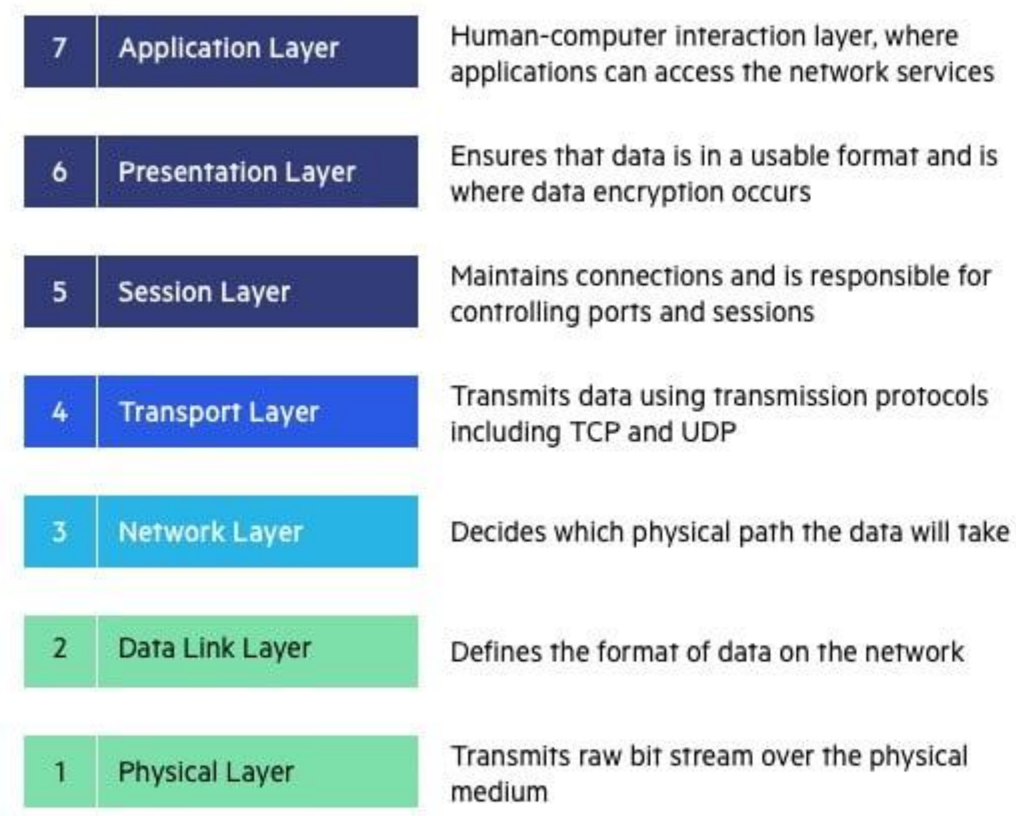
Question:
Draw the layers of the OSI model and explain each layer in detail.

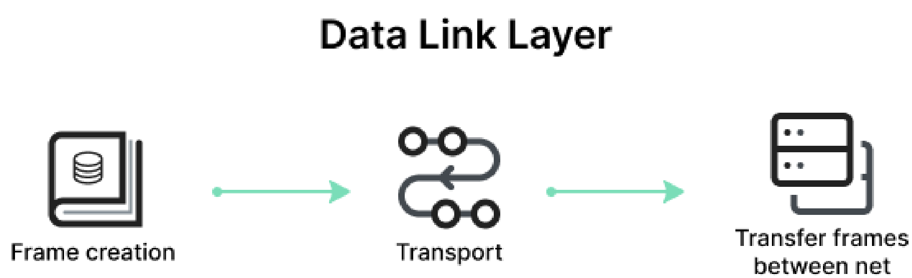
Answer:
The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes network communication into seven layers. Below is a diagram representing the OSI model:



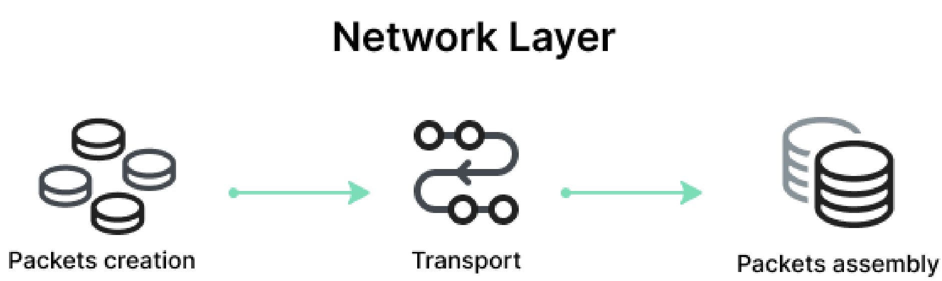
Explanation of Each Layer:

1. **Physical Layer:**
   - Responsible for transmitting raw binary data over the network.
   - Deals with hardware components like cables, switches, and network adapters.
   - Converts digital data into electrical, optical, or radio signals.

2. **Data Link Layer:**
   - Ensures reliable data transfer between two directly connected devices.
   - Handles framing, error detection (e.g., CRC), and MAC addressing.
   - Divided into two sub-layers:
     - **Logical Link Control (LLC):** Error control and flow control.
     - **Media Access Control (MAC):** Access to physical media (Ethernet, Wi-Fi).

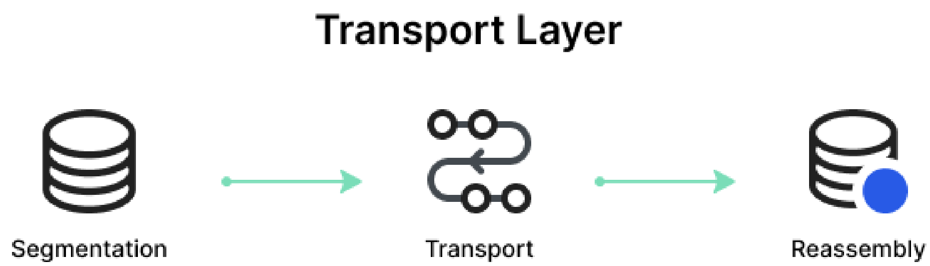


3. **Network Layer:**
   - Responsible for routing packets from source to destination across multiple networks.
   - Uses logical addressing (IP addresses).
   - Protocols: **IP (IPv4, IPv6), ICMP, ARP, RIP, OSPF.**

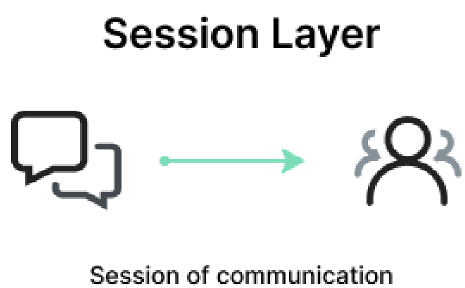


4. **Transport Layer:**
   - Ensures end-to-end communication between devices.
   - Provides segmentation, flow control, and error correction.

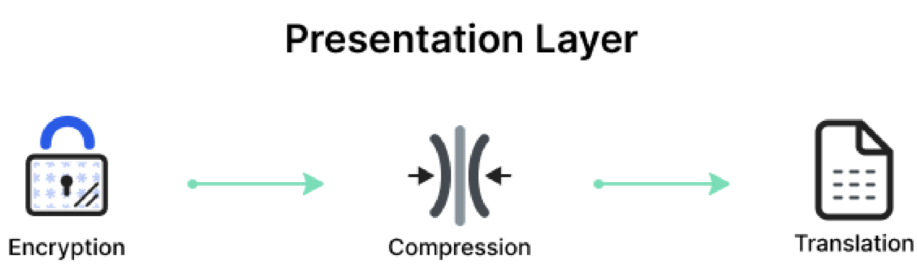
- Protocols: **TCP (reliable, connection-oriented), UDP (fast, connectionless).**



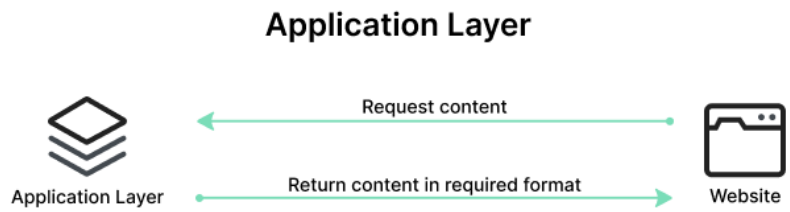
5. **Session Layer:**
   - Manages sessions (connections) between applications.
   - Controls dialogues, synchronization, and session recovery.
   - Example: Managing multiple connections in a video conference.



6. **Presentation Layer:**
   - Converts data into a format understood by the application layer.
   - Handles encryption, compression, and character encoding.
   - Example: SSL/TLS encryption in secure communication.



7. **Application Layer:**
   - Provides network services directly to end-users.
   - Examples: Web browsing (HTTP), Email (SMTP, IMAP), File Transfer (FTP).



○

Question:

Explain the **High-Level Data Link Control (HDLC) protocol** with a neat diagram.

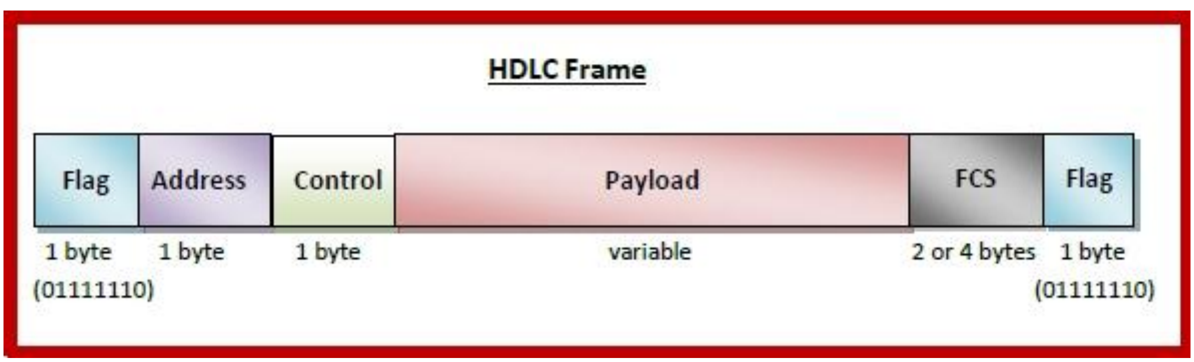
Answer:

High-Level Data Link Control (HDLC) is a **bit-oriented** protocol used for reliable data transmission at the data link layer (Layer 2) of the OSI model. It was developed by **ISO (International Organization for Standardization)** and is widely used in both point-to-point and multipoint communication.

HDLC Frame Structure:

The HDLC frame consists of six key fields:

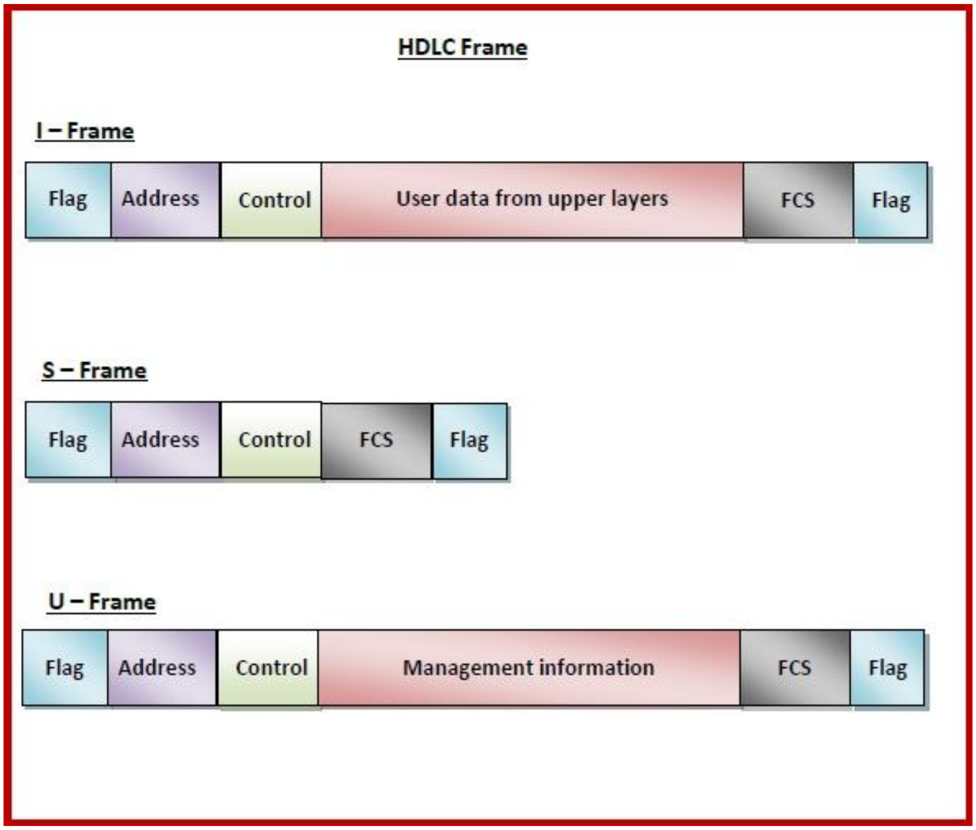
1. **Flag (8 bits)** – Marks the beginning and end of a frame (**01111110**).
2. **Address (8-16 bits)** – Identifies the sender or receiver in multipoint configurations.
3. **Control (8-16 bits)** – Defines frame type (I-frame, S-frame, or U-frame) and flow/error control.
4. **Information (Variable length)** – Contains actual data (present only in I-frames).
5. **Frame Check Sequence (FCS) (16-32 bits)** – Used for error detection.
6. **Flag (8 bits)** – Marks the end of the frame (**01111110**).



Types of HDLC Frames:

HDLC frames are categorized into three types:

1. **Information (I) Frame**
    - Used for sending data.
    - Contains **sequence numbers** and **flow control** information.
2. **Supervisory (S) Frame**
    - Used for acknowledgment and flow control.
    - No information field is present.
3. **Unnumbered (U) Frame**
    - Used for control functions such as establishing or terminating links.

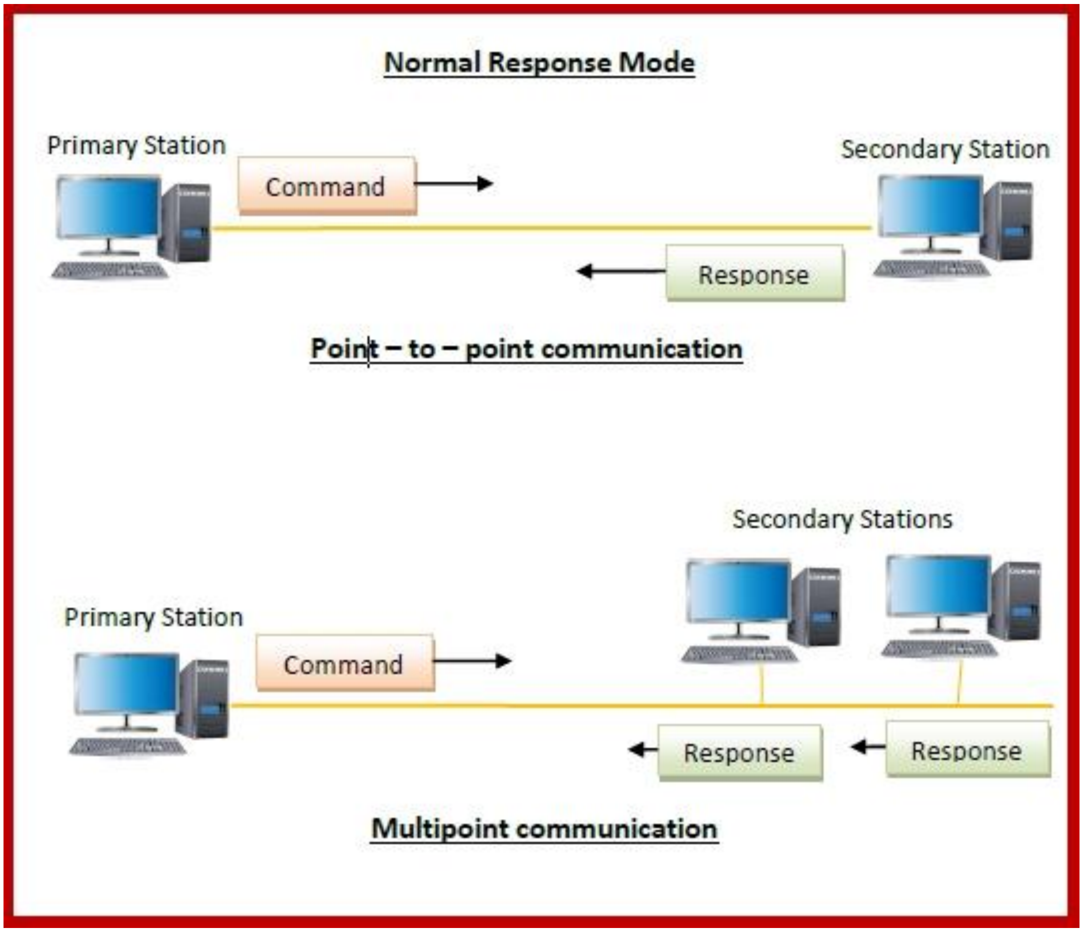


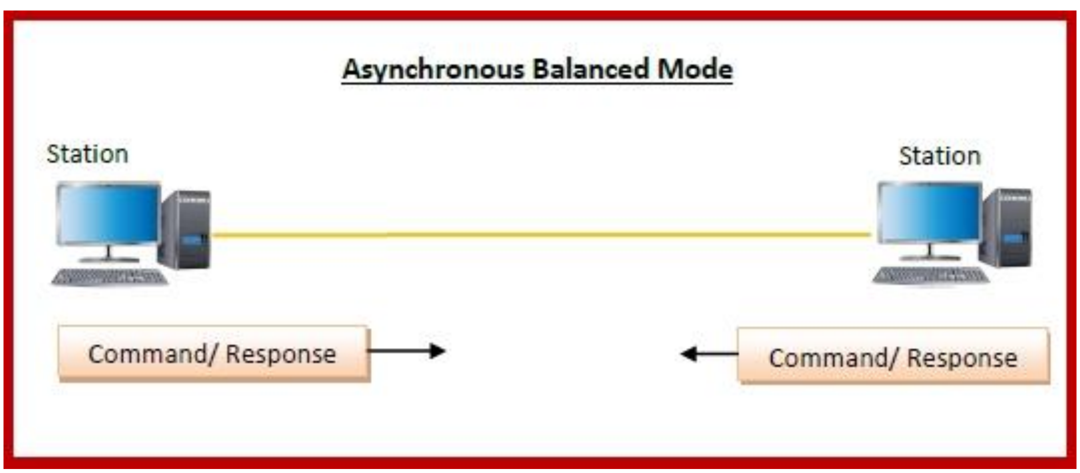
HDLC Modes of Operation:

HDLC supports three modes:

1. **Normal Response Mode (NRM)** – Unbalanced mode where the **secondary station** sends data only when allowed by the **primary station**.
2. **Asynchronous Balanced Mode (ABM)** – Both stations operate as **peers**, meaning either can initiate communication.

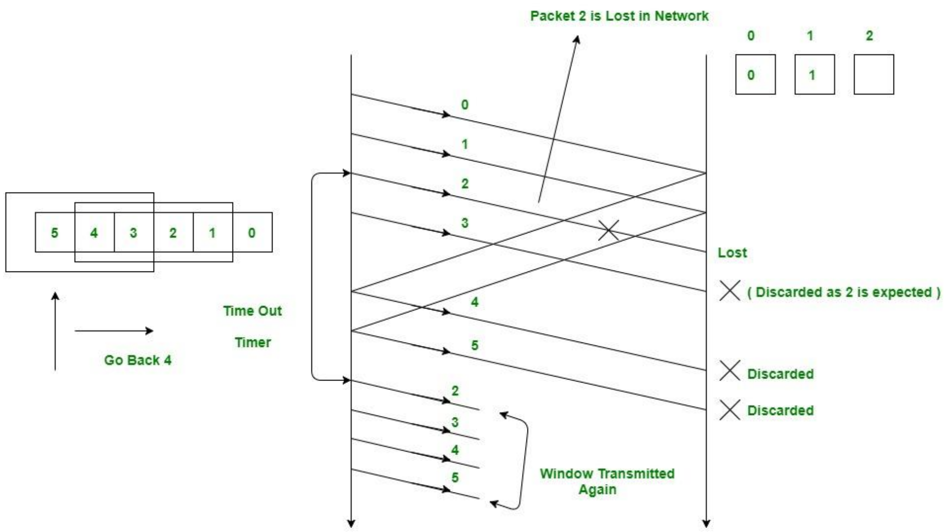
3. **Asynchronous Response Mode (ARM)** – The secondary station can transmit without waiting for permission.





Question:
Explain the Go-Back-N (GBN) protocol in detail. Discuss its working, advantages, and disadvantages. *(7 Marks)*

Answer:
The **Go-Back-N (GBN) protocol** is a type of **Sliding Window Protocol** used in **reliable data**



transmission over networks. It is an **ARQ (Automatic Repeat reQuest) protocol** that ensures correct delivery of data frames even in the presence of errors.

Working of Go-Back-N Protocol:

1. **Sliding Window Mechanism:**
    - The sender can transmit **multiple frames** (up to a window size 'N') before receiving an acknowledgment.
    - It maintains a **window** of 'N' frames, meaning it can send up to 'N' unacknowledged frames at a time.
2. **Acknowledgment & Retransmission:**
    - The receiver sends an **ACK (Acknowledgment)** only for the last correctly received frame.
    - If a frame is lost or an error occurs, the receiver **discards all subsequent frames**, and the sender has to **retransmit from the lost frame** onwards.
    - This leads to **retransmission of multiple frames**, even if only one frame is lost.

Question:

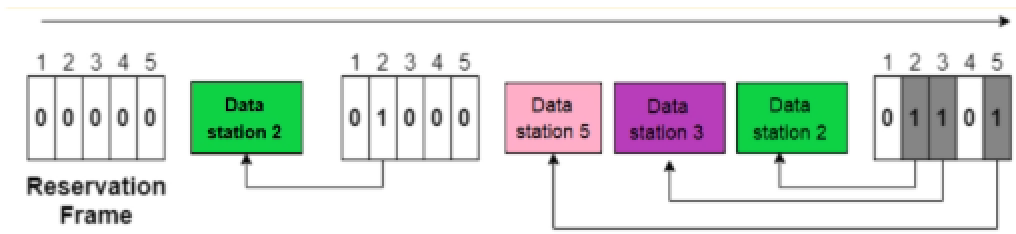
Describe controlled access protocols. How do they ensure orderly access to the shared communication medium? *(5 Marks)*

Answer:

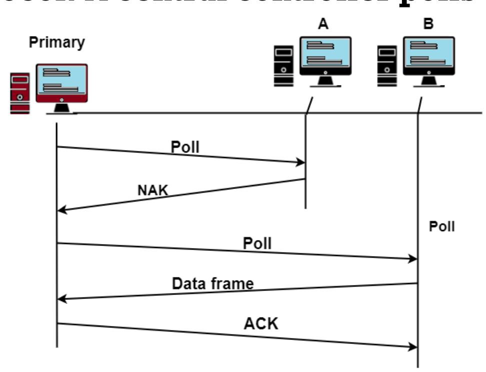
Controlled access protocols are **MAC (Medium Access Control) protocols** that regulate access to a shared communication medium in an **organized and collision-free** manner. They allow only one device to transmit at a time, ensuring efficient and fair communication.

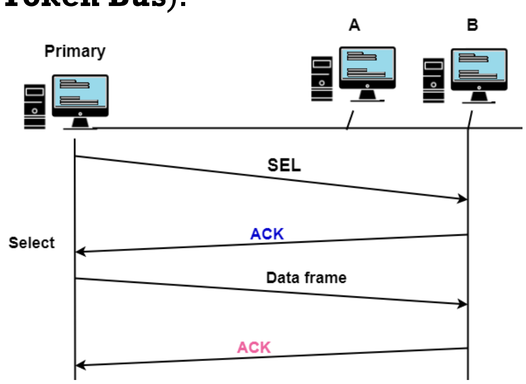
Types of Controlled Access Protocols:

1. **Reservation Protocol:** Devices **reserve** the medium before transmission (e.g., **TDMA**).

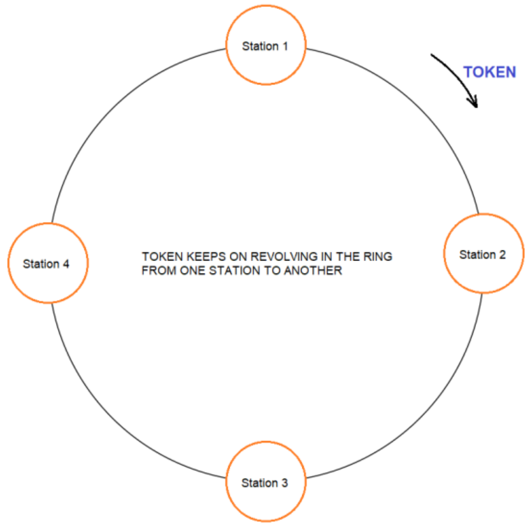


2. **Polling Protocol:** A **central controller polls** each device in sequence (e.g., **Token Bus**).





3. **Token Passing Protocol:** A **special token circulates**, allowing only the token holder to transmit (e.g., **Token Ring**).



How They Ensure Orderly Access:

- **Prevents Collisions:** Only one device transmits at a time.
- **Fair Access:** Ensures every device gets a turn.
- **Efficient Bandwidth Use:** Reduces retransmissions.
- **Guaranteed Access:** Avoids device starvation.
- **Ideal for High-Traffic Networks:** More efficient than contention-based protocols.

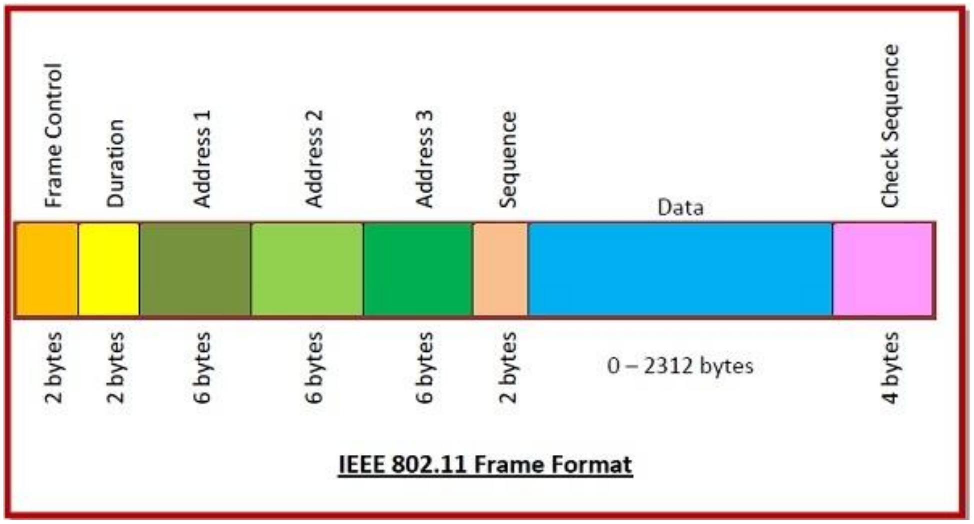
Question:
Differentiate between the OSI reference model and the TCP/IP reference model.

Summary Table:

Feature	OSI Model	TCP/IP Model
Developed by	ISO	DoD (USA)
Number of Layers	7	4
Layers	Physical, Data Link, Network, Transport, Session, Presentation, Application	Network Access, Internet, Transport, Application
Reliability	Strictly defined	More flexible, practical
Protocol Dependency	Protocol-independent	Uses TCP/IP suite
Usage	Theoretical model	Real-world networking (Internet)
Example Protocols	HDLC, Ethernet	TCP, UDP, IP, FTP, HTTP
Implementation	Not directly used	Used in real networks

Question:

Discuss the various features of Wi-Fi and the architectural functions of IEEE 802.11. *(5 Marks)*



Answer:

Features of Wi-Fi:

Wi-Fi (Wireless Fidelity) is a wireless communication technology based on IEEE 802.11 standards. Its key features include:

- **Wireless Connectivity** without cables.
- **High-Speed Data Transfer** up to several Gbps.
- **Multiple Frequency Bands** (2.4 GHz, 5 GHz, and 6 GHz).
- **Security Mechanisms** like WPA2 and WPA3.
- **Multiple Access Support** using **CSMA/CA.**

Architectural Functions of IEEE 802.11:

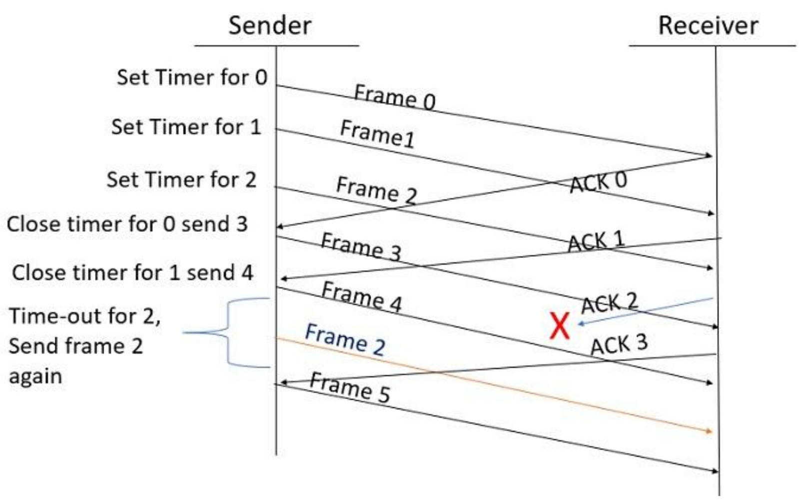
The IEEE 802.11 standard defines Wi-Fi network architecture with:

- **Basic Service Set (BSS):** Fundamental network unit.
- **Extended Service Set (ESS):** Multiple BSS interconnected.
- **Access Points (APs):** Manage communication.
- **Stations (STAs):** Devices connecting to APs.
- **Distribution System (DS):** Connects multiple APs.
- **Frame Structure:** Uses MAC frames for data transmission.

Wi-Fi advancements (e.g., Wi-Fi 6, Wi-Fi 7) improve speed, security, and efficiency.

Question:
Explain the **Selective Repeat Protocol** in data communication.

Answer:
Selective Repeat (SR) Protocol is an **error control protocol** used in data communication to ensure reliable transmission. It is an improvement over the **Go-Back-N** protocol by selectively retransmitting only the erroneous or lost frames instead of all frames after an error.



Working of Selective Repeat Protocol:

1. **Sliding Window Mechanism:**
   - Both the sender and receiver use a **window** to manage frames.
   - The sender can send multiple frames (up to the window size) before needing an acknowledgment (ACK).
   - The receiver can accept frames out of order and store them in a buffer.
2. **Error Handling:**
   - If a frame is received with an error, the receiver **discards it** and requests only that specific frame to be resent.
   - Other correctly received frames are stored until the missing frame arrives, ensuring efficiency.
3. **Acknowledgment (ACK):**
   - The receiver sends an acknowledgment (ACK) only for correctly received frames.
   - If the sender does not receive an ACK within a timeout period, it **retransmits only the missing frame** instead of all frames.

Question:
Explain the basic concept of Data Communications, Data Flow, and Categories of Network Interconnection.

Answer:

1. Data Communications:

Data communication refers to the process of transferring data between two or more devices through a transmission medium such as cables or wireless signals. The key components of data communication include:

- **Sender** – The device that sends the data.
- **Receiver** – The device that receives the data.
- **Transmission Medium** – The physical or wireless channel through which data is transmitted.
- **Message** – The actual data being transmitted.
- **Protocol** – A set of rules that govern communication between devices.

2. Data Flow:

Data flow represents how data moves between devices in a network. There are three types:

- **Simplex** – Data flows in only one direction (e.g., TV broadcasting).
- **Half-Duplex** – Data flows in both directions, but only one direction at a time (e.g., walkie-talkies).
- **Full-Duplex** – Data flows in both directions simultaneously (e.g., telephone communication).

3. Categories of Network Interconnection:

Network interconnection refers to how different networks or devices connect and communicate. The main categories are:

- **Local Area Network (LAN):** Connects devices within a small geographical area like an office or home.
- **Metropolitan Area Network (MAN):** Covers a city or large campus, connecting multiple LANs.
- **Wide Area Network (WAN):** Covers large geographical areas, such as the internet, connecting multiple LANs and MANs.

Question:
Explain Virtual Circuit (VC) and Datagram networks

Answer:

Virtual Circuit (VC) Network:

- A **VC network** establishes a **predefined path** before data transmission.
- It works similarly to a **telephone call** where a connection is established first, then data is transmitted, and finally, the connection is terminated.
- Each packet follows the same **pre-established route**, ensuring **orderly delivery**.
- Used in technologies like **ATM (Asynchronous Transfer Mode) and MPLS (Multiprotocol Label Switching)**.

Datagram Network:

- A **Datagram network** sends each packet **independently**, choosing the best available path dynamically.
- Similar to **postal mail**, where each letter can take a different route to reach the same destination.
- Packets may **arrive out of order** and require reassembly at the receiver's end.
- Used in the **Internet (IP-based networks)**

Comparison Table:

Feature	Virtual Circuit (VC) Network	Datagram Network
Path	Predefined before transmission	Dynamic for each packet
Reliability	More reliable, ordered delivery	Packets may arrive out of order
Overhead	Low after setup	High due to per-packet routing
Flexibility	Less flexible	More flexible and fault-tolerant
Example	ATM, MPLS	Internet (IP networks)

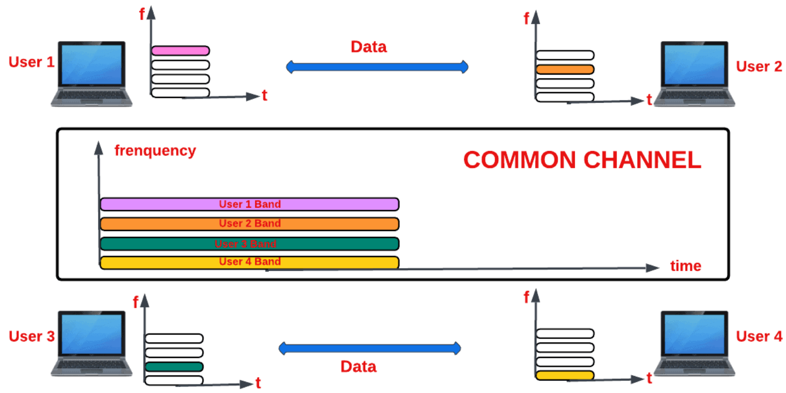
Question:

Explain Channelization Protocols in networking. (5 Marks)

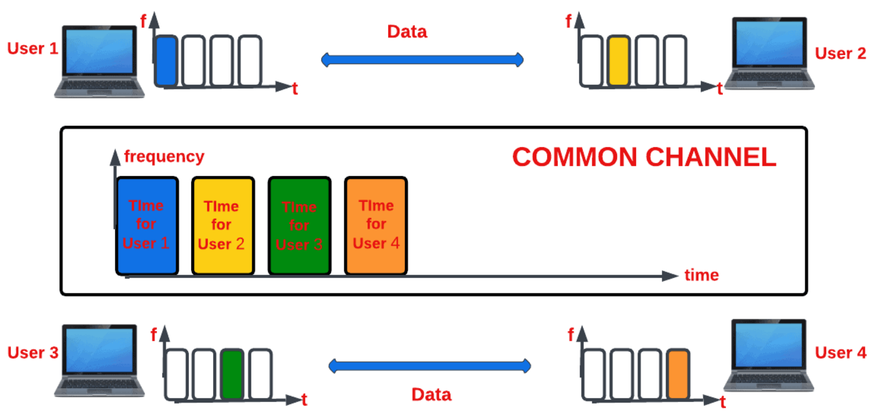
Answer:

Channelization protocols are multiple access protocols used in networking to allow multiple users to share a common communication channel efficiently. These protocols divide the available bandwidth into separate channels to avoid collisions and ensure smooth data transmission. The main types of channelization protocols are:

1. **Frequency Division Multiple Access (FDMA)**
    - The available bandwidth is divided into multiple frequency bands, each assigned to a specific user.
    - Example: Traditional radio and TV broadcasting.

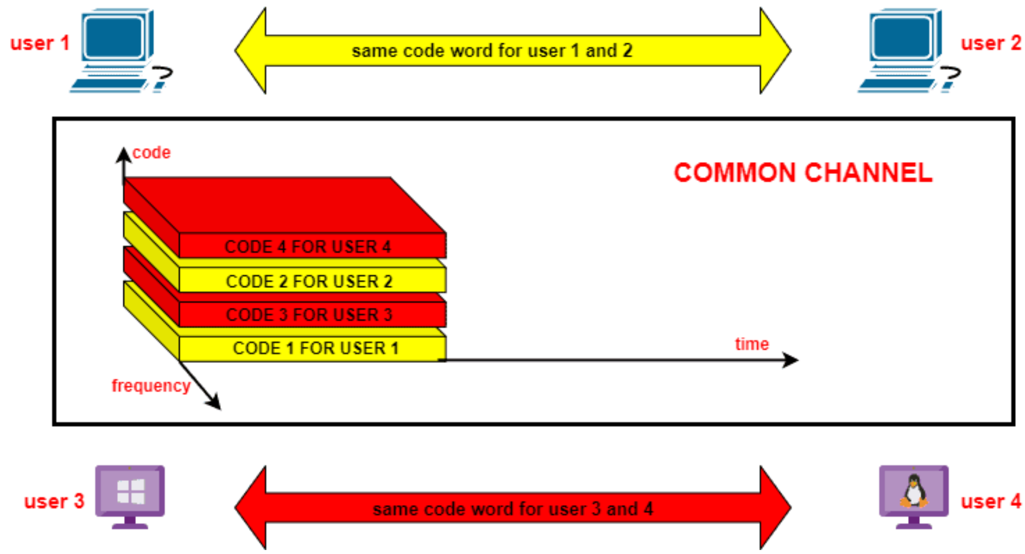


2. **Time Division Multiple Access (TDMA)**
    - The entire bandwidth is shared based on time slots, where each user gets a dedicated time interval for transmission.
    - Example: GSM mobile n



etworks.

3. **Code Division Multiple Access (CDMA)**
    - All users share the same bandwidth, but each user is assigned a unique code to differentiate their signals.
    - Example: 3G mobile networks.

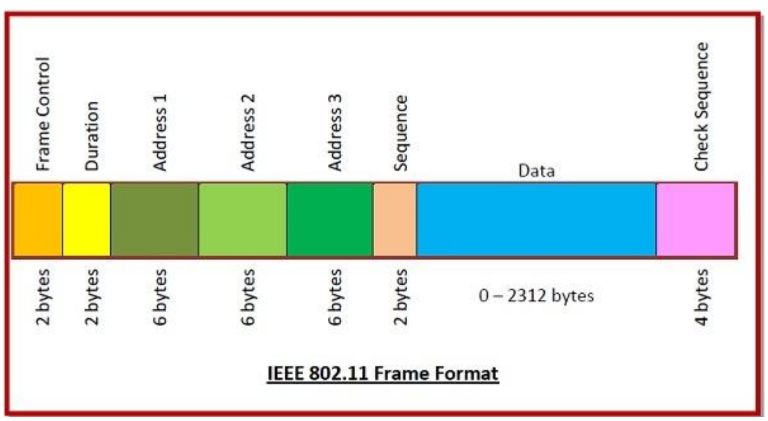


Question:

Explain the structure and components of the IEEE 802.11 frame with a diagram. (5 Marks)

Answer:

IEEE 802.11 is a standard for wireless local area networks (WLANs). The MAC (Media Access Control) frame structure in IEEE 802.11 consists of multiple fields that ensure reliable communication between wireless devices.



Frame Structure of IEEE 802.11:

The **IEEE 802.11 frame format** manages wireless communication with key fields:

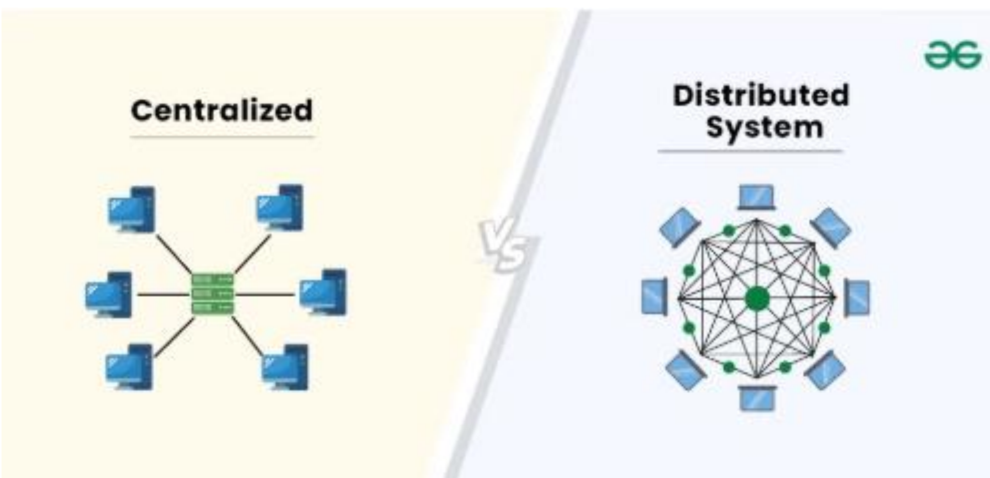
- **Frame Control (2 bytes):** Contains 11 subfields like frame type, retry, power management, and encryption.
- **Duration (2 bytes):** Specifies channel reservation time.
- **Address 1, 2, 3 (6 bytes each):** Represent receiver, sender, and final destination MAC addresses.
- **Sequence (2 bytes):** Helps in ordering frames and detecting duplicates.
- **Data (0–2312 bytes):** Carries the actual payload.
- **Frame Check Sequence (4 bytes):** Uses CRC for error detection.

Question:

What is Distributed Processing? Discuss the advantages of distributed processing over centralized processing in modern networks.

Answer:

Distributed Processing refers to a computing approach where multiple processors or computers work together to perform tasks by sharing resources and data across a network. Unlike centralized processing, where all tasks are handled by a single central computer, distributed processing divides workloads among multiple interconnected devices, improving efficiency and reliability.



Advantages of Distributed Processing Over Centralized Processing:

1. **Improved Performance:**
    - Tasks are executed in parallel, reducing processing time and increasing system efficiency.
2. **Scalability:**
    - New nodes (computers) can be added easily without affecting system performance, making it ideal for growing networks.
3. **Fault Tolerance and Reliability:**

    - If one node fails, other nodes can continue processing, ensuring system availability and minimizing downtime.
4. **Better Resource Utilization:**
    - Workloads are distributed among multiple computers, reducing the burden on a single system and optimizing resource use.
5. **Reduced Network Congestion:**
    - Since processing happens at multiple locations, data traffic is minimized, improving network speed and performance.

. **Question:**
Explain output processing in a router. How does it ensure that packets are transmitted efficiently to the next hop?

Answer:
Output processing in a router is the final stage before forwarding a packet to the next hop. It includes:

1. **Route Lookup:** Determines the outgoing interface and next-hop address.
2. **Queuing & Scheduling:** Manages packet order and priority for transmission.
3. **Traffic Shaping & Policing:** Regulates flow to prevent congestion.
4. **Encapsulation & Framing:** Formats packets for the data link layer.
5. **Physical Transmission:** Sends packets through the selected interface.

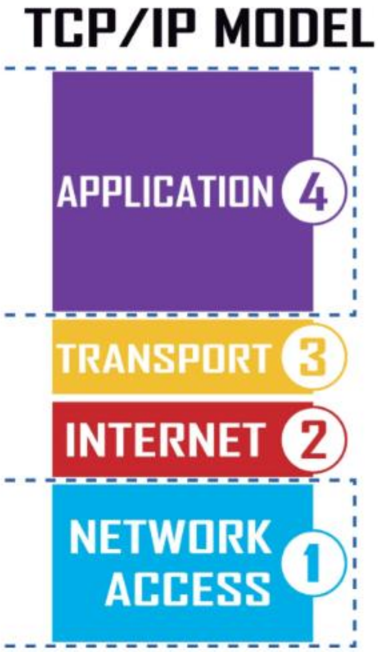
Efficient Transmission Mechanisms:

- **Buffer Management** prevents packet loss.
- **Congestion Control** (e.g., RED) avoids overload.
- **Quality of Service (QoS)** prioritizes critical packets.
- **Load Balancing** optimizes network usage.

Question:
Describe the function of the TCP/IP protocol suite. Explain the function of each layer in the suite. *(5 Marks)*

Answer:
The **TCP/IP protocol suite** is a set of communication protocols used for networking and the internet. It provides end-to-end data communication by defining how data should be formatted, transmitted, addressed, routed, and received. The TCP/IP model consists of **four layers**, each performing specific functions to ensure reliable data transmission.

Layers of the TCP/IP Model and Their Functions:



1. **Application Layer**
   - Provides network services to applications such as web browsing, email, and file transfer.
   - Includes protocols like HTTP, FTP, SMTP, DNS, and Telnet.
2. **Transport Layer**
   - Ensures reliable or connectionless data delivery between devices.
   - Uses **TCP (Transmission Control Protocol)** for reliable, connection-oriented communication and **UDP (User Datagram Protocol)** for fast, connectionless communication.
3. **Internet Layer**
   - Handles addressing, packet routing, and forwarding of data.
   - Uses protocols like **IP (Internet Protocol)** for addressing and routing, **ICMP (Internet Control Message Protocol)** for error reporting, and **ARP (Address Resolution Protocol)** for IP-to-MAC address mapping.
4. **Network Access Layer (Link Layer)**
   - Manages physical transmission of data over network hardware.
   - Includes Ethernet, Wi-Fi, and MAC (Media Access Control) protocols.

Question:

Write short notes on **ALOHA** and **Controlled Access** in the Data Link Layer. *(5 Marks)*

Answer:

ALOHA:

ALOHA is a **random access protocol** used for **medium access control (MAC)** in network communication. It allows multiple devices to transmit data without coordination, leading to possible collisions. There are two types:

1. **Pure ALOHA –** Transmissions occur at any time, causing higher collisions. Maximum efficiency is **18.4%.**
2. **Slotted ALOHA –** Time is divided into slots; devices transmit only at the beginning of a time slot, reducing collisions. Maximum efficiency is **36.8%.**

Controlled Access:

In **Controlled Access**, stations **coordinate before transmitting** to avoid collisions. It ensures efficient channel usage. The main types are:

1. **Reservation –** Stations reserve time slots before sending data.
2. **Polling –** A central controller polls each station for permission to send.
3. **Token Passing –** A token (a special control frame) circulates; a station can transmit only if it holds the token.

Comparison:

- **ALOHA** is simple but less efficient due to collisions.
- **Controlled Access** avoids collisions but requires coordination, making it more efficient for large networks.

.