Computer Network

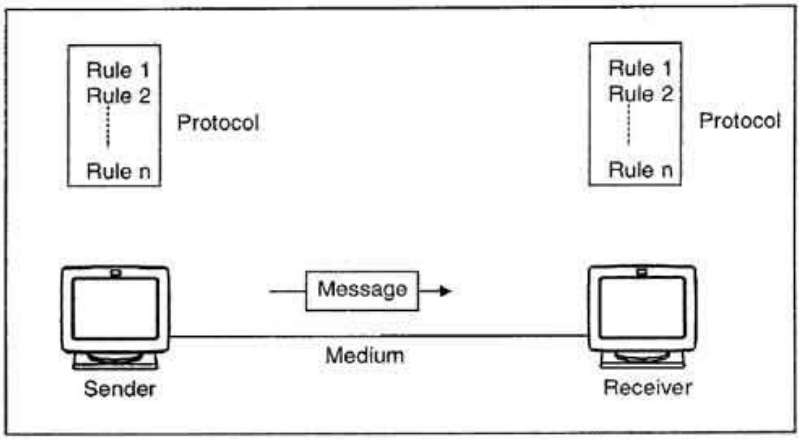
Unit 1 Questions:

Q1. What is Data Communication?

Ans. Data communications is the process of transmitting and receiving data between two devices or systems through a medium such as a wired or wireless connection. It plays a fundamental role in computer networks and is essential for information exchange.

Q2. What are components of data communications?

Ans.



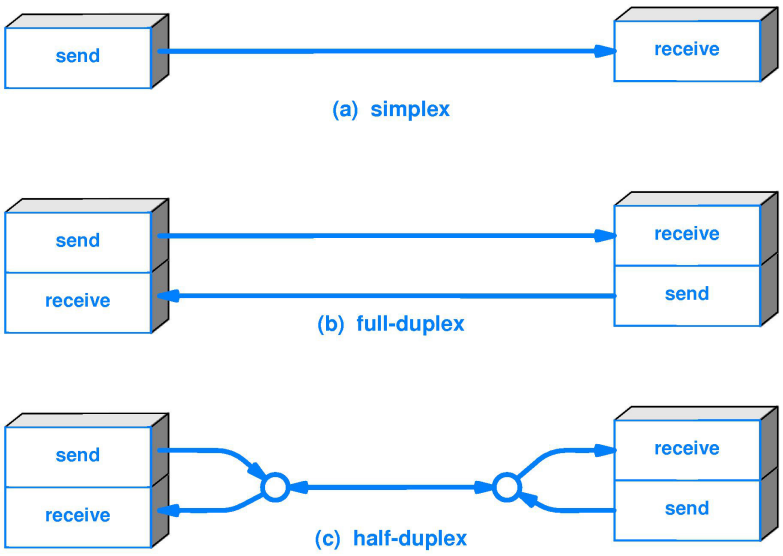
Key components of data communication include:

1. **Message**: The information (text, images, audio, video) being transmitted.
2. **Sender**: The device that initiates and encodes the message.
3. **Receiver**: The device that decodes and processes the message.
4. **Transmission Medium**: The physical or wireless path for transmitting data.
5. **Protocol**: Rules that govern data transmission to ensure successful communication.
6. **Modem**: Converts digital data to analog for transmission and back to digital on reception.
7. **Switches/Routers**: Switches connect devices in a LAN, and routers direct data between networks.
8. **Gateway**: A gateway connects networks with different protocols, allowing data to flow between them. It translates data from one network format to another
9. **Error Detection and Correction**: Ensures data integrity during transmission.

Q3. What are the different Data Transmission Modes?

Ans. Types of data Transmission include:

1. **Simplex**: Communication is unidirectional, with data flowing in one direction only (e.g., keyboards to computers).
2. **Half-Duplex**: Data can flow in both directions, but only one direction at a time (e.g., walkie-talkies).
3. **Full-Duplex**: Data flows simultaneously in both directions (e.g., phone calls, internet communication).



Q4. What are the different Data Communication?

Ans. Types of data communication can be categorized as:

1. **Analog Communication**: Data is transmitted as continuous, variable waveforms (e.g., analog telephones, AM/FM radio).
2. **Digital Communication**: Data is transmitted in discrete, binary form, commonly used in modern computer networks (e.g., digital modulation, encoding).

Q5. What are the different Data Transmission Techniques?

Ans. Data transmission techniques include:

1. **Serial Transmission**: Data is transmitted one bit at a time over a single channel (e.g., USB communication).
2. **Parallel Transmission**: Multiple bits are transmitted simultaneously across multiple channels (e.g., internal data buses in computers).
3. **Synchronous Transmission**: Data is transmitted in a continuous stream, synchronized by a clock signal.
4. **Asynchronous Transmission**: Data is transmitted one byte at a time with start and stop bits, without a continuous clock signal.
5. **Baseband Transmission**: The entire bandwidth of the channel is used to send a single signal.
6. **Broadband Transmission**: Multiple signals are transmitted simultaneously over a wide bandwidth, typically used in networks like cable TV.

Q6. What are some Data Communication Protocols?

Ans.

1. **TCP/IP**: The foundation of the internet, ensuring reliable data delivery between devices.
2. **HTTP/HTTPS**: Used for transmitting web content, with HTTPS providing secure transmission.
3. **SMTP/POP3/IMAP**: Protocols used for email communication, where SMTP sends emails, and POP3/IMAP are used for receiving and managing emails.

4. **FTP**: Protocol for transferring files between computers.

Q7. What is Network Topology?

Ans. Network topology refers to the arrangement of devices and connections within a network. It defines the layout of the network, including how devices (nodes) are interconnected and how data flows between them. Common types include bus, star, ring, mesh, and hybrid topologies.

Q8. What are Multiplexing Techniques?

Ans. Multiplexing techniques allow multiple signals to share a single communication channel. Common techniques include:

1. **Time-Division Multiplexing (TDM)**: Divides time into slots and assigns each signal a specific time slot for transmission.
2. **Frequency-Division Multiplexing (FDM)**: Divides the available bandwidth into different frequency bands, with each signal using a separate frequency.
3. **Wavelength-Division Multiplexing (WDM)**: Used in fiber optics, it separates signals using different light wavelengths.
4. **Code-Division Multiplexing (CDM)**: Assigns unique codes to each signal, allowing multiple signals to be transmitted simultaneously over the same channel.

Q9 What is Flow Control?

Ans. Flow control is a technique used in data communication to manage the rate of data transmission between sender and receiver. It ensures that the sender does not overwhelm the receiver with too much data at once, maintaining data integrity and synchronization.

Q10. What are the different network types?

Ans.

- **Local Area Network (LAN):** Covers a small geographical area, such as an office or building, typically using Ethernet technology.
- **Wide Area Network (WAN):** Connects multiple LANs over large geographical distances, often using the Internet or leased lines.
- **Metropolitan Area Network (MAN):** Falls between LAN and WAN, covering a city or large campus

Q11. Name different network topologies?

Ans.

- **Bus Topology:** All devices are connected to a single central cable.
- **Star Topology:** All devices connect to a central hub or switch.
- **Ring Topology:** Devices are connected in a circular manner, with data traveling from one device to the next.
- **Mesh Topology:** Every device is connected to every other device, providing multiple pathways for data transmission.

Q12.What are some network devices?

Ans.

- **Router:** Connects different networks and forwards data between them.
- **Switch:** Connects devices within a single network and forwards data based on MAC addresses.
- **Hub:** Broadcasts data to all devices on a network, with no filtering.
- **Gateway:** Connects networks with different protocols and translates data formats.

Q13. What are network protocols?

Ans. Network protocols are a set of rules and conventions that govern how data is transmitted over a network. They ensure the compatibility of communication between devices, enabling effective data exchange. Examples include TCP/IP, HTTP/HTTPS, and FTP.

Q14. What is network addressing?

Ans. Network addressing refers to the methods used to identify devices on a network. This includes IP addresses, which are logical addresses used for routing data, and MAC addresses, which are hardware addresses used within local networks.

Q15. What is Subnetting and CIDR?

Ans.

- **Subnetting:** The practice of dividing an IP network into smaller, manageable subnetworks to improve organization, security, and performance.
- **CIDR (Classless Inter-Domain Routing):** A method for allocating IP addresses more efficiently than traditional classful addressing, allowing for flexible subnetting.

Q16. What is DNS?

Ans. The Domain Name System (DNS) is a system that translates human-readable domain names (like www.example.com) into IP addresses, enabling users to easily locate resources on the internet.

Q17. What is Firewall?

Ans. A firewall is a security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It helps protect networks from unauthorized access and cyber threats by filtering traffic.

Q18 Write Short Note on:

a) WWW, b) ISP, c) URL, d) IP Address, e) HTTP and HTTPS.

Ans. a) **WWW (World Wide Web):**

- An information system enabling access to multimedia content over the internet.
- Uses hypertext to link documents for easy navigation through web browsers.
- Built on standard protocols like HTTP.
- Integrates text, images, videos, and interactive elements.

b) **ISP (Internet Service Provider):**

- A company that provides internet access to individuals and organizations.
- Offers services like broadband, dial-up, and fiber-optic connections.

- Facilitates internet connectivity and may provide web hosting, email, and domain registration.

c) **URL (Uniform Resource Locator):**

- The address used to access resources on the internet.
- Specifies the location of a resource and the protocol used.
- Typically includes the protocol (HTTP or HTTPS), domain name (www.example.com), and resource path (/page1).

d) **IP Address:**

- A unique numerical label assigned to each device on a network using Internet Protocol.
- Identifies the host or network interface and provides the device's location in the network.
- Can be IPv4 (e.g., 192.168.1.1) or IPv6 (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

e) **HTTP and HTTPS:**

- HTTP (Hypertext Transfer Protocol) is used for transferring data over the web.
- Defines message formatting and transmission between web servers and clients.
- HTTPS (HTTP Secure) is the secure version of HTTP, using encryption (SSL/TLS).
- Ensures confidentiality and integrity of sensitive information during transmission.

Q19. What is a protocol?

Ans. A protocol is a set of rules and conventions that govern how data is transmitted, received, and processed in a network. It ensures that devices can understand and work together effectively.

Q20 Explain TCP/IP Protocol Suite?

Ans. The TCP/IP (Transmission Control Protocol/Internet Protocol) suite is a crucial set of networking protocols that underpins the internet and most modern networks. It is organized into four primary layers, each serving specific functions in data communication. Here’s a detailed overview of the TCP/IP Protocol Suite:

1. Network Interface Layer (Link Layer)

The Network Interface Layer is the lowest layer of the TCP/IP model, focusing on the physical and data link aspects of network communication. It interacts directly with hardware and handles addressing at the MAC (Media Access Control) level.

- **Responsibilities**:
  - Manages physical connections and data transmission over the network medium.
  - Defines protocols for accessing the physical network and addressing.
- **Examples**:
  - Ethernet
  - Wi-Fi (802.11)
  - ARP (Address Resolution Protocol)

2. Internet Layer

The Internet Layer is responsible for routing packets across different networks and providing logical addressing (IP addresses) to devices. It facilitates communication between networks and ensures that data packets reach their intended destinations.

- **Responsibilities**:
    - Handles routing decisions and logical addressing.
    - Transmits data across multiple networks using IP addresses.
- **Examples**:
    - IPv4 (Internet Protocol version 4)
    - IPv6 (Internet Protocol version 6)
    - ICMP (Internet Control Message Protocol)

3. Transport Layer

The Transport Layer ensures reliable end-to-end communication between devices. It segments and reassembles data, provides flow control, and performs error detection and correction.

- **Responsibilities**:
    - Ensures reliable data transmission.
    - Manages flow control to prevent data overload.
    - Provides mechanisms for error detection and recovery.
- **Examples**:
    - TCP (Transmission Control Protocol), which is connection-oriented and ensures reliable delivery.
    - UDP (User Datagram Protocol), which is connectionless and prioritizes speed over reliability.

4. Application Layer

The Application Layer interacts directly with end-user applications and provides the necessary network services. It encompasses a wide range of protocols tailored for specific applications.

- **Responsibilities**:
    - Provides services for applications such as web browsing, email, and file transfer.
    - Facilitates communication between software applications and the underlying network.
- **Examples**:
    - HTTP (Hypertext Transfer Protocol) for web communication.
    - FTP (File Transfer Protocol) for transferring files.
    - SMTP (Simple Mail Transfer Protocol) for email transmission.

Key Points

- The TCP/IP suite is modular, allowing it to adapt to various networking technologies, making it versatile and widely utilized.
- IPv4 and IPv6 are the primary protocols at the Internet Layer, with IPv6 designed to address the limitations of IPv4 address exhaustion and to offer enhanced features.

Q21 Write some Security Standards?

Ans. **TLS/SSL (Transport Layer Security/Secure Sockets Layer):**

- Protocols that provide encryption and secure communication over a computer network.
- TLS is the successor to SSL and ensures confidentiality, integrity, and authentication of data between clients and servers.
- Commonly used in web browsers to secure HTTPS connections.

- **IPsec (Internet Protocol Security):**
- A framework for securing internet protocol (IP) communications by authenticating and encrypting each IP packet in a communication session.
- Operates at the network layer, providing end-to-end security and protecting data integrity.
- Widely used in virtual private networks (VPNs) to secure data traffic between devices over the internet.

Q22. Write short note on:

a) Web Services Standards, b) ITU-T and IEEE Standard, c) RFCs.

Ans. a) **Web Services Standards:**
Web services standards define the protocols and technologies used for communication between web services. Key standards include:

- **SOAP (Simple Object Access Protocol):** A protocol for exchanging structured information in web services.
- **WSDL (Web Services Description Language):** A XML-based language for describing the services offered by a web service.
- **UDDI (Universal Description, Discovery, and Integration):** A directory service for listing web services and enabling discovery.

b) **ITU-T and IEEE Standards:**

- **ITU-T (International Telecommunication Union - Telecommunication Standardization Sector):** Develops global telecommunications standards, covering areas like data transmission, networking, and multimedia.
- **IEEE (Institute of Electrical and Electronics Engineers):** Develops standards for electrical and electronic engineering, including networking protocols (e.g., IEEE 802 standards for local area networks).

c) **RFCs (Request for Comments):**
RFCs are a series of documents that describe specifications, protocols, and standards related to the internet. They cover a wide range of topics, including networking protocols (e.g., TCP/IP), system architectures, and application guidelines. RFCs are published by the Internet Engineering Task Force (IETF) and serve as a foundation for internet standards.

Q23. Explain OSI Model in detail.

Ans. The OSI (Open Systems Interconnection) model is a conceptual framework that helps understand and implement networking protocols across seven distinct layers. Each layer serves a specific function and interacts with the layers directly above and below it, creating a comprehensive approach to data communication.

1. Physical Layer

The **Physical Layer**, or Layer 1, is responsible for the physical connection between devices. It handles the transmission of raw bitstreams over a physical medium, which includes cables, connectors, and hardware such as switches. Standards like Ethernet and USB are part of this layer, focusing on signal encoding, transmission medium, bit rate, and physical topology.

2. Data Link Layer

Moving up, the **Data Link Layer** (Layer 2) ensures the reliable transmission of data frames between devices on the same network segment. This layer manages error detection and correction and flow control. Network interface cards, switches, and bridges operate at this layer, with protocols like Ethernet and Wi-Fi defining how data frames are structured and transmitted. Key concepts include MAC addressing, framing, and link establishment.

3. Network Layer

The **Network Layer** (Layer 3) manages the routing of data packets across multiple networks. It determines the best path for data transmission using routers and layer 3 switches. Protocols such as IP and ICMP are integral to this layer, which focuses on IP addressing, packet forwarding, and routing algorithms.

4. Transport Layer

At the **Transport Layer** (Layer 4), the focus shifts to ensuring complete data transfer with error recovery and flow control. This layer segments data into manageable chunks for transmission and uses protocols like TCP and UDP. TCP provides reliable, connection-oriented communication, while UDP is faster and connectionless, emphasizing speed over reliability.

5. Session Layer

The **Session Layer** (Layer 5) manages sessions or connections between applications. It establishes, maintains, and terminates communication sessions. This layer relies on APIs and session management software, using protocols like NetBIOS and RPC to handle session establishment and synchronization.

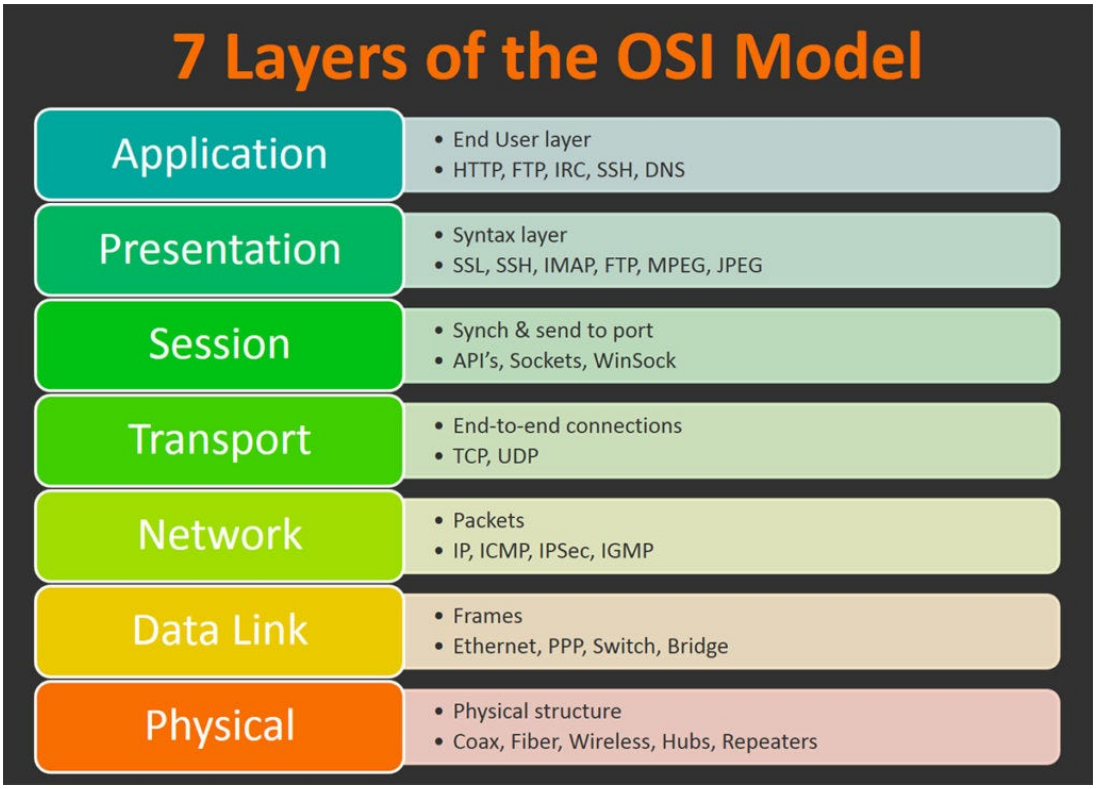
6. Presentation Layer

Next is the **Presentation Layer** (Layer 6), which translates data between the application layer and the network. It formats and encrypts data for the application layer, ensuring that the data is presented in a usable form. Standards like ASCII and TLS for encryption are part of this layer, focusing on data compression, encryption, and character encoding.

7. Application Layer

Finally, the **Application Layer** (Layer 7) provides network services to end-user applications. This layer is closest to the end user and directly interacts with software applications such as web

browsers and email clients. Protocols like HTTP, FTP, and SMTP operate at this layer, enabling user interfaces and application services to function effectively.



Q24 Write functions of each layer of an OSI Model.

Ans. **1. Physical Layer**

- **Bit Transmission**: Transmits raw bits over a physical medium.
- **Signal Encoding**: Converts digital data into signals suitable for transmission.
- **Physical Medium**: Defines the characteristics of the physical medium (cables, connectors).
- **Data Rate Control**: Determines the rate of data transmission (bit rate).
- **Topology Definition**: Specifies the layout and arrangement of network devices.

2. Data Link Layer

- **Framing**: Packages bits into frames for error detection and correction.
- **Error Detection and Correction**: Identifies and corrects errors in transmitted frames.
- **Flow Control**: Manages the rate of data transmission between devices.
- **MAC Addressing**: Assigns and recognizes unique hardware addresses for devices on the same local network.
- **Link Establishment**: Initiates and terminates communication links between devices.

3. Network Layer

- **Routing**: Determines the optimal path for data packets across multiple networks.

- **Logical Addressing**: Provides logical addressing (IP addresses) to devices for identification on a network.
- **Packet Forwarding**: Forwards data packets based on routing decisions.
- **Fragmentation and Reassembly**: Divides packets into smaller fragments for transmission and reassembles them at the destination.
- **Traffic Control**: Manages network congestion and data flow.

4. Transport Layer

- **Segmentation**: Divides data into smaller segments for transmission.
- **Connection Control**: Establishes, maintains, and terminates connections between devices.
- **Reliability**: Ensures reliable data delivery through error recovery and retransmission (e.g., TCP).
- **Flow Control**: Regulates data transmission rates between sender and receiver.
- **Multiplexing**: Allows multiple applications to use the network simultaneously.

5. Session Layer

- **Session Establishment**: Initiates and maintains sessions between applications.
- **Session Management**: Controls dialog between applications (half-duplex or full-duplex).
- **Synchronization**: Coordinates data exchange and maintains data consistency.
- **Session Termination**: Closes communication sessions when data exchange is complete.

6. Presentation Layer

- **Data Translation**: Converts data formats (e.g., from EBCDIC to ASCII).
- **Data Compression**: Reduces the size of data to optimize bandwidth usage.
- **Data Encryption**: Protects data by converting it into a secure format for transmission.
- **Character Code Translation**: Ensures that character encoding is compatible between different systems.

7. Application Layer

- **User Interface**: Provides interfaces for user interaction with network services.
- **Application Services**: Facilitates services such as email, file transfer, and web browsing.
- **Protocol Support**: Implements application-level protocols (e.g., HTTP, FTP, SMTP).
- **Data Formatting**: Prepares data for application use, ensuring it is in a readable format.
- **End-User Communication**: Manages communication between user applications and lower OSI layers.

Q25. Do comparison of TCP/IP and OSI model.

Ans. The TCP/IP and OSI models are both frameworks that describe how data is transmitted across networks. While they serve similar purposes, they differ significantly in structure and approach. Here's a comparison of the two models:

1. Structure

- **TCP/IP Model**: The TCP/IP model has four layers:
    1. **Network Interface Layer** (Link Layer)
    2. **Internet Layer**

3. **Transport Layer**
4. **Application Layer**

- **OSI Model**: The OSI model has seven layers:
  1. **Physical Layer**
  2. **Data Link Layer**
  3. **Network Layer**
  4. **Transport Layer**
  5. **Session Layer**
  6. **Presentation Layer**
  7. **Application Layer**

2. Layer Functionality

- **TCP/IP Model**:
  - Combines functionalities of several OSI layers. For example, the Network Interface Layer encompasses both the Physical and Data Link Layers of OSI.
  - Focuses more on the protocols used rather than the layers themselves.
- **OSI Model**:
  - Clearly separates functionalities into seven distinct layers, allowing for modular design.
  - Each layer has specific responsibilities, making it easier to understand the role of each part of the communication process.

3. Protocol Dependency

- **TCP/IP Model**:
  - Protocols are integral to the model. It was designed specifically for the Internet, with protocols such as TCP and IP as foundational elements.
  - Emphasizes the importance of protocol functionality over strict adherence to layers.
- **OSI Model**:
  - Designed as a theoretical model, it does not specify protocols. Various protocols can be mapped to each layer.
  - Provides a standard for different types of network protocols to interact.

4. Development and Adoption

- **TCP/IP Model**:
  - Developed in the 1970s by ARPANET, it gained prominence due to the rapid growth of the Internet.
  - Widely adopted in practical applications and forms the basis of Internet communication.
- **OSI Model**:
  - Developed by the International Organization for Standardization (ISO) in the late 1970s and early 1980s.

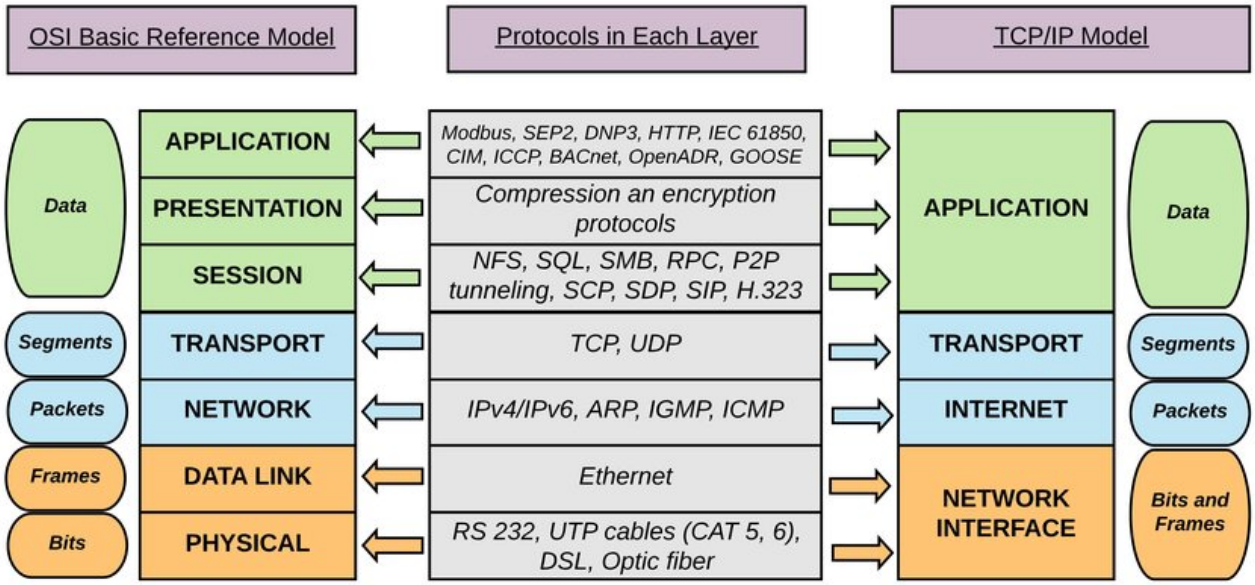
- While it is a comprehensive framework, it is less frequently used in practice compared to TCP/IP.

5. Data Transmission

- **TCP/IP Model**:
  - Prioritizes the transmission of data packets. The Internet Layer is responsible for routing packets across different networks.
  - Utilizes connection-oriented (TCP) and connectionless (UDP) transport methods.
- **OSI Model**:
  - Emphasizes both the connection setup and data flow management through its layered structure.
  - Contains layers like the Session and Presentation layers, which are not explicitly addressed in the TCP/IP model.

6. Complexity

- **TCP/IP Model**:
  - Generally considered simpler and more efficient due to its fewer layers.
  - Less formal in terms of structure, which can lead to practical implementation challenges.
- **OSI Model**:
  - More complex with its seven layers, which can provide clarity and separation of concerns.
  - Can be seen as more theoretical, leading to potential overhead in practical applications.



Q26. What is Addressing? Write Short note on: a) MAC Address, b) Port Number, c) Subnet Mask, d) Logical Addressing, e) Public and Private Addresses.

Ans. Addressing in networking refers to the methods and techniques used to identify devices and facilitate communication within a network. Proper addressing ensures that data packets can be

correctly routed to their intended destinations, enabling effective data transmission. Here's a short note on various addressing types:

a) MAC Address

A MAC (Media Access Control) address is a unique identifier assigned to network interfaces for communication on the physical network segment. It is a 48-bit address usually represented in hexadecimal format. MAC addresses operate at the Data Link layer of the OSI model and are used for local network communication. Since MAC addresses are hardcoded into the hardware, they are static and do not change, making them essential for identifying devices on a LAN.

b) Port Number

A port number is a numerical label assigned to specific processes or services on a device, allowing multiple applications to use network resources simultaneously. Port numbers range from 0 to 65535, with well-known ports (0-1023) designated for common services like HTTP (80), FTP (21), and SMTP (25). Port numbers operate at the Transport layer of the OSI model and help direct data to the appropriate application or service on a device.

c) Subnet Mask

A subnet mask is a 32-bit address that divides an IP address into a network and host portion, helping to identify which part of the IP address is used for the network and which part is used for individual devices. The subnet mask determines the number of available addresses within a subnet, enabling efficient IP address management. Common subnet masks include 255.255.255.0 (for Class C networks) and 255.255.0.0 (for Class B networks).

d) Logical Addressing

Logical addressing refers to the use of IP addresses, which are assigned to devices within a network to identify them uniquely. Unlike MAC addresses, which are fixed to a device, logical addresses can change as devices move between networks. Logical addressing operates at the Network layer of the OSI model and is crucial for routing data packets across different networks, facilitating communication over the internet.

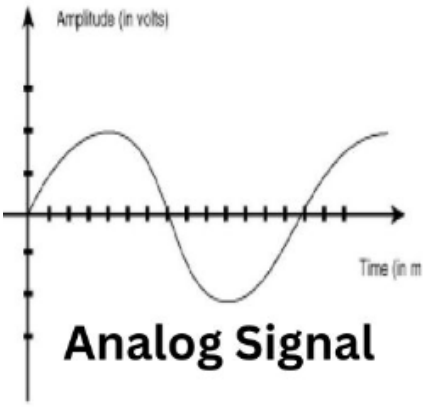
e) Public and Private Addresses

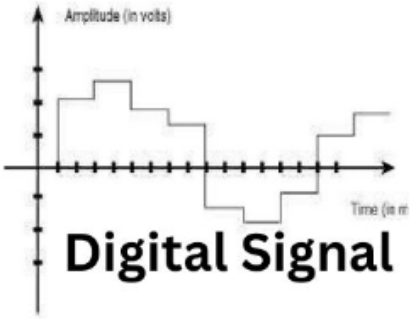
Public addresses are IP addresses that are globally unique and can be accessed over the internet. They are assigned by the Internet Assigned Numbers Authority (IANA) and are routable on the internet. Examples include IP addresses like 192.0.2.1.

Private addresses, on the other hand, are used within local networks and are not routable on the internet. They provide a way for devices to communicate within a private network while conserving public IP addresses. Examples of private address ranges include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.

Q27. Compare between Analog and Digital Signals.

Ans.

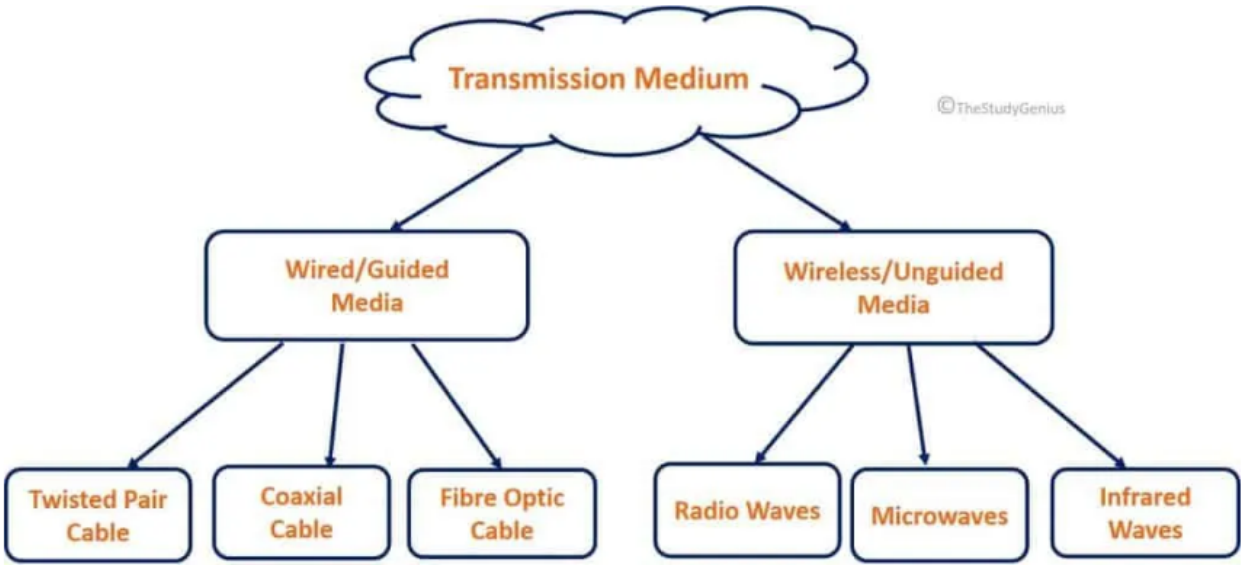




Header label	Analog Signal	Digital Signal
Signal	1) In an Analog, signals are continuous.	1) In a Digital, Signals are discrete.
Transformation	2) In analog systems electronic circuits are used for the transformation of signals.	2) In Digital Signals, the transformation is done using the logic circuit.
Transmission	3) Data transmission is not of high quality.	3) Data transmission has high quality.
Flexibility	4) In an Analog signal, their hardware is not flexible.	4) In Digital signals, their hardware is not flexible.
Noise	5) Analog signals are more likely to get affected and result in reduced accuracy.	5) Digital signals are discrete time signals that are generated by digital modulation.
Power Consumptions	6) Analog signals use more power.	6) Digital signals use less power compared to analog.
Waves	7) It is denoted by the sine waves.	7) It is denoted by the square form.
Example	8) Human Voice, Tape recorder, Temperature, etc.	8) Mp3 players, Digital phones, computers, etc.

Q28. What are the transmission Media used?

Ans.



Guided Media

Guided media involve physical pathways that direct the transmission of data signals along a specific route. Examples include:

1. **Twisted Pair Cable**

- **Unshielded Twisted Pair (UTP)**: Used in Ethernet networks; cost-effective and easy to install.
- **Shielded Twisted Pair (STP)**: Provides shielding against electromagnetic interference; used in environments with high interference.

2. **Coaxial Cable**
    - Comprises a central conductor, insulation, a metallic shield, and an outer insulating layer. It offers better protection against interference and is commonly used for cable television and broadband internet connections.
3. **Fiber Optic Cable**
    - Transmits data as light signals through thin strands of glass or plastic fibers. Offers high bandwidth and long-distance transmission with minimal signal loss, immune to electromagnetic interference. Commonly used in high-speed internet connections and data centers.

Unguided Media

Unguided media transmit data signals through the air or space without a physical medium, allowing for more flexible and mobile communication. Examples include:

1. **Wireless Transmission**
    - **Wi-Fi**: Utilizes radio waves to connect devices in local area networks.
    - **Bluetooth**: Enables short-range communication between devices.
    - **Cellular Networks**: Provide wireless communication over wide areas using cellular towers.
2. **Infrared Transmission**
    - Uses infrared light to transmit data over short distances; commonly used in remote controls and certain wireless devices. Requires a line-of-sight connection.
3. **Microwave Transmission**
    - Utilizes high-frequency radio waves for long-distance communication. Typically requires line-of-sight between transmission towers, commonly used in point-to-point communication.

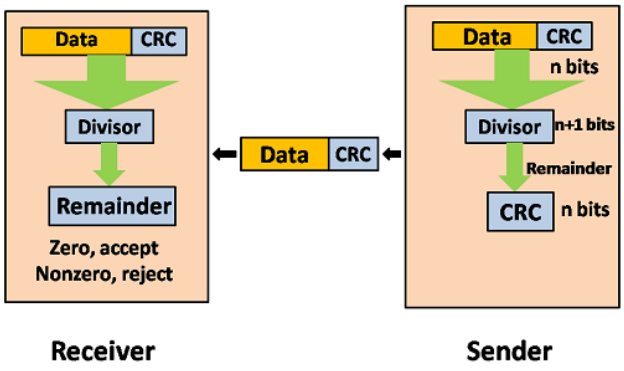
Q29. Write down the different Error Detection and Correction Codes.

Ans. Error Detection

1. **Parity Bit:**
    - **Description:** A parity bit is a basic error detection method where an extra bit is added to a data word (usually 7 or 8 bits) to ensure the total number of 1s is even (even parity) or odd (odd parity). If the parity bit does not match the received data, an error is detected.
    - **Use:** Commonly utilized in memory systems and basic communication protocols.
2. **Cyclic Redundancy Check (CRC):**
    - **Description:** CRC is a more advanced error detection technique that employs polynomial division to generate a checksum, which is appended to the data. The

receiver performs the same calculation to verify if the received checksum matches the calculated one. A mismatch indicates an error.

- **Use:** Frequently used in network communication and data storage systems.



Error Correction

1. **Hamming Code:**
    - **Description:** Hamming codes are error-correcting codes that add redundant bits to the data in such a way that they can correct single-bit errors and detect two-bit errors.
    - **Use:** Commonly applied in computer memory systems and data transmission scenarios where error correction is critical.
2. **Reed-Solomon Code:**
    - **Description:** Reed-Solomon codes are versatile error correction codes capable of correcting multiple errors and are particularly resilient.
    - **Use:** Widely used in data storage and transmission applications, including CDs, DVDs, and QR codes.
3. **Turbo Codes and LDPC (Low-Density Parity-Check) Codes:**
    - **Description:** These sophisticated error correction codes are employed in modern wireless communication and satellite transmission. They provide highly efficient error correction capabilities.
    - **Use:** Applied in 4G and 5G mobile networks, deep-space communication, and high-speed internet connections.

Q30. Explain Circuit switching in Detail.

Ans. Circuit switching is a fundamental communication technique that establishes a dedicated path between two devices in a network for the duration of their communication. This method is widely recognized in traditional telephone networks and can take various forms to meet different communication requirements. Here's a detailed overview of circuit switching methods:

1. Space-Division Circuit Switching

Description: Space-division circuit switching establishes a dedicated physical pathway, or circuit, between the calling and receiving devices. This means a physical connection is maintained for the entire duration of the communication, even if no data is actively being transmitted.

Use: This approach is often found in early telephone networks and some legacy communication systems. It provides a straightforward and reliable connection, making it suitable for voice communication where a continuous link is essential.

2. Time-Division Circuit Switching

Description: Time-division circuit switching allocates the communication channel into discrete time slots. Each user is assigned a specific time slot during which they can transmit data. This allows multiple users to share the same channel through time-division multiplexing (TDM), making efficient use of the available bandwidth.

Use: Time-division circuit switching is more efficient than space-division switching because it allows several users to share the same channel. This method is commonly used in digital telephone networks, such as T1 and E1 lines, as well as in various legacy systems.

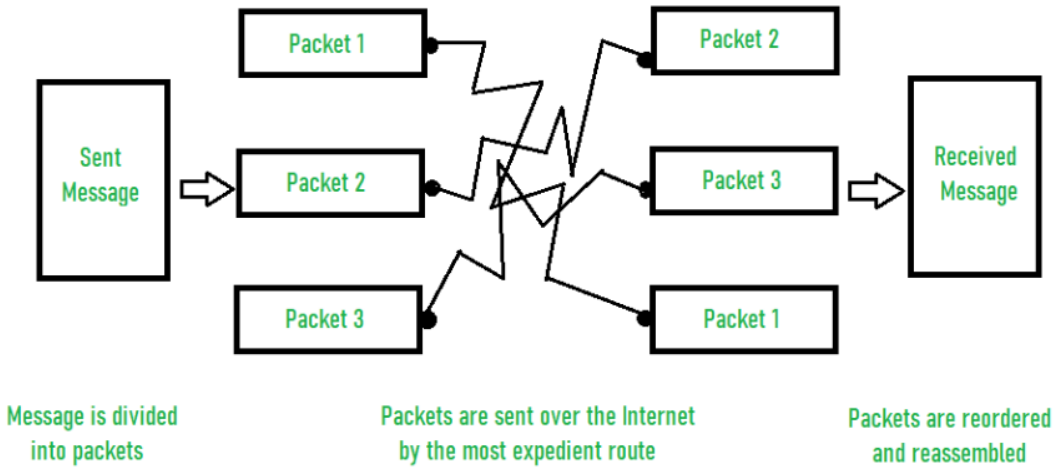
3. Space-Time Division Circuit Switching

Description: Space-time division circuit switching integrates both space-division and time-division techniques. It utilizes a combination of physical pathways and time slots to create dedicated connections, allowing for greater flexibility and efficiency in managing network resources.

Use: This method is applied in complex telecommunication systems that require both spatial and temporal division capabilities, facilitating a more efficient use of network infrastructure while accommodating multiple simultaneous connections.

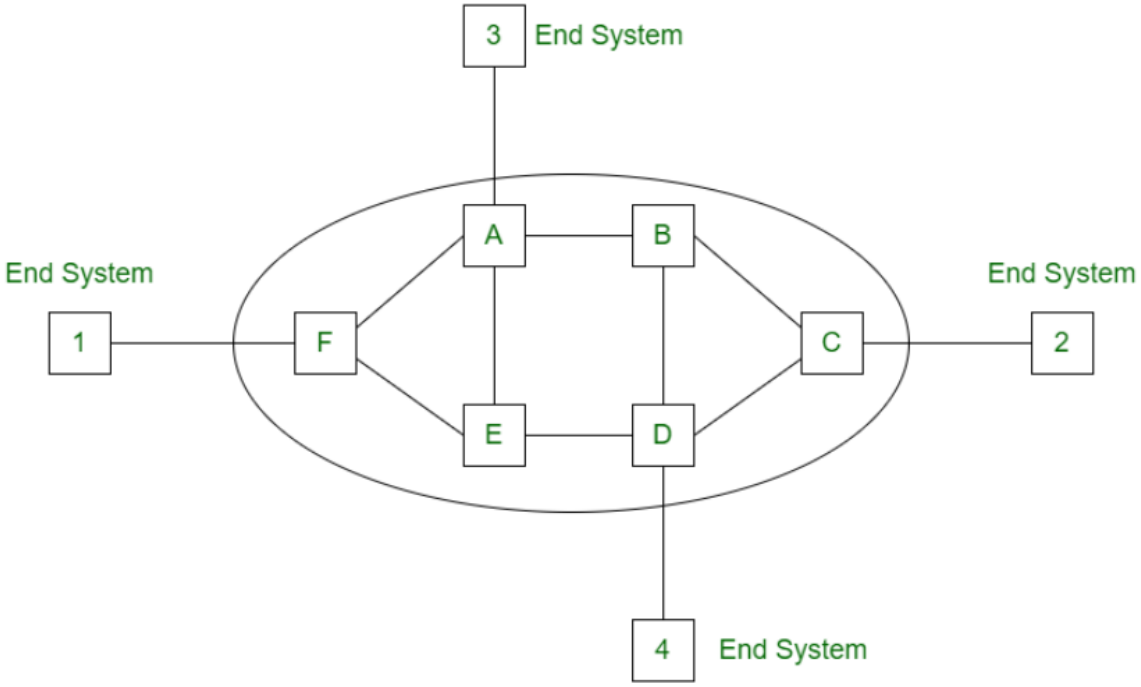
Q31. Explain the Packet Switching.

Ans. Packet switching is a fundamental technique in data communication, especially in modern computer networks. It involves dividing data into smaller units called packets and routing these packets independently to their destination. Two common approaches to packet switching are the virtual circuit approach and the datagram approach.



Virtual Circuit Approach

1. **Description:** In the virtual circuit approach, a logical path, known as a "virtual circuit," is established prior to data transmission. This method resembles circuit switching, where a dedicated circuit is created, but instead of a physical connection, it utilizes a logical connection.
2. **Characteristics:**
    - **Setup Phase:** Before any data is transmitted, a connection is established. During this phase, a route is determined, and network resources are allocated for the duration of the connection.
    - **Connection Identifier:** Each packet is tagged with a connection identifier, which simplifies the routing process.
    - **Sequencing and Flow Control:** Packets can be sent in a predetermined order, making sequencing and flow control more straightforward.
3. **Use:** The virtual circuit approach is employed in technologies like Frame Relay and ATM (Asynchronous Transfer Mode) networks. It is particularly useful when a stable, predictable connection is needed, allowing for more reliable data transmission.

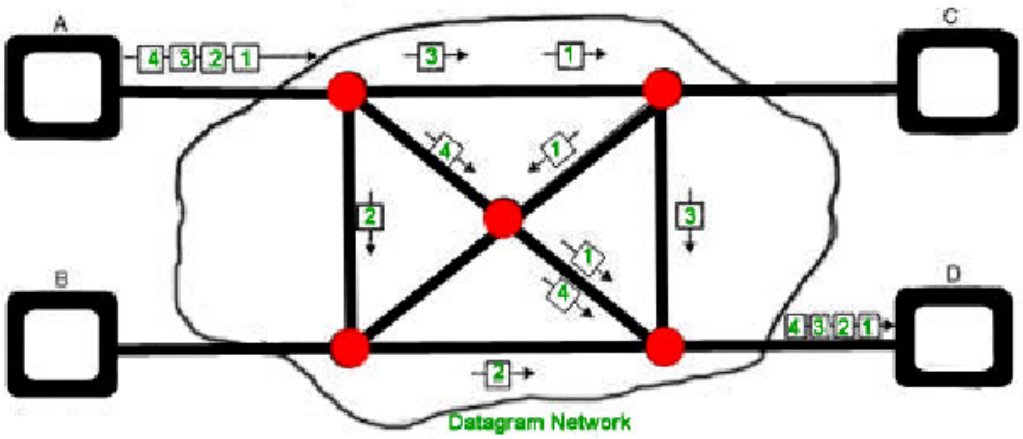


Datagram Approach

1. **Description:** In the datagram approach, each packet is treated as an independent entity. There is no prior establishment of a connection or a predefined route; instead, packets are routed based solely on the destination address contained within each packet.
2. **Characteristics:**
    - **No Setup Phase:** Unlike the virtual circuit approach, there is no initial connection setup. Each packet is self-contained and includes its destination information for routing.

- **Independent Routing:** Packets can take different paths to reach the destination. This characteristic allows for greater network redundancy, as alternative routes can be utilized in case of congestion or failures in certain paths.
- **Flexibility and Challenges:** The datagram approach offers greater flexibility in routing but may lead to challenges such as out-of-order delivery or packet loss. Each packet may arrive at the destination at different times, necessitating mechanisms at higher layers to manage these issues.

3. **Use:** The datagram approach forms the backbone of the Internet Protocol (IP) and is fundamental to both the global internet and local area networks (LANs). It enables efficient and robust communication across diverse and dynamic network environments.



Datagram Packet Switching

Q32. Explain Message Switching.

Ans. Message switching is a communication technique that predates modern packet switching and circuit switching. It involves the transmission of complete messages or data units rather than breaking data into smaller packets, as seen in packet switching. Here's a detailed overview of message switching:

1. **Message-Based Communication:** In message switching, the entire message is treated as a single unit of data for transmission. This message can be of arbitrary size and may contain various forms of data, such as text or voice. Each message can include routing information to help guide its path through the network.

2. **Store-and-Forward Process:** When a sender wishes to transmit a message to a receiver, the message is first stored at the source node. The source node then forwards the entire message to the next hop in the network. Each node in the network stores the complete message before forwarding it, hence the term "store-and-forward."

3. **Message Handling:** Message switching networks utilize message switches, specialized devices responsible for routing, storing, and forwarding messages. Each message switch examines the routing information within the message to determine the next destination.

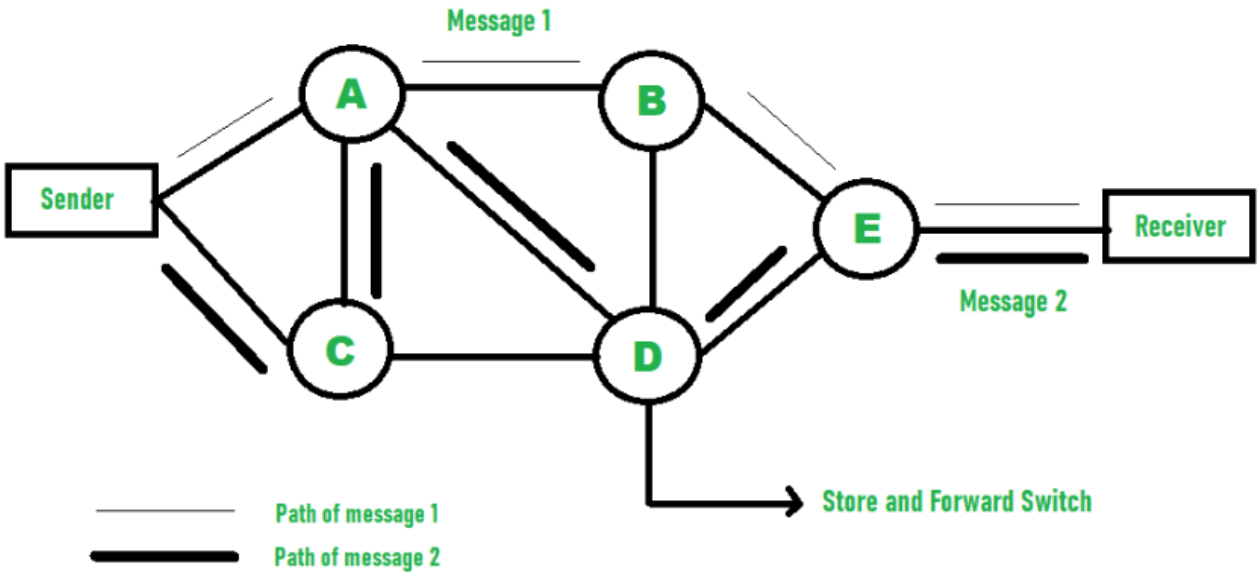
4. **Message Queuing:** Messages may need to wait in queues at each node if the next hop is unavailable immediately. This queuing mechanism can introduce delays in the transmission process.

5. **Completion-Based Communication:** In message switching, the sender considers the transmission successful only when the entire message reaches its destination. There is no division of data into packets or datagrams, unlike packet switching.

Advantages and Disadvantages:

- **Advantages:**
    - **Simplicity:** Message switching is conceptually straightforward, as it operates on complete messages.
    - **Suitability for Low-Data-Rate Applications:** It can be efficient for low-volume, store-and-forward applications.
- **Disadvantages:**
    - **Inefficiency:** Message switching can be inefficient for handling large volumes of data, as the entire message must be stored and forwarded.
    - **Longer Delays:** Due to the store-and-forward process and message queuing, this technique can introduce longer delays compared to packet switching.
    - **Lack of Scalability:** It is not as scalable or adaptable as packet switching for modern, high-speed networks.

Message switching was more prevalent in earlier communication networks, such as early telegraph and telex systems. However, it has largely been supplanted by packet switching, which offers greater efficiency, flexibility, and speed in handling data communications today.



Q33. Difference between Message and Packet Switching.

Ans.

Aspect	Message Switching	Packet Switching
Data Unit	A complete message is passed across a network.	Message is broken into smaller units known as Packets.
Data Representation	Uses computer languages like ASCII, Baudot, Morse code.	In packet switching, binary data is used.
Block Size	There is no limit on block size.	Packet switching places a tight upper limit on block size.
Message Location	A message exists in only one location in the network.	Parts (i.e., packets) of the message exist in many places in the network.
Examples	Hop-by-hop Telex forwarding and UUCP (UNIX-to-UNIX Copy Protocol).	Examples include Frame Relay, IP (Internet Protocol), and X.25.
Link Allocation	Physical links are allocated dynamically.	Virtual links are made simultaneously.
Storage Location	Access time is reduced due to an increase in performance as packets are stored on disk.	Packets are stored in main memory.

Q34. Mention any two different Modes of wireless communication.

Ans. Two different modes of wireless communication are:

1. **Broadcast Mode**:
    - In this mode, a single sender transmits data to multiple receivers within a specified range. The communication is typically one-to-many, meaning that all devices within the broadcast range can receive the same message. This mode is commonly used in radio and television broadcasting.
2. **Point-to-Point Mode**:
    - This mode involves direct communication between two specific devices. It is a one-to-one communication setup where data is sent from one device to another without interference from other devices. Examples include Wi-Fi connections between a laptop and a router or cellular communication between two mobile phones.

Q35. Mention any two addressing schemes used in an internet employing the TCP/IP protocols.

Ans. Two addressing schemes used in an internet employing the TCP/IP protocols are:

1. **IP Addressing**:
    - Each device on a network is assigned a unique Internet Protocol (IP) address, which can be IPv4 or IPv6. This address identifies the device's location on the network and is essential for routing data packets to the correct destination.
2. **Port Addressing**:
    - In addition to an IP address, a port number is used to identify specific processes or services on a device. This allows multiple applications to run on the same IP address

but use different port numbers for communication, such as HTTP using port 80 and FTP using port 21.

Q36. Explain principles of optical fibre communication and briefly describe its different modes.

Ans. **Principles of Optical Fiber Communication**
Optical fiber communication transmits data as light pulses through a fiber optic cable. It uses total internal reflection to guide the light through the core of the fiber, minimizing loss and allowing high-speed, long-distance communication. A transmitter converts electrical signals into light pulses, which are then transmitted through the optical fiber and converted back into electrical signals at the receiver.
Different Modes of Optical Fiber:

1. **Single-mode Fiber**:
    - Uses a very narrow core (around 8-10 microns) to allow light to travel in a single path. It supports high bandwidth and long-distance transmission, commonly used in telecommunications and internet backbone networks.
2. **Multi-mode Fiber**:
    - Has a larger core (50-62.5 microns), allowing multiple light paths or modes to travel simultaneously. It is used for shorter distances, like within data centers or local area networks, due to higher dispersion and signal loss over long distances.

Q37. What is the concept of redundancy in error detection?

Ans. Redundancy in error detection refers to adding extra bits or information to the original data to detect errors during transmission. These extra bits do not carry useful data but help the receiver identify any errors by checking if the redundant information aligns with the expected values. Common techniques include parity bits, checksums, and cyclic redundancy checks (CRC).

Q38. Difference between Circuit Switching and Packet Switching.

Ans.

Circuit Switching	Packet Switching
In-circuit switching has there are 3 phases: i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place.
In-circuit switching, each data unit knows the entire path address which is provided by the source.	In Packet switching, each data unit just knows the final destination address intermediate path is decided by the routers.
In-Circuit switching, data is processed at the source system only	In Packet switching, data is processed at all intermediate nodes including the source system.
The delay between data units in circuit switching is uniform.	The delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because the path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources is more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source.	Transmission of the data is done not only by the source but also by the intermediate routers.
Congestion can occur during the connection establishment phase because there might be a case where a request is being made for a channel but the channel is already occupied.	Congestion can occur during the data transfer phase, a large number of packets comes in no time.

Q39. **Give two advantages of using optical fiber cable compared to coaxial cable.**

1. **Higher Bandwidth**: Optical fiber provides significantly higher data transmission rates.
2. **Less Signal Loss**: It has lower attenuation, resulting in less signal loss over long distances.

Q40. **For ‘n’ devices in a network, what is the number of cable links required for mesh, ring, bus, and star topology?**

- **Mesh**: n(n−1)2\frac{n(n-1)}{2}2n(n−1)
- **Ring**: nnn
- **Bus**: 1 shared cable
- **Star**: nnn cables (one per device)

Q41. **Explain the role of Repeater.**

A repeater amplifies or regenerates signals to extend the transmission distance in a network by compensating for signal loss and degradation.

Q42. **Explain the difference between an Internal draft and a proposed standard.**

- **Internal Draft**: A preliminary version of a standard, still being reviewed within an organization.
- **Proposed Standard**: A more formal version submitted to a standards body for public review and approval.

Q43. **In ring topology, what happens if one of the stations is unplugged?**

If one station is unplugged, the entire network may fail as the signal cannot circulate, breaking the communication loop.

Q44. **Explain why collision is a problem in random access protocol but not in controlled access protocol.**

- **Random Access**: Multiple devices transmit simultaneously, leading to collisions.
- **Controlled Access**: Devices take turns or are managed by a central authority, avoiding collisions.

Q45. **How does a single bit error differ from a burst error?**

- **Single Bit Error**: Only one bit in the data frame is corrupted.
- **Burst Error**: Multiple consecutive bits are corrupted.

Q46. **Describe the need for switching.**

Switching is needed to efficiently route data between multiple devices in a network, ensuring that the data reaches the correct destination while optimizing network resources.

Q47. **Why is channel allocation a difficult task?**

Channel allocation is difficult due to limited bandwidth, varying network demand, the need to avoid interference, and balancing efficient resource usage while ensuring fair access to all devices.