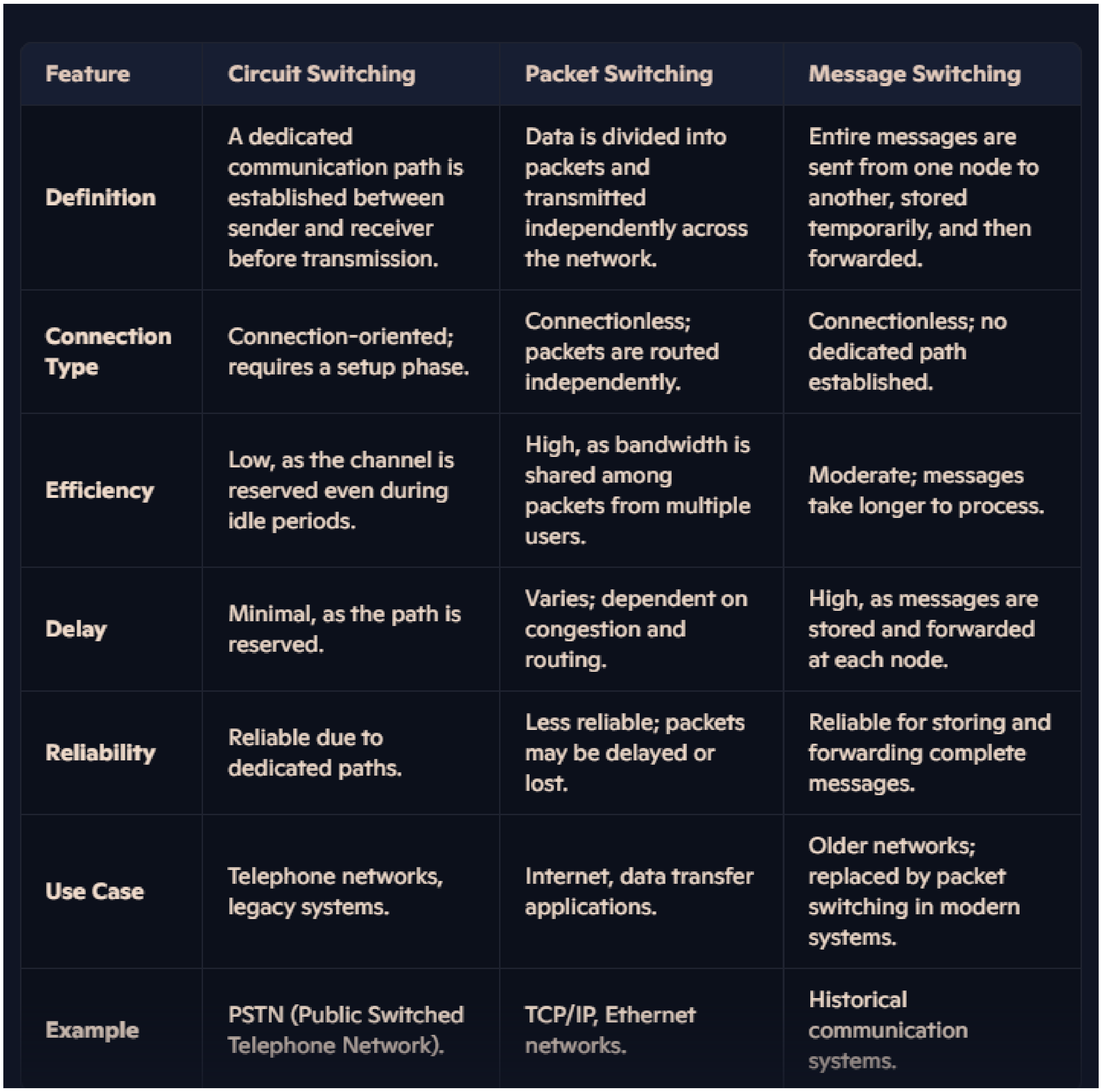
1. **Fast Transmission**:
   - Connectionless and efficient, ideal for time-sensitive applications.
2. **Low Complexity**:
   - Easy to implement and operate.

Limitations of UDP

1. **No Reliability**:
   - No acknowledgment mechanism to confirm data delivery.
2. **No Ordering**:
   - Data may arrive out of order.
3. **No Error Correction**:
   - UDP only detects errors but does not fix them.

Q2

b) Compare the switching technologies.



Feature	Circuit Switching	Packet Switching	Message Switching
Definition	A dedicated communication path is established between sender and receiver before transmission.	Data is divided into packets and transmitted independently across the network.	Entire messages are sent from one node to another, stored temporarily, and then forwarded.
Connection Type	Connection-oriented; requires a setup phase.	Connectionless; packets are routed independently.	Connectionless; no dedicated path established.
Efficiency	Low, as the channel is reserved even during idle periods.	High, as bandwidth is shared among packets from multiple users.	Moderate; messages take longer to process.
Delay	Minimal, as the path is reserved.	Varies; dependent on congestion and routing.	High, as messages are stored and forwarded at each node.
Reliability	Reliable due to dedicated paths.	Less reliable; packets may be delayed or lost.	Reliable for storing and forwarding complete messages.
Use Case	Telephone networks, legacy systems.	Internet, data transfer applications.	Older networks; replaced by packet switching in modern systems.
Example	PSTN (Public Switched Telephone Network).	TCP/IP, Ethernet networks.	Historical communication systems.

Q4

a) What is controlled media access? Explain the controlled media access techniques.

Controlled media access refers to a method used in computer networks to regulate which device or node can access the shared communication medium (such as a wired or wireless channel) at a given time. The goal is to avoid collisions and ensure efficient use of the network resources.

In controlled media access, devices must wait for explicit permission to transmit data, unlike random access methods (like CSMA). This is particularly useful in networks where orderly communication and collision avoidance are important.

Controlled Media Access Techniques
Here are the primary techniques used for controlled media access:

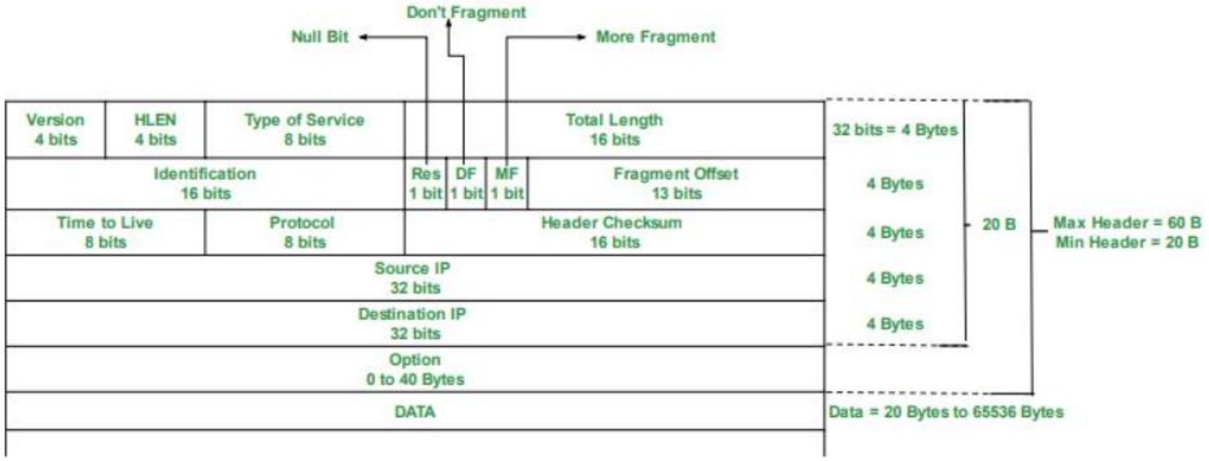
1. **Polling**:
   - A central controller or a master device asks each device (or node) sequentially whether it has data to transmit.
   - If a device responds positively, it is granted permission to send its data.
   - *Example*: Used in point-to-multipoint networks like Wi-Fi (in certain modes) and modems.

2. **Token Passing**:
   - A special "token" is passed around the network in a predefined order. A device can only transmit data if it holds the token.
   - Once the transmission is done, the token is released for the next device to use.
   - *Example*: Common in Token Ring networks and some industrial control systems.

3. **Time Division Multiple Access (TDMA)**:
   - The communication channel is divided into fixed time slots.
   - Each device is assigned a specific time slot during which it can transmit data.
   - *Example*: Widely used in cellular networks and satellite communication systems.

b) Draw the IPv4 Header and explain the header format.

The **IPv4 Header** is a crucial part of the IPv4 protocol, providing necessary information for the transmission of packets across networks. It is 20 to 60 bytes long (depending on options) and is structured into several fields.



IPv4 Datagram Header

Explanation of IPv4 Header Fields:

1. **Version (4 bits):** Indicates the IP version. For IPv4, this value is **4**.

2. **IHL (Internet Header Length) (4 bits):** Specifies the **length of the header** in 32-bit words. Minimum value is 5 (i.e., 20 bytes).

3. **Type of Service (ToS) (8 bits):** Used to specify **priority and quality** of the packet.

4. **Total Length (16 bits):** Specifies the **total size** of the packet (header + data) in bytes. Maximum value: **65,535 bytes**.

5. **Identification (16 bits):** Used to **identify fragments** of a single IP datagram.

6. **Flags (3 bits):**
   Control flags:
   - Bit 0: Reserved
   - Bit 1: Don't Fragment (DF)
   - Bit 2: More Fragments (MF)

7. **Fragment Offset (13 bits):** Indicates the **position** of a fragment in the original packet.

8. **Time to Live (TTL) (8 bits):** Limits the **lifetime** of the packet in the network. Prevents looping.

9. **Protocol (8 bits):** Specifies the **higher-layer protocol** (e.g., 6 for TCP, 17 for UDP).

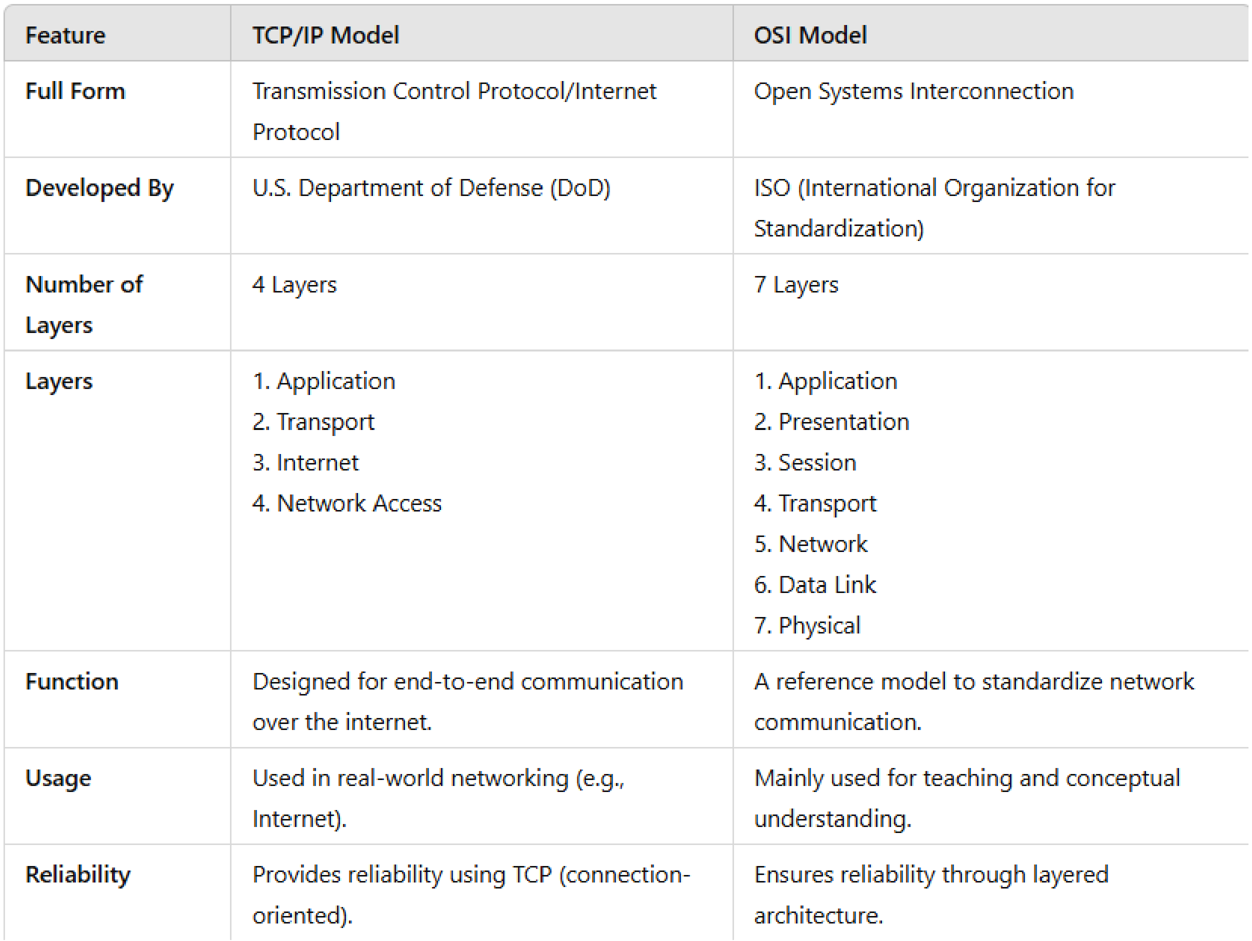
10. **Header Checksum (16 bits):** Used for **error-checking** of the header.

11. **Source IP Address (32 bits):** IP address of the **sender**.

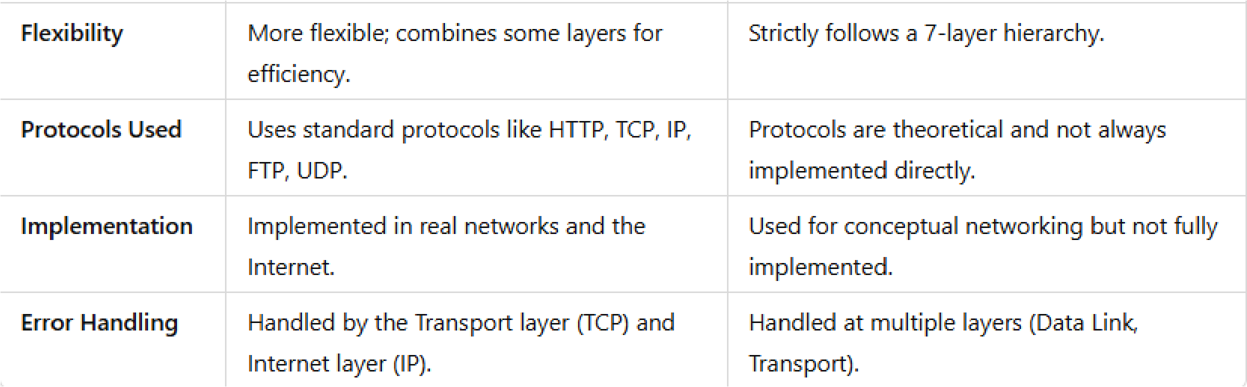
12. **Destination IP Address (32 bits):** IP address of the **receiver**.

Q5

a) Compare TCP/IP and OSI.



Feature	TCP/IP Model	OSI Model
Full Form	Transmission Control Protocol/Internet Protocol	Open Systems Interconnection
Developed By	U.S. Department of Defense (DoD)	ISO (International Organization for Standardization)
Number of Layers	4 Layers	7 Layers
Layers	1. Application 2. Transport 3. Internet 4. Network Access	1. Application 2. Presentation 3. Session 4. Transport 5. Network 6. Data Link 7. Physical
Function	Designed for end-to-end communication over the internet.	A reference model to standardize network communication.
Usage	Used in real-world networking (e.g., Internet).	Mainly used for teaching and conceptual understanding.
Reliability	Provides reliability using TCP (connection-oriented).	Ensures reliability through layered architecture.



Flexibility	More flexible; combines some layers for efficiency.	Strictly follows a 7-layer hierarchy.
Protocols Used	Uses standard protocols like HTTP, TCP, IP, FTP, UDP.	Protocols are theoretical and not always implemented directly.
Implementation	Implemented in real networks and the Internet.	Used for conceptual networking but not fully implemented.
Error Handling	Handled by the Transport layer (TCP) and Internet layer (IP).	Handled at multiple layers (Data Link, Transport).

b) Explain the distance vector routing with an example.

Distance Vector Routing is a routing algorithm used in computer networks to determine the best path for data packets. Routers exchange information about the distances (or costs) to other nodes in the network, and the routing decision is based on the shortest path. It is characterized by simplicity and local sharing of routing information.

How It Works

1. **Initialization**:
   - Each router maintains a table listing the cost (distance) to all other nodes and the next hop to reach each destination.
   - Initially, routers only know the distance to their directly connected neighbors.

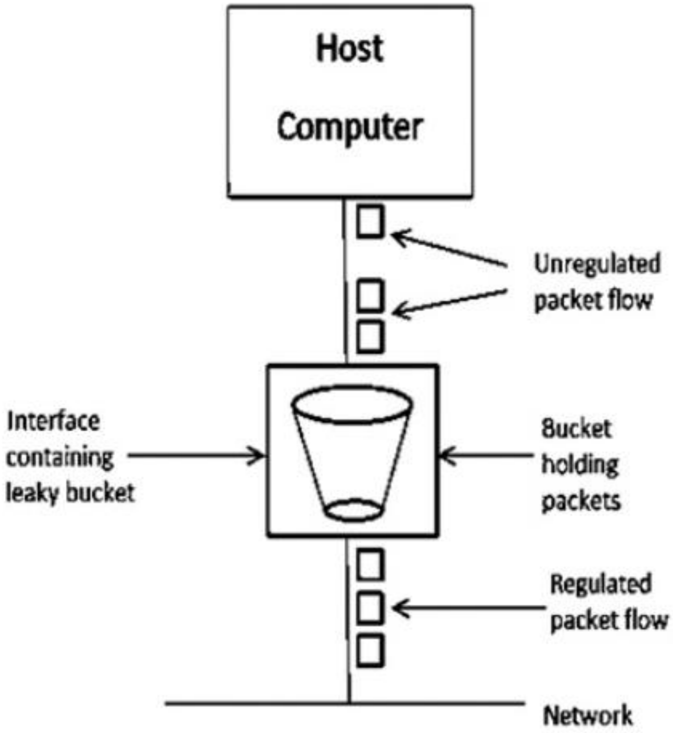
2. **Periodic Updates**:
   - Routers periodically share their routing tables with immediate neighbors.
   - Upon receiving an update, each router compares the existing cost to a destination with the cost received from a neighbor, adding the neighbor's link cost.

3. **Convergence**:
   - Over time, routers iteratively update their tables, ensuring that all routes reflect the shortest path across the network.

Q6. Write a Short Notes on

a) Leaky bucket

The **Leaky Bucket Algorithm** is a traffic shaping mechanism used in computer networks to control the data flow. It ensures a steady transmission rate, preventing bursts of data from overloading network resources.



How It Works
The algorithm is based on a simple analogy of a bucket with a hole in its base:

1. **Input**: Data packets are added into the bucket at varying rates.
2. **Output**: Data leaks out of the bucket at a constant rate through the hole.
3. **Overflow**: If the bucket fills beyond its capacity (due to excessive data input), the excess data is discarded, ensuring controlled output.

Key Features

- **Traffic Shaping**: Maintains a uniform data flow rate, smoothing traffic bursts.
- **Queue Management**: Implements a finite buffer (the bucket), ensuring no overflow beyond capacity.
- **Efficiency**: Prevents congestion in the network by regulating data flow.

Applications

- Used in networks to enforce quality of service (QoS).
- Helps in managing bandwidth allocation and maintaining stability in traffic-heavy scenarios.

b) SMTP

Definition:

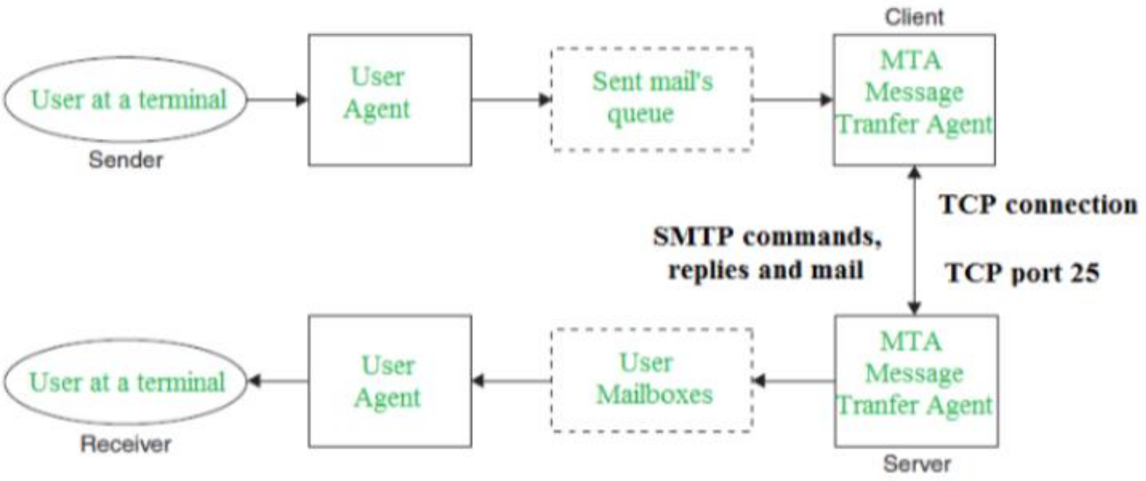
SMTP stands for Simple Mail Transfer Protocol. It is a standard protocol used to send emails from a client to a mail server or between mail servers.

How it Works:

1. User composes an email in a client (like Outlook or Gmail).
2. SMTP sends the email to the **recipient's mail server**.
3. The recipient then retrieves it using **POP3** or **IMAP**.

Key Features:

- Works on **TCP port 25**
- Follows **push model** – sends email from sender to receiver's mail server
- Used only for **sending emails**, not receiving


Client
User at a terminal
Sender
User Agent
Sent mail's queue
MTA Message Tranfer Agent
TCP connection
SMTP commands, replies and mail
TCP port 25
User at a terminal
Receiver
User Agent
User Mailboxes
MTA Message Tranfer Agent
Server