COMPUTER NETWORKS

UNIT-I

COMPONENTS OF DATA COMMUNICATION

Data communication involves the transmission of data between devices or systems using various components and protocols. These components work together to ensure that data is accurately and efficiently transmitted from a sender to a receiver. Here are the key components of data communication:

1. Sender/Transmitter:

The sender, also known as the transmitter, is the device that initiates the data communication process. It converts the data into a suitable format for transmission. This could be a computer, smartphone, sensor, or any other device capable of generating and sending data.

2. Message:

The message is the actual data that needs to be transmitted from the sender to the receiver. It can be in the form of text, numbers, images, audio, video, or any other type of digital information.

3. Encoding:

Before transmission, the message is encoded into a format suitable for transmission over the chosen communication channel. Encoding involves converting the original data into a standardized format that can be easily transmitted and decoded by the receiver. Common encoding schemes include ASCII, Unicode, and various binary formats.

4. Transmission Medium/Channel:

The transmission medium is the physical or logical pathway through which the encoded data travels from the sender to the receiver. There are various types of transmission media, such as:

- Guided Media: These are physical pathways that guide the signal, such as twisted-pair cables, coaxial cables, and fiber-optic cables.

- Unguided Media: These are wireless transmission paths that do not require physical cables, such as radio waves, microwaves, and infrared signals.

5. Modemulation (Modulation and Demodulation):

In many cases, the transmission medium carries analog signals, while digital data is in a binary format. Modulation is the process of superimposing the digital signal onto an analog carrier signal, making it suitable for transmission over the medium. At the receiver's end, demodulation extracts the original digital signal from the modulated carrier signal.

6. Receiver:

The receiver is the device that captures the transmitted signal from the medium, extracts the encoded data, and prepares it for further processing. The receiver then decodes the data to its original format for interpretation.

7. Decoding:

Decoding is the process of converting the encoded data back into its original format. This involves reversing the encoding process performed by the sender. The decoded data is then ready for use by the receiver.

8. Protocols:

Communication protocols are sets of rules and conventions that define how data is exchanged between sender and receiver. They ensure that data is transmitted correctly, efficiently, and in a structured manner. Protocols cover aspects such as error detection and correction, data flow control, addressing, and synchronization. Examples of communication protocols include TCP/IP (Transmission Control Protocol/Internet Protocol) for the internet and Bluetooth for wireless devices.

9. Error Detection and Correction:

Data transmission can introduce errors due to various factors such as noise, interference, or signal attenuation. Error detection techniques, such as checksums or cyclic redundancy checks (CRC), help identify errors in the received data. Error correction techniques, such as Forward Error Correction (FEC), allow the receiver to correct certain types of errors without the need for retransmission.

10. Acknowledgments and Flow Control:

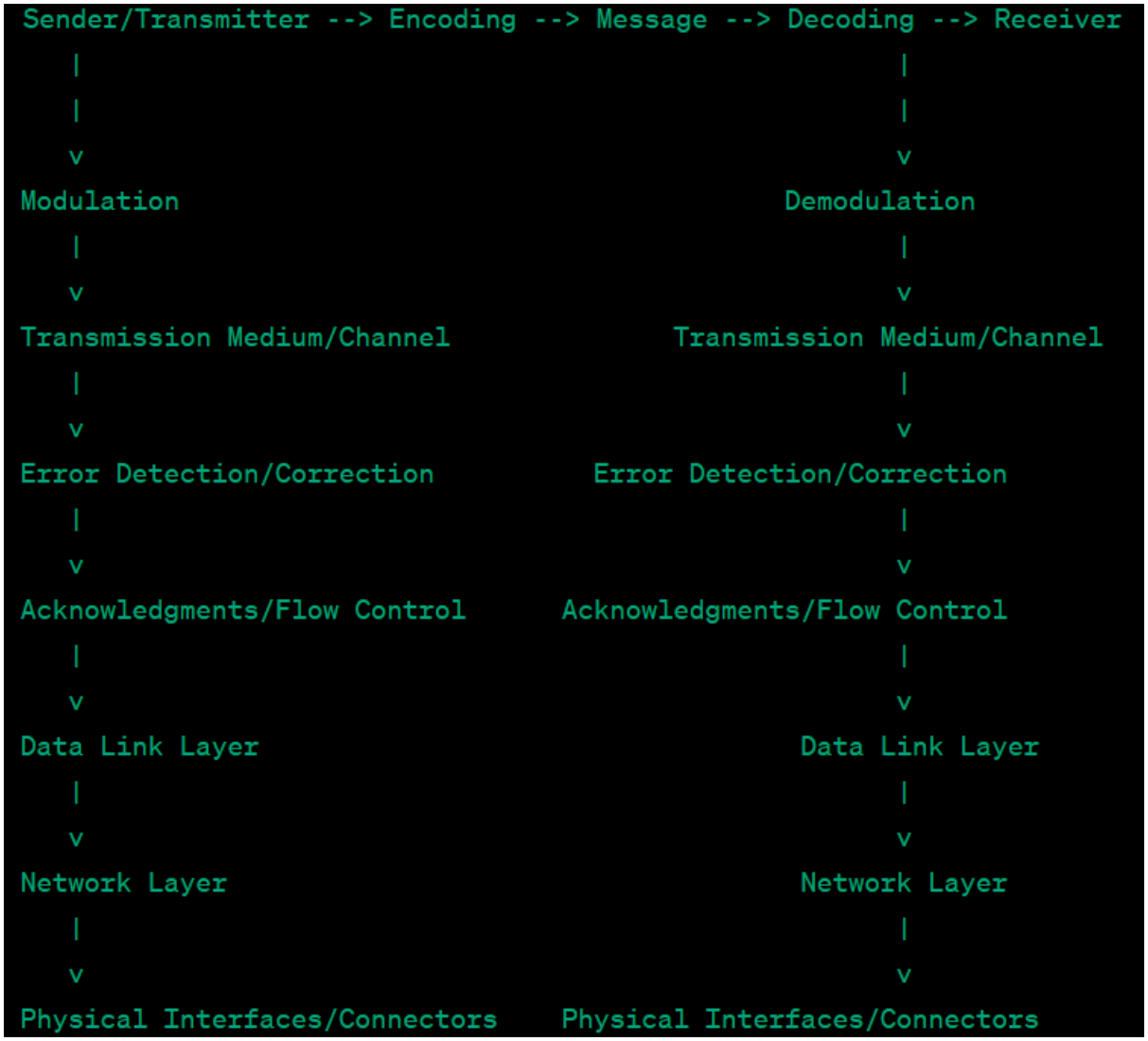
Acknowledgment mechanisms ensure that the receiver informs the sender about the successful receipt of data packets. Flow control mechanisms manage the rate of data transmission to prevent overwhelming the receiver with more data than it can handle.

11. Data Link and Network Layers:

In layered communication architectures like the OSI model, the data communication process is divided into different layers, each responsible for specific functions. The data link layer handles the framing of data into frames for transmission, as well as error detection and correction within a local network. The network layer deals with routing data between different networks.

12. Physical Interfaces and Connectors:

The physical interfaces and connectors are the hardware components that physically connect devices to the transmission medium. Examples include Ethernet ports, USB ports, HDMI connectors, and wireless antennas.

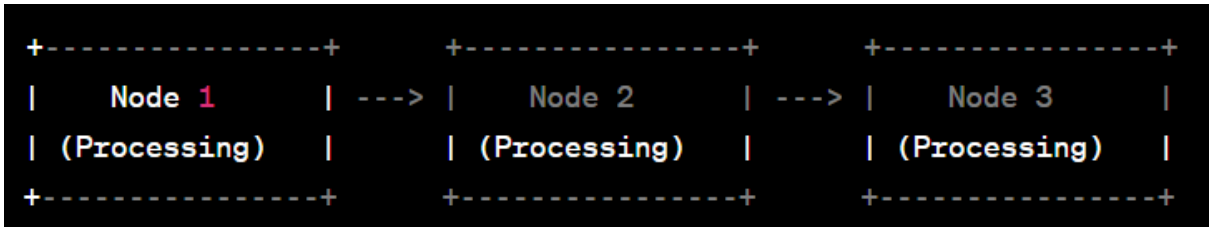


DISTRIBUTED PROCESSING:

Distributed processing refers to a computing model in which tasks or processes are divided and distributed across multiple interconnected computers or nodes. These nodes work together to solve a problem or execute a task, often in parallel, to achieve higher processing power, improved performance, and increased fault tolerance. The primary goal of distributed processing is to harness the combined computational resources of multiple machines to tackle complex problems efficiently. This concept is commonly used in cloud computing, grid computing, and cluster computing environments.

Key Features of Distributed Processing:

- Parallelism: Multiple nodes work on different parts of a task simultaneously.
- Scalability: Additional nodes can be easily added to handle increased workloads.
- Fault Tolerance: If one node fails, other nodes can continue processing.
- Resource Sharing: Nodes share resources like memory, storage, and processing power.

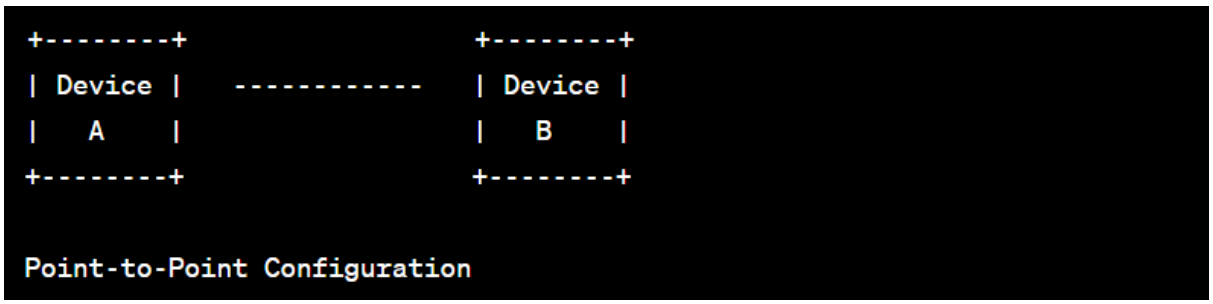


LINE CONFIGURATION:

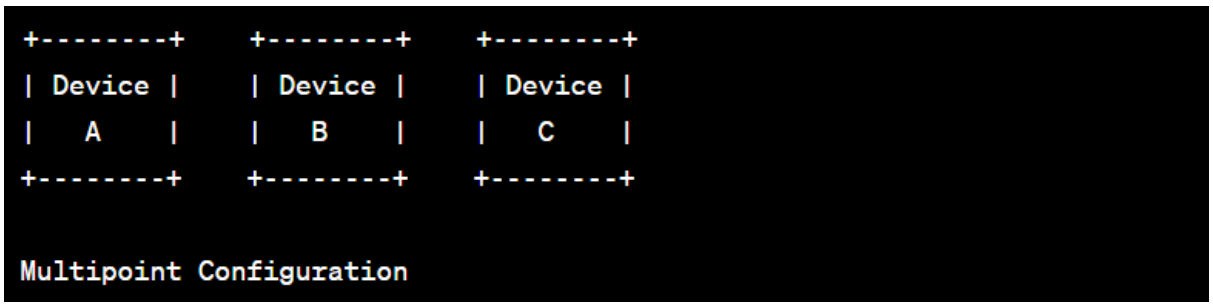
Line configuration, also known as transmission mode or transmission configuration, refers to the arrangement of communication links between devices in a network. It determines how data is transmitted and received between devices connected by a communication channel.

There are three main types of line configurations:

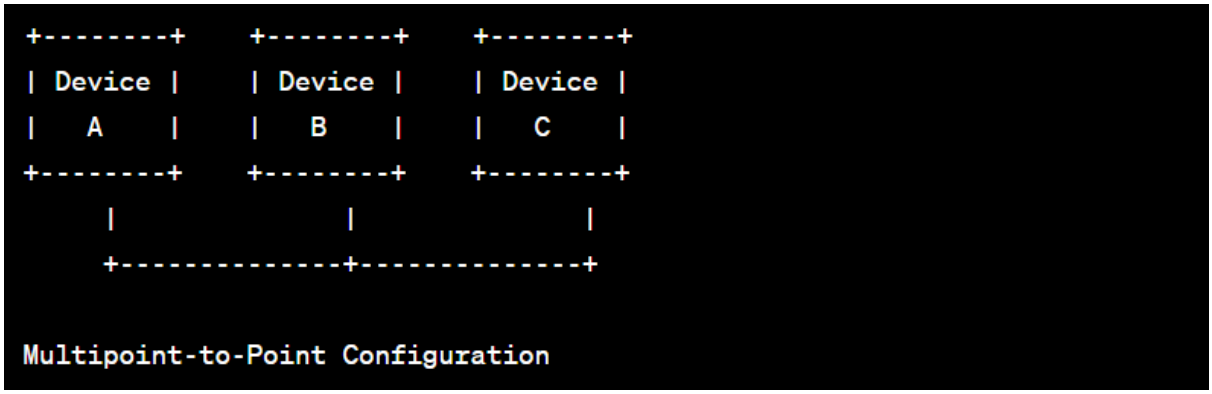
- **Point-to-Point Configuration:** In this configuration, a direct link exists between two devices, allowing communication between them. Examples include a telephone call or a direct cable connection between two computers.



- **Multipoint Configuration:** This configuration involves multiple devices connected to a single communication channel, with data being transmitted from one device to all other devices. An example is a broadcast radio or television transmission.



- **Multipoint-to-Point Configuration:** This configuration combines elements of both point-to-point and multipoint configurations. It allows multiple devices to communicate with a single central device, but the central device can communicate only with one device at a time. This setup is common in satellite communication.



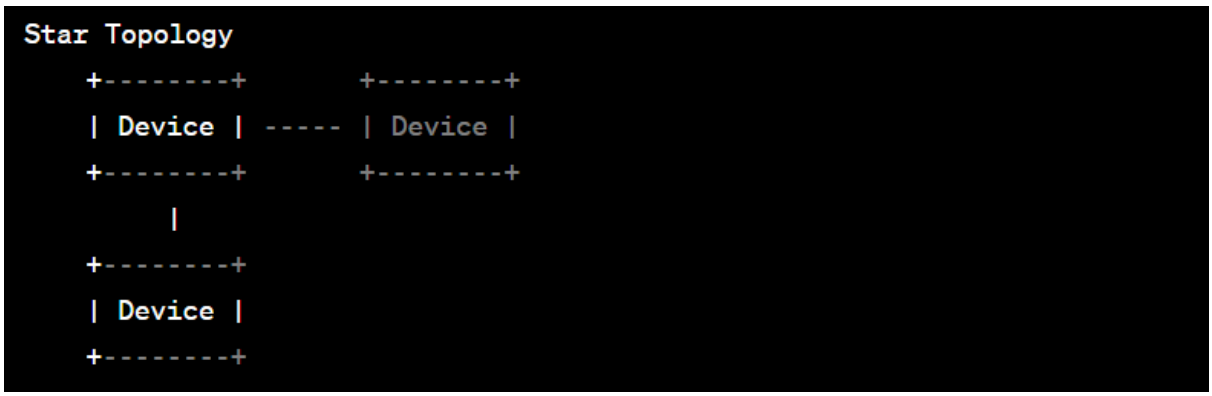
TOPOLOGY:

Topology refers to the physical or logical arrangement of devices and links in a network. It outlines how devices are interconnected and how data flows between them. Different network topologies offer distinct advantages and disadvantages in terms of cost, scalability, and fault tolerance.

Common network topologies include:

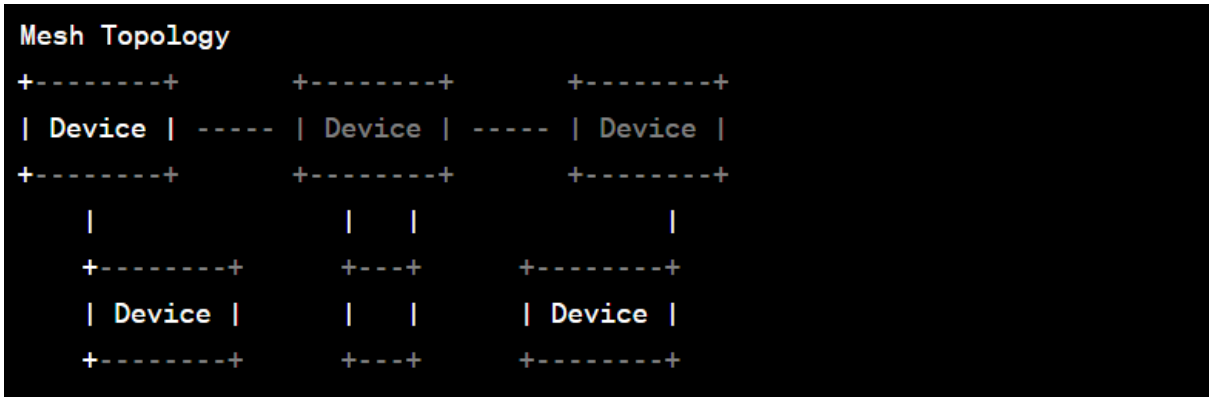
- **Bus Topology:** Devices are connected to a single central cable (bus). Data is transmitted from one end of the bus to the other, and all devices on the bus can receive the data. A break in the bus can disrupt communication.

- **Star Topology:** All devices are connected to a central hub or switch. Data traffic passes through the hub, which manages communication between devices. If the hub fails, only the affected connection is disrupted.

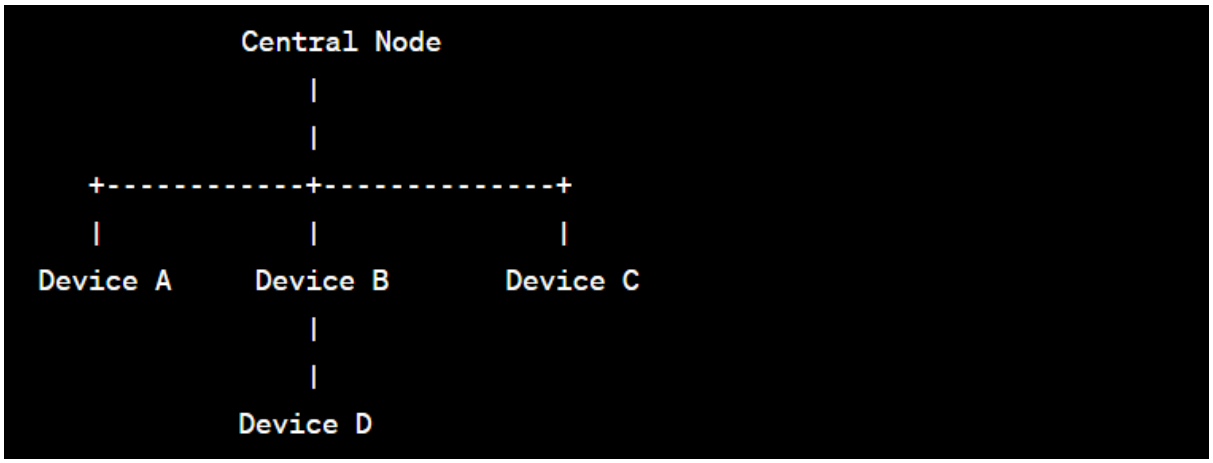


- **Ring Topology:** Devices are connected in a closed loop, where each device is connected to exactly two other devices. Data travels in one direction around the ring. Failure of a single device can disrupt the entire network.

- **Mesh Topology:** Every device is connected to every other device. Mesh networks provide high redundancy and fault tolerance but can be expensive to implement.



- **Tree (Hierarchical) Topology:** Devices are organized in a hierarchical structure resembling a tree. This topology is often used in larger networks and allows for better organization and management.



- **Hybrid Topology:** A combination of two or more topology types. For example, a network might combine star and bus topologies to balance redundancy and scalability.

TRANSMISSION MODE:

Transmission mode, also known as line configuration or communication mode, defines the direction of data flow between devices in a network. It outlines how data is transmitted and received across communication channels.

There are three main transmission modes:

1. Simplex Mode:

In simplex mode, communication occurs in only one direction. One device acts as the sender, and the other acts as the receiver. The receiver can only receive data and has no capability to send data back to the sender. Examples of simplex mode include television broadcasting and radio transmission.

```
Sender --> Data --> Receiver
```

2. Half-Duplex Mode:

Half-duplex mode allows communication in both directions, but not simultaneously. Devices can either send or receive data at a given time, but not both. When one device is sending, the other device must be in a receiving state. Walkie-talkies and some computer networks operate in half-duplex mode.

```
Sender --> Data --> Receiver
       <--- ACK ----
```

3. Full-Duplex Mode:

Full-duplex mode enables simultaneous bidirectional communication. Devices can both send and receive data concurrently. This mode is commonly used in telephone networks and modern computer networks, such as Ethernet.

```
Sender --> Data --> Receiver
Sender <-- ACK ---- Receiver
```

CATEGORIES OF NETWORKS:

Networks are categorized based on their scale, purpose, and geographic scope. Here are the main categories:

1. Personal Area Network (PAN):

A PAN is the smallest network and connects devices within the range of an individual person, typically within a few meters. Examples include Bluetooth connections between devices like smartphones, headphones, and smartwatches.

2. Local Area Network (LAN):

A LAN spans a small geographic area, such as a home, office, or campus. LANs are often used for connecting computers, printers, and other devices within a building. Ethernet and Wi-Fi are common technologies for LANs.

3. Metropolitan Area Network (MAN):

A MAN covers a larger geographic area than a LAN but is smaller than a wide area network (WAN). It connects multiple LANs within a city or metropolitan area. MANs are used to provide high-speed connectivity for businesses and organizations.

4. Wide Area Network (WAN):

A WAN covers a large geographic area and can span cities, countries, or even continents. The internet is the largest example of a WAN. WANs use technologies like leased lines, satellites, and fiber optics for long-distance communication.

5. Global Area Network (GAN):

A GAN is an extension of a WAN that covers a large geographic area, often on a global scale. It may use a combination of satellite links, undersea cables, and other communication technologies.

6. Wireless Networks:

Wireless networks use wireless communication technologies like Wi-Fi, cellular networks, and satellite links to connect devices without physical cables. These networks can span various scales, from PANs to global wireless networks.

7. Internet of Things (IoT) Networks:

IoT networks connect various smart devices and sensors to share data and interact. These networks are used in applications such as home automation, industrial automation, and smart cities.

8. Intranets and Extranets:

Intranets are private networks used within organizations for sharing information and resources. Extranets extend this concept to include communication with external partners, suppliers, or customers, while still maintaining security.

9. Virtual Private Network (VPN):

A VPN is a secure network that enables users to access resources on a private network over a public network like the internet. It provides encryption and security for data transmission.

10. Cloud Networks:

Cloud networks involve the use of remote servers hosted on the internet to store, manage, and process data. Cloud services allow users to access resources and applications without

OSI & TCP/IP MODEL

OSI Model:

The OSI model is a conceptual framework used to standardize the functions of a communication system or network into seven distinct layers. Each layer has specific responsibilities, and the model helps ensure interoperability between different systems and protocols.

1. Physical Layer:

Deals with the physical connection between devices and the transmission of raw bits over a physical medium. It defines specifications for cables, connectors, and the electrical/optical signals used for data transmission.

2. Data Link Layer:

Provides error detection and correction, as well as addressing within the local network. It divides data into frames and manages access to the transmission medium. Ethernet is an example of a data link layer protocol.

3. Network Layer:

Focuses on routing data packets from the source to the destination across different networks. It deals with logical addressing (IP addresses) and determines the best path for data delivery. IP (Internet Protocol) operates at this layer.

4. Transport Layer:

Manages end-to-end communication, ensuring reliable data delivery. It provides error detection and correction, flow control, and data segmentation. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) operate at this layer.

5. Session Layer:

Establishes, maintains, and terminates communication sessions between two devices. It manages session synchronization, data exchange, and error recovery.

6. Presentation Layer:

Handles data translation, encryption, and compression to ensure that data from the application layer of one system can be understood by the application layer of another system.

7. Application Layer:

Provides network services directly to end-users or applications. It encompasses various application-specific protocols such as HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol).

TCP/IP Model:

The TCP/IP model is another networking framework used for designing and implementing the Internet. It consists of four layers, which map to some extent to the OSI model's layers.

1. Network Interface Layer:

Equivalent to the combination of OSI's Physical and Data Link layers, it deals with the physical and data link aspects of data transmission, including addressing, framing, and error detection.

2. Internet Layer:

Similar to OSI's Network Layer, it manages IP addressing, routing, and the fragmentation and reassembly of packets. IP (Internet Protocol) operates here.

3. Transport Layer:

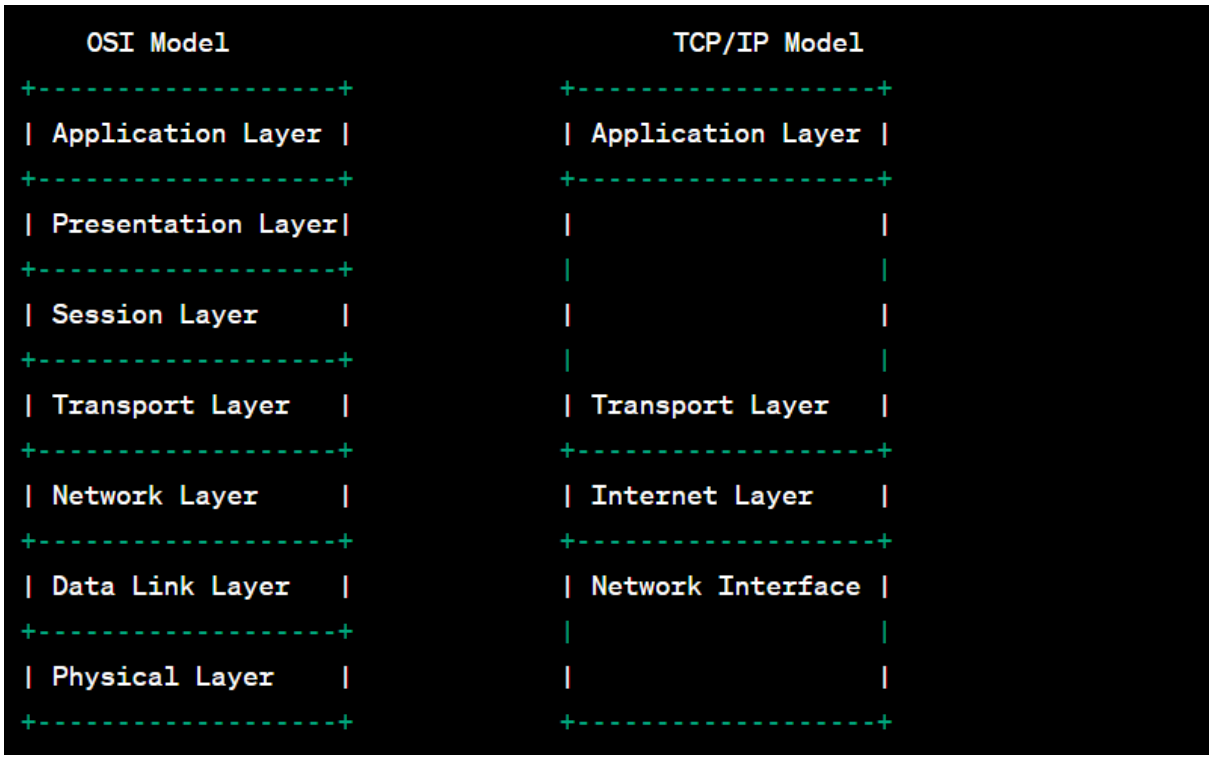
Comparable to OSI's Transport Layer, it ensures end-to-end communication, reliability, and data segmentation. TCP and UDP operate here.

4. Application Layer:

Corresponds roughly to OSI's top three layers (Session, Presentation, and Application). It includes protocols for various applications, such as HTTP, FTP, SMTP, and more.

Comparison of OSI and TCP/IP Models:

Here's a comparison between the two models using a block diagram:



Key Comparison Points:

- The OSI model has 7 layers, while the TCP/IP model has 4 layers.

- The TCP/IP model's Internet Layer encompasses functions of both OSI's Network and Data Link layers.

- The OSI model is more comprehensive and abstract, while the TCP/IP model is more closely aligned with the functionality of the Internet.

- The TCP/IP model's Application Layer combines the functionality of the top three layers of the OSI model.

- The OSI model is often used as a teaching tool, while the TCP/IP model is widely used in real-world networking.

TRANSMISSION MEDIA:

Transmission media, also known as communication channels, are the pathways through which data travels from one device to another in a network. There are two main categories of transmission media: guided (wired) and unguided (wireless).

1. Guided Transmission Media:

Guided transmission media use physical pathways to transmit signals. These media provide a controlled environment for signal propagation, which helps minimize signal degradation and interference.

Common types of guided transmission media include:

- Twisted Pair Cable: Consists of pairs of insulated copper wires twisted together. Used in telephone lines and Ethernet connections.

- Coaxial Cable: Contains a central conductor, insulating layer, metallic shield, and protective covering. Used in cable TV and broadband connections.

- Fiber-Optic Cable: Transmits data using light signals through glass or plastic fibers. Offers high bandwidth and immunity to electromagnetic interference.

2. Unguided Transmission Media:

Unguided transmission media do not have a physical pathway and use open space to transmit signals. These media are susceptible to interference and attenuation but offer the advantage of mobility and flexibility.

Common types of unguided transmission media include:

- Radio Waves: Used in wireless communication, including Wi-Fi and cellular networks.

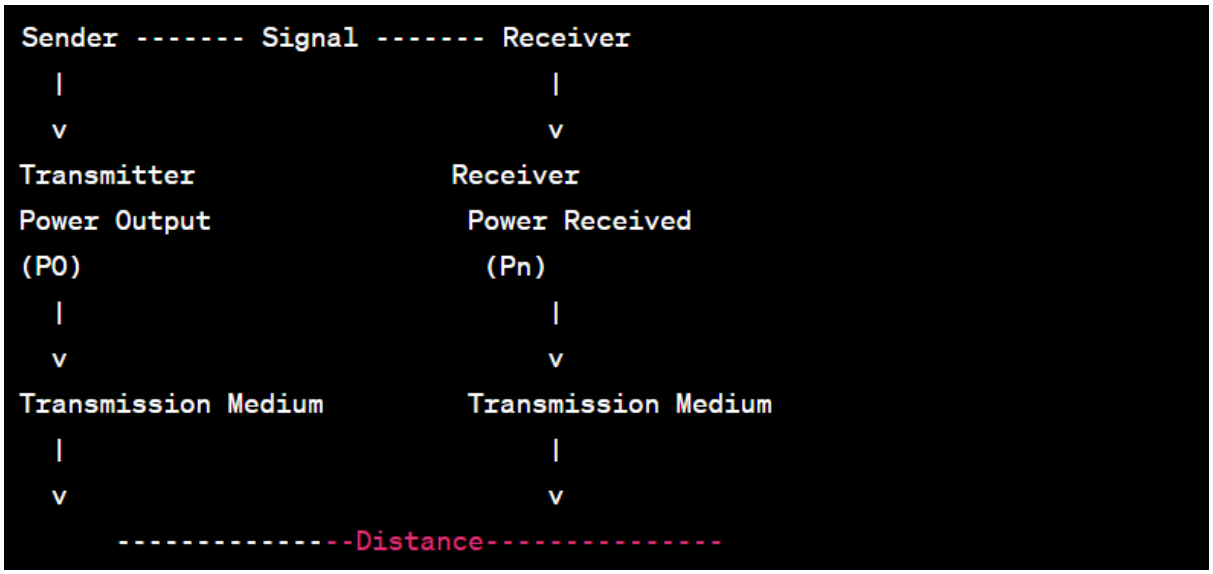
- Microwaves: Used in point-to-point communication, satellite links, and some wireless networks.

- Infrared Waves: Used for short-range communication, such as remote controls and infrared data transmission.

ATTENUATION:

Attenuation refers to the gradual loss of signal strength as it travels through a transmission medium. This loss occurs due to factors like distance, interference, and the properties of the medium itself. Attenuation can result in reduced signal quality and lower transmission distances.

Block Diagram for Attenuation:



In the block diagram:

- The "Sender" generates a signal with a certain initial power output (P0).

- The signal travels through the "Transmission Medium" (guided or unguided).

- As the signal travels over a certain "Distance," it experiences attenuation, which reduces its power.

- The "Receiver" detects the signal with a reduced power (Pn).

Factors contributing to attenuation:

- Distance: The signal weakens as it travels over greater distances.

- Signal Interference: External signals and electromagnetic interference can distort the signal.

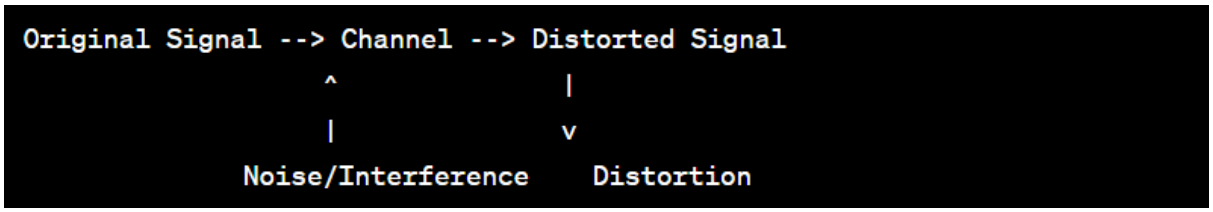
- Medium Properties: Different media have varying levels of attenuation. For example, fiber-optic cables have lower attenuation compared to copper cables.

- Frequency: Higher-frequency signals tend to attenuate more than lower-frequency signals.

DISTORTION:

Distortion refers to any undesired alteration of a signal waveform as it passes through a communication channel. It can be caused by various factors such as noise, interference, and signal degradation. Distortion can result in the loss of signal quality and information.

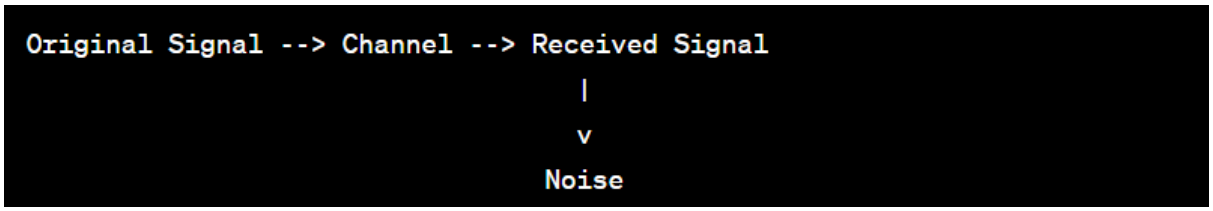
Block Diagram for Distortion:



NOISE:

Noise is any unwanted or random signal that interferes with the transmission and reception of desired signals. It can result from external sources, such as electromagnetic interference or thermal noise, and degrade the quality of the transmitted signal.

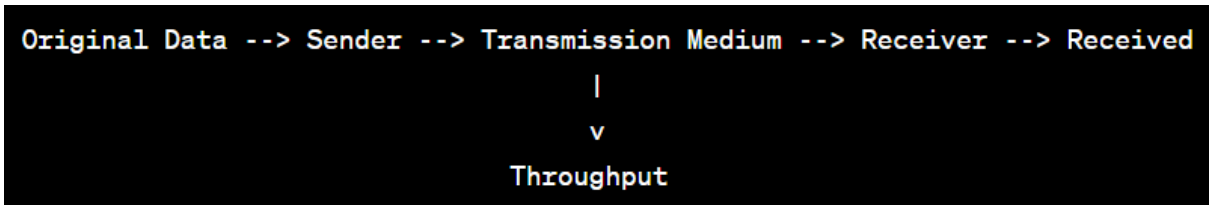
Block Diagram for Noise:



THROUGHPUT:

Throughput is the actual amount of data that can be transmitted over a communication channel in a given time period. It considers factors like transmission speed, efficiency, and potential overhead. Throughput is a key metric for assessing the efficiency of a communication system.

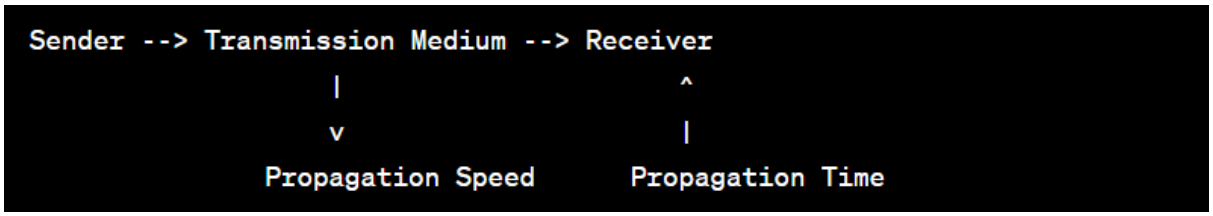
Block Diagram for Throughput:



PROPAGATION SPEED AND TIME:

Propagation speed is the speed at which a signal travels through a transmission medium. Propagation time is the time it takes for a signal to travel from the sender to the receiver. These factors are influenced by the type of medium and its physical properties.

Block Diagram for Propagation Speed and Time:



WAVELENGTH:

Wavelength is the distance between two consecutive peaks (or troughs) of a waveform. It is a fundamental property of a signal and is related to its frequency. In communication systems, wavelength is crucial for understanding signal propagation and interference.

Block Diagram for Wavelength:

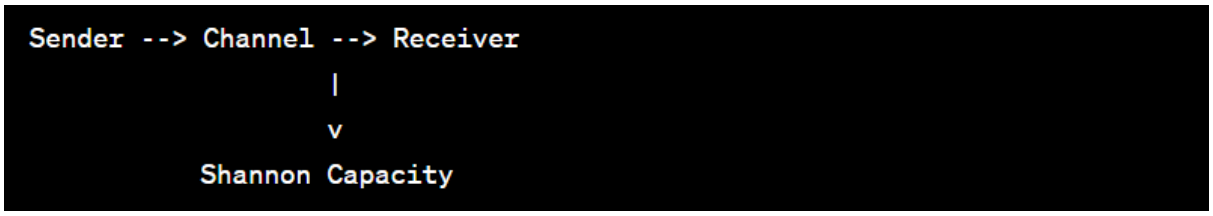
SHANNON CAPACITY:

Shannon Capacity, also known as channel capacity, is the maximum data rate at which information can be transmitted over a communication channel without error. It takes into account the signal-to-noise ratio and the available bandwidth.

OR

The Shannon Capacity, also known as the Shannon-Hartley theorem, defines the theoretical maximum data rate (in bits per second) that can be reliably transmitted over a communication channel without error, given a certain bandwidth and signal-to-noise ratio. The formula for Shannon Capacity is: $C = B * \log2(1 + S/N)$, where C is the capacity, B is the bandwidth, S is the signal power, and N is the noise power.

Block Diagram for Shannon Capacity:



UNIT-II

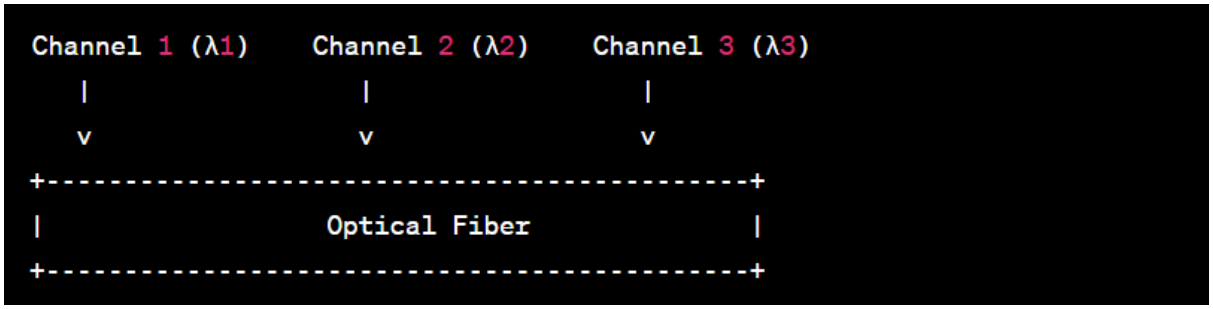
MULTIPLEXING:

Multiplexing is a technique used in telecommunications and networking to combine multiple data streams or signals into a single transmission medium, such as a cable or a fiber optic link. Multiplexing allows efficient use of resources and higher data transmission capacity.

WAVELENGTH DIVISION MULTIPLEXING (WDM):

WDM is a multiplexing technique that combines multiple optical signals of different wavelengths (colors) onto a single optical fiber. Each wavelength corresponds to a different communication channel, allowing simultaneous transmission of multiple data streams over a single fiber.

Block Diagram for WDM:



In the block diagram:

- Each "Channel" represents a separate wavelength (color) of light.

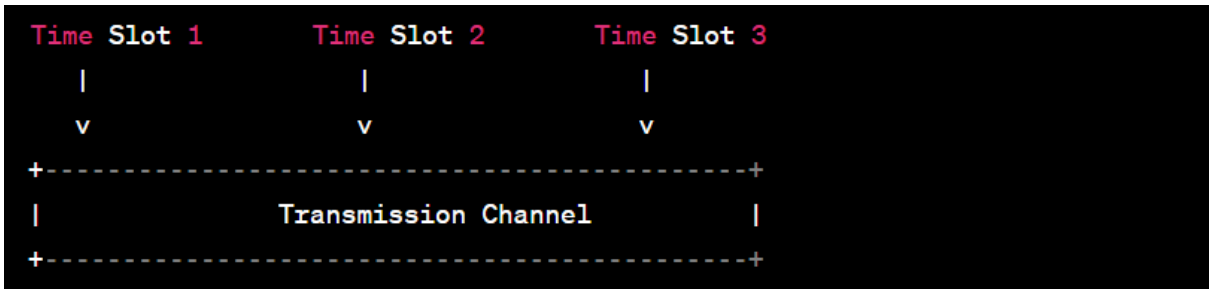
- The optical fiber carries multiple channels simultaneously.

- WDM enables high data transmission capacity by utilizing different wavelengths for different signals.

TIME DIVISION MULTIPLEXING (TDM):

TDM is a multiplexing technique that divides a transmission channel into time slots, with each time slot allocated to a different data stream. The data streams take turns using the channel during their respective time slots.

Block Diagram for TDM:



In the block diagram:

- Each "Time Slot" represents a designated period of time.

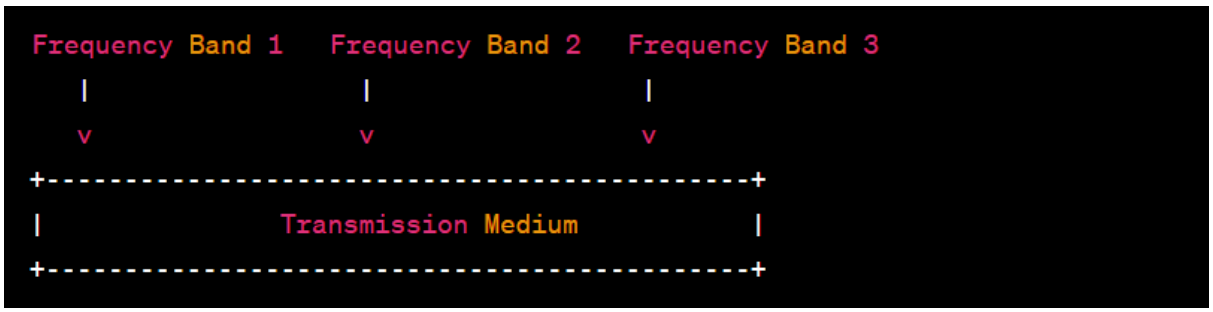
- Data streams are interleaved within their respective time slots.

- TDM enables multiple data streams to share the same channel without overlap.

FREQUENCY DIVISION MULTIPLEXING (FDM):

FDM is a multiplexing technique that divides a transmission medium into multiple frequency bands. Each band is allocated to a different data stream, allowing them to be transmitted simultaneously without interference.

Block Diagram for FDM:



In the block diagram:

- Each "Frequency Band" represents a range of frequencies.

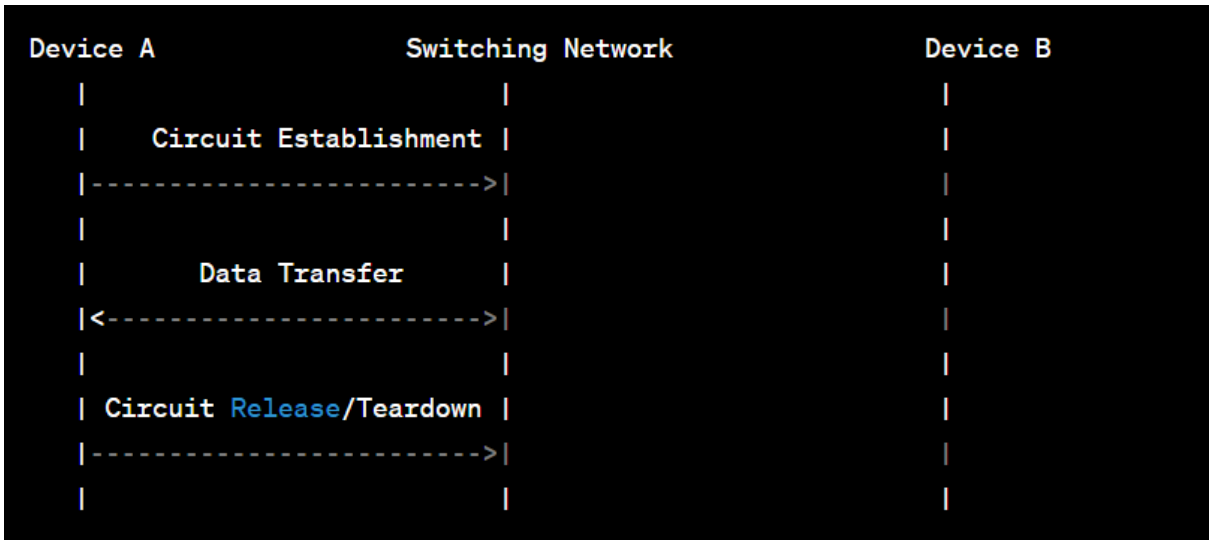
- Data streams are allocated to different frequency bands.

- FDM enables simultaneous transmission of multiple data streams by utilizing different frequency ranges.

CIRCUIT SWITCHING:

Circuit switching is a communication method that establishes a dedicated communication path, or circuit, between two devices for the duration of their conversation. This approach is commonly associated with traditional telephone networks.

Block Diagram for Circuit Switching:



In the block diagram:

- Circuit Establishment: A dedicated communication path (circuit) is established between Device A and Device B through the switching network.

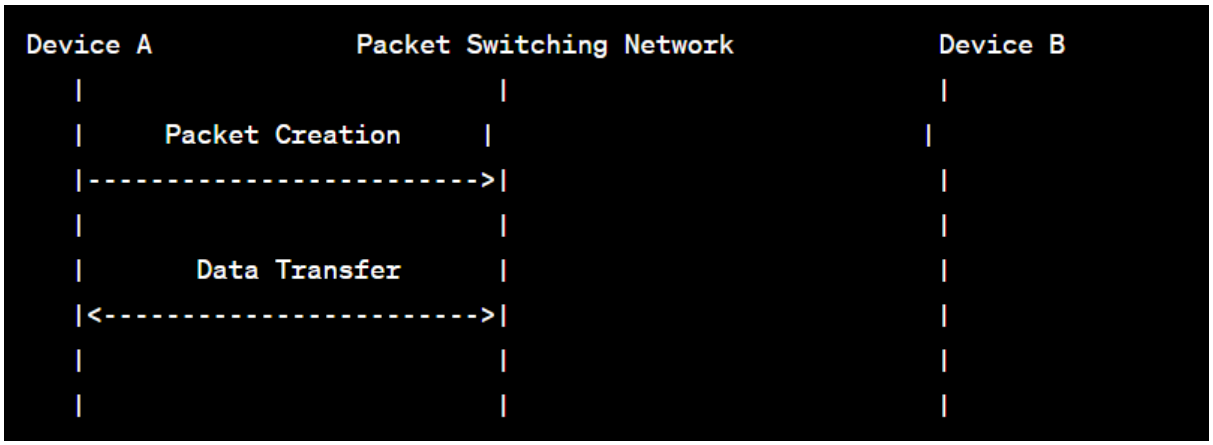
- Data Transfer: Data is continuously exchanged over the established circuit.

- Circuit Release/Teardown: After the conversation is complete, the circuit is released.

PACKET SWITCHING:

Packet switching is a communication method where data is divided into smaller packets and transmitted separately over a shared network. Each packet contains a header with addressing information, allowing them to be routed independently. Packet switching is commonly used in modern computer networks, including the internet.

Block Diagram for Packet Switching:



In the block diagram:

- Packet Creation: Data from Device A is divided into packets, each with its own header containing addressing information.

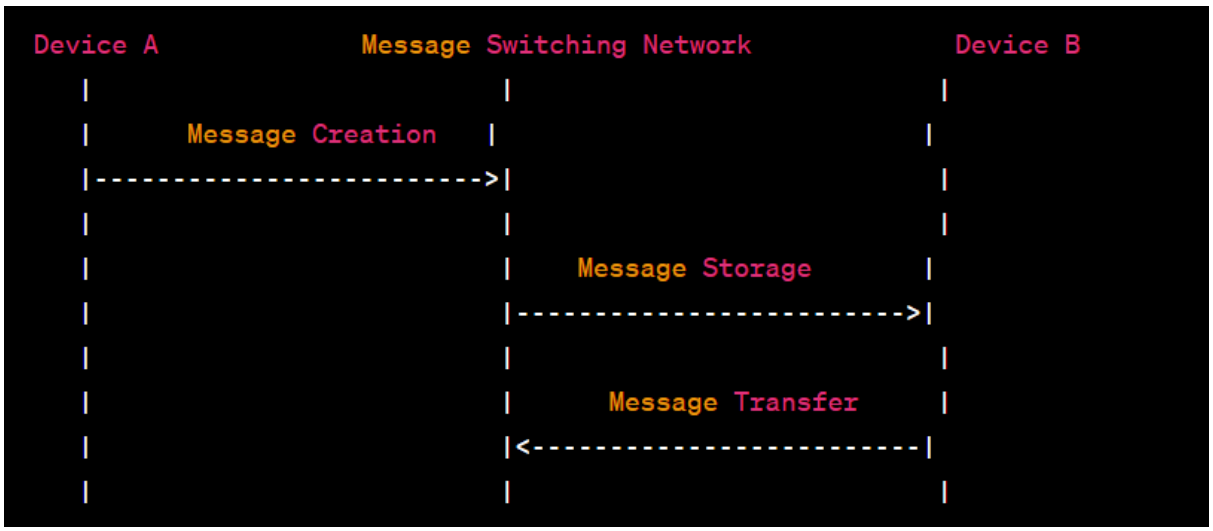
- Data Transfer: Packets are transmitted independently over the packet switching network.

- Packet Reception: Device B receives the packets and reassembles them to reconstruct the original data.

MESSAGE SWITCHING:

Message switching involves sending complete messages from source to destination through intermediate nodes. Each intermediate node temporarily stores the entire message before forwarding it to the next node. This approach was common in early data communication systems.

Block Diagram for Message Switching:



In the block diagram:

- Message Creation: A complete message is created at Device A.

- Message Storage: Each intermediate node stores the entire message temporarily before forwarding it.

- Message Transfer: The message is forwarded sequentially through the message switching network until it reaches Device B.

DATA LINK LAYER:

The Data Link Layer is the second layer of the OSI Model. It provides error detection and correction, as well as reliable data transmission between directly connected devices over a physical link. It breaks down data from the Network Layer into frames for transmission.

Types of Errors:

1. Single-Bit Error: A single bit in the data changes its value due to noise or interference.

2. Burst Error: A sequence of consecutive bits gets corrupted due to sustained noise or interference.

3. Checksum Errors: The calculated checksum of a frame doesn't match the received checksum, indicating data corruption.

4. Frame Loss: The entire frame is lost during transmission due to network issues.

5. Out-of-Sequence Error: Frames are received out of order, disrupting the data stream's sequence.

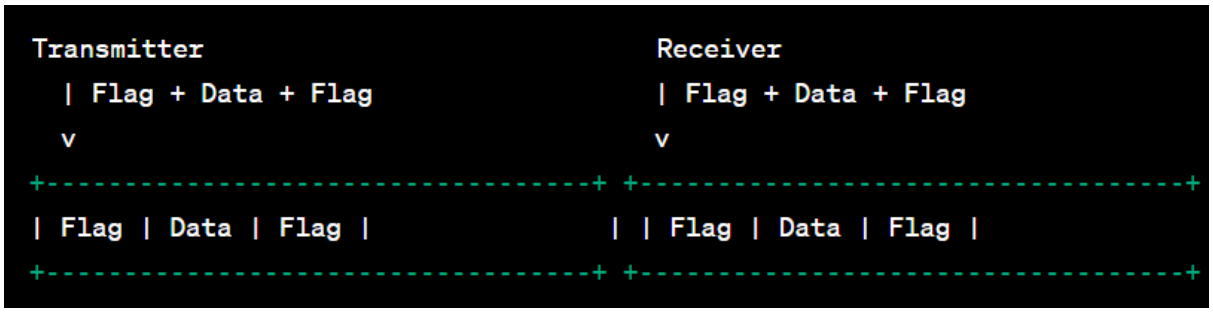
FRAMING:

Framing is the process of dividing the data stream into frames for transmission. The receiver uses framing to identify the beginning and end of each frame, allowing for correct frame extraction.

CHARACTER STUFFING:

In character stuffing, a special flag character is used to mark the beginning and end of each frame. If the flag character appears within the data, it's "stuffed" with an escape sequence to avoid confusion with the flag.

Block Diagram for Character Stuffing:



In the block diagram:

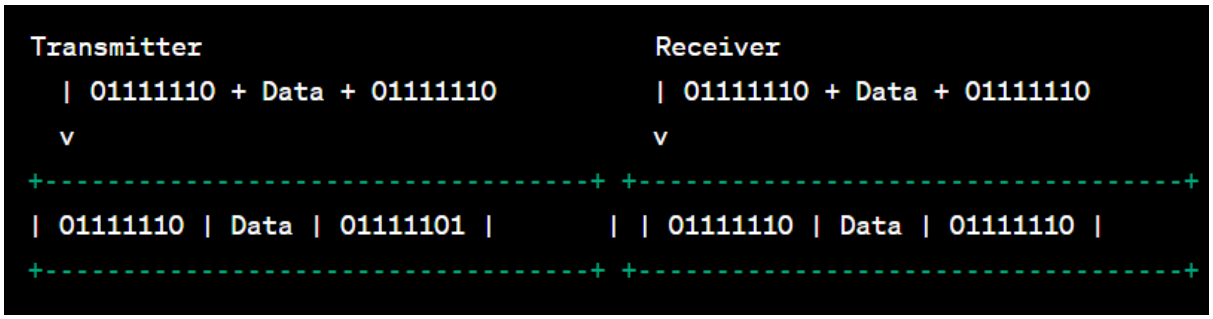
- Data is framed between two flag characters.

- If a flag character appears in the data, it's stuffed with an escape sequence.

BIT STUFFING:

In bit stuffing, a predefined pattern of bits is used as a delimiter for frame boundaries. If the pattern appears in the data, an extra bit is inserted to ensure that it's not mistaken for a delimiter.

Block Diagram for Bit Stuffing:



In the block diagram:

- Data is framed between two occurrences of the pattern 01111110.

- If the pattern appears in the data, an extra 0 is stuffed after five consecutive 1s to ensure accurate framing.

ERROR DETECTION AND CORRECTION METHODS:

Error Detection:

Error detection methods are used to identify the presence of errors in data transmission. They help ensure data integrity during communication.

Some common error detection methods include:

1. Parity Bit: A parity bit is added to the data so that the total number of ones (or zeros) is always even (even parity) or odd (odd parity). If the received data has a different parity, an error is detected.

2. Checksum: A checksum is calculated by adding all data bytes and then adding the result to the transmitted data. The receiver calculates the checksum and checks if it matches the received checksum. If not, an error is detected.

3. Cyclic Redundancy Check (CRC): CRC is a more robust error detection method. A polynomial code is used to generate a checksum, which is appended to the data. The receiver performs the same calculation and checks if the received checksum matches. If not, an error is detected.

Error Correction:

Error correction methods not only detect errors but also attempt to recover the original data by making educated guesses.

Some common error correction methods include:

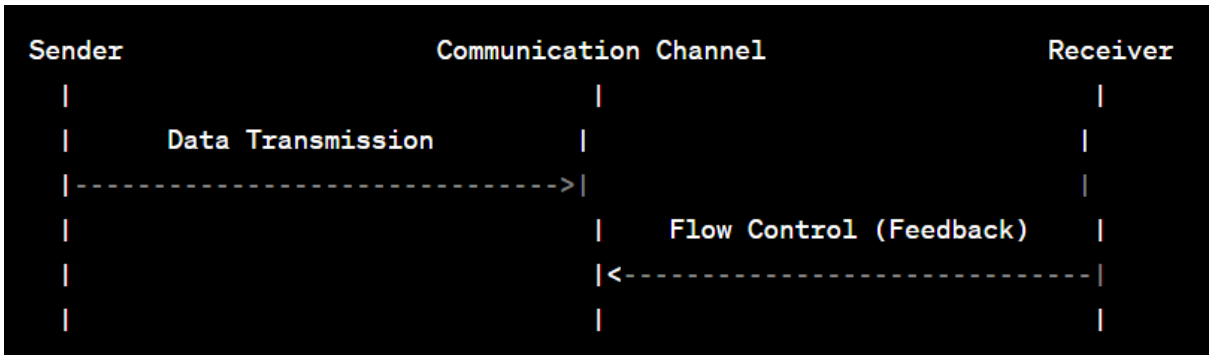
1. Hamming Code: Hamming codes add redundant bits to data to create a code that can correct single-bit errors and detect multiple-bit errors.

2. Reed-Solomon Code: Reed-Solomon codes are used for correcting errors in data transmission. They work well for burst errors, common in digital communication.

FLOW CONTROL:

Flow control is a mechanism that ensures data transmission occurs at an appropriate rate between sender and receiver to avoid overwhelming the receiver with data or causing data loss due to congestion.

Block Diagram for Flow Control:



In the block diagram:

- The "Sender" sends data to the "Receiver" through the communication channel.

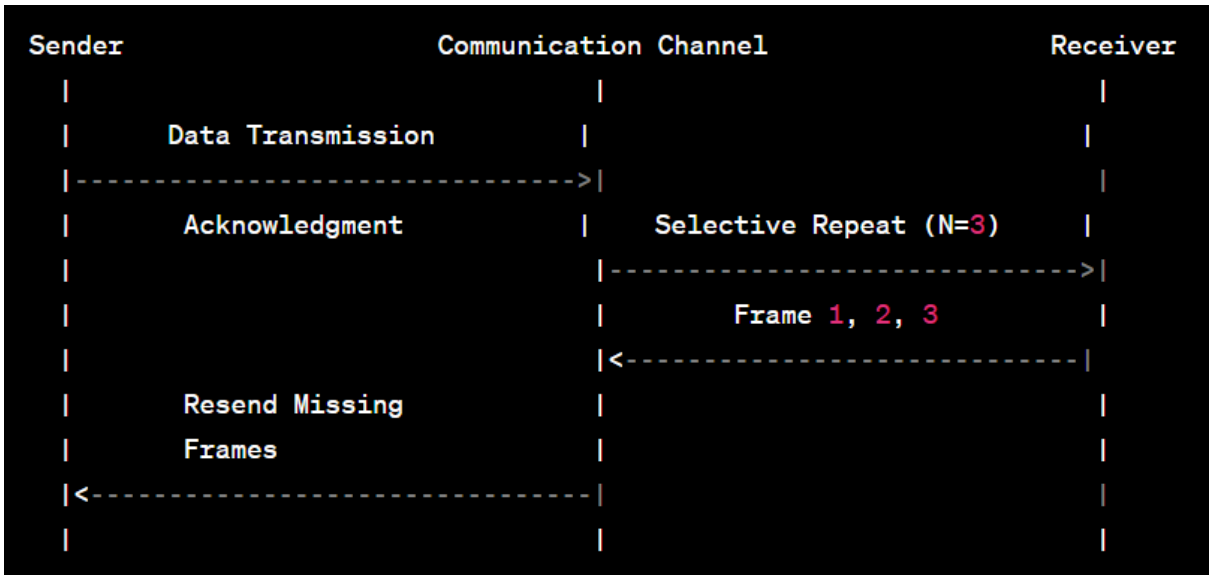
- The "Receiver" provides feedback to the "Sender" about its readiness to receive data, indicating the appropriate flow rate.

- This feedback helps the "Sender" adjust its transmission rate to match the "Receiver's" ability to process the data.

SELECTIVE REPEAT FLOW CONTROL:

Selective Repeat is a flow control mechanism in which the receiver acknowledges the receipt of specific frames, allowing the sender to resend only the frames that were not successfully received.

Block Diagram for Selective Repeat Flow Control:



In the block diagram:

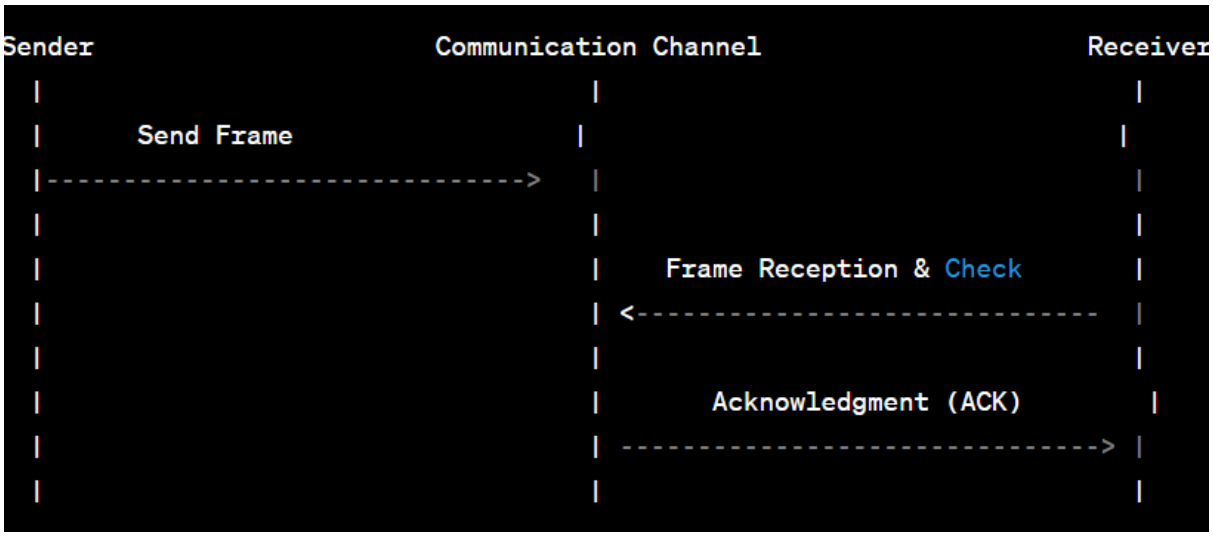
- The "Receiver" acknowledges receipt of specific frames, in this case, frames 1, 2, and 3.

- If frames are missing or have errors, the "Sender" resends only those specific frames.

STOP-AND-WAIT ARQ:

In Stop-and-Wait ARQ, the sender transmits a single data frame and then waits for an acknowledgment from the receiver before sending the next frame. If an acknowledgment is not received within a timeout period or if a negative acknowledgment (NAK) is received, the sender retransmits the frame.

Block Diagram for Stop-and-Wait ARQ:



In the block diagram:

- The "Sender" sends a frame and waits for an acknowledgment from the "Receiver."

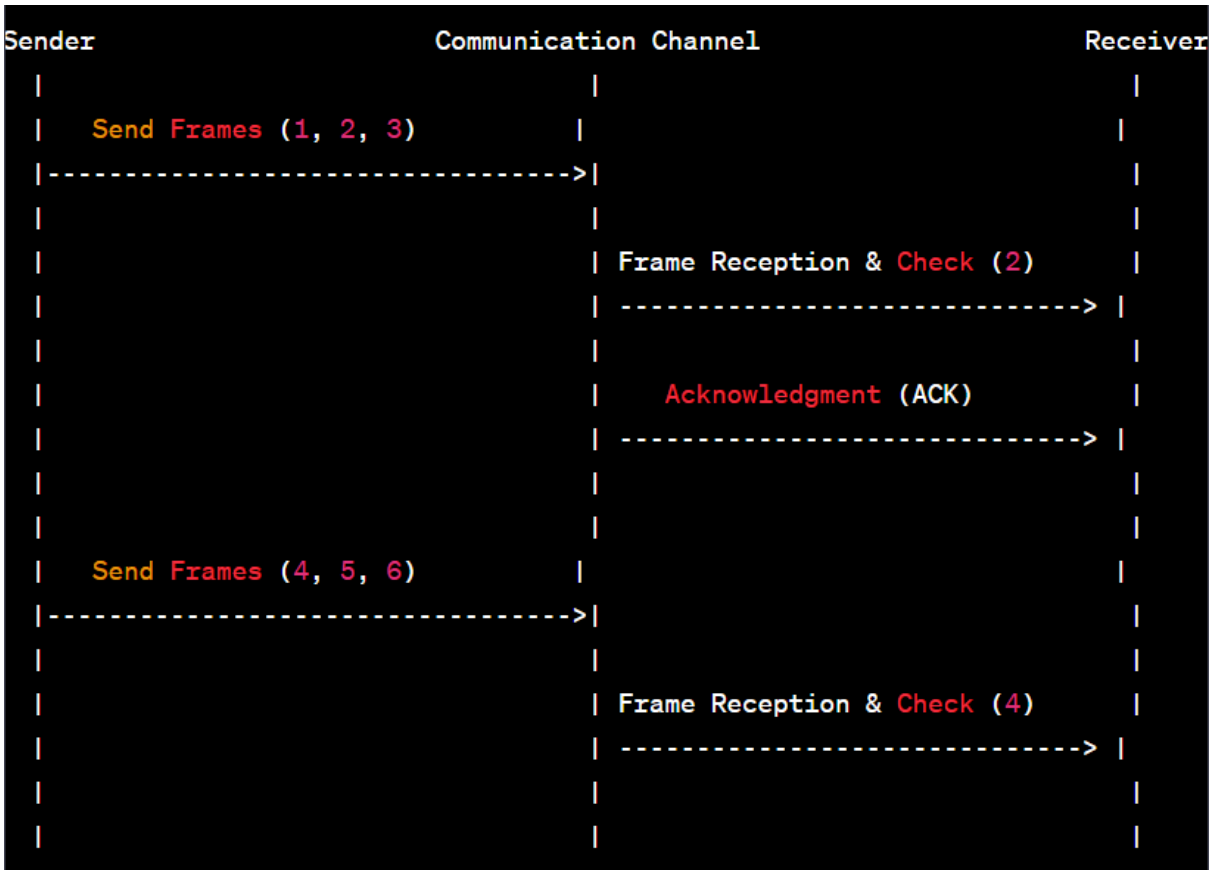
- Upon receiving the frame, the "Receiver" performs error checking and sends an acknowledgment (ACK) if the frame is error-free.

- If the frame is corrupted or lost, the "Receiver" sends a negative acknowledgment (NAK), prompting the "Sender" to retransmit the frame.

GO-BACK-N ARQ:

Go-Back-N ARQ allows the sender to transmit multiple frames before waiting for acknowledgments. The receiver can accept a sequence of correctly received frames. If an error is detected or a frame is lost, the receiver discards subsequent frames until the expected frame is received.

Block Diagram for Go-Back-N ARQ:



In the block diagram:

- The "Sender" transmits multiple frames (1, 2, 3) before waiting for acknowledgments.

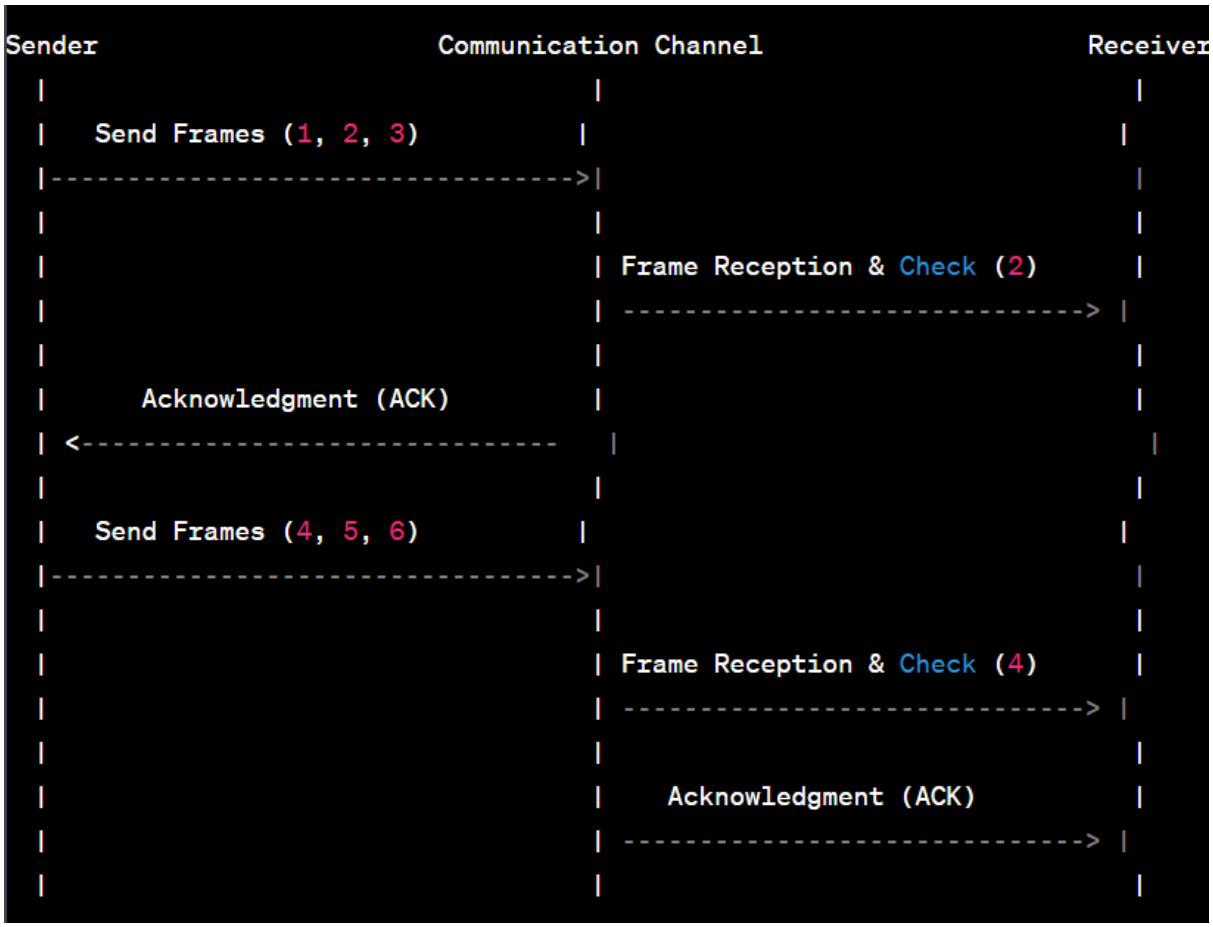
- The "Receiver" acknowledges frame 2, and frames 1 and 3 are still in the buffer.

- Frames 4, 5, and 6 are transmitted and similarly acknowledged.

SELECTIVE REPEAT ARQ:

Selective Repeat ARQ allows the sender to transmit multiple frames before waiting for acknowledgments. The receiver acknowledges individual frames, allowing for retransmission of only the missing or erroneous frames.

Block Diagram for Selective Repeat ARQ:



In the block diagram:

- The "Sender" transmits multiple frames (1, 2, 3) before waiting for acknowledgments.

- The "Receiver" acknowledges frame 2 and also acknowledges frame 4.

- Only missing or erroneous frames (e.g., frame 4) are retransmitted.

UNIT-III

INTERNETWORKING:

Internetworking, also known as networking or network interconnection, refers to the practice of connecting multiple separate networks to create a larger network. It involves the use of various networking devices and technologies to enable communication and data exchange between these networks. The goal of internetworking is to create a unified and seamless communication infrastructure.

NETWORKING DEVICES:

1. Repeater:

A repeater is a device used to extend the reach of a network by amplifying and retransmitting signals. It operates at the physical layer of the OSI model and is used to overcome signal attenuation, allowing data to travel longer distances without significant degradation.

2. Hub:

A hub is a basic networking device that connects multiple devices in a network. It operates at the physical layer and broadcasts incoming data to all connected devices. Hubs do not provide any intelligence for data forwarding and do not differentiate between devices.

3. Bridge:

A bridge is used to connect and segment larger networks into smaller segments, creating separate collision domains. It operates at the data link layer and can selectively forward or filter traffic based on MAC addresses. Bridges improve network efficiency by reducing collision domains and increasing overall bandwidth.

4. Switch:

A switch is an intelligent device that operates at the data link layer and makes forwarding decisions based on MAC addresses. Unlike hubs, switches create separate collision domains for each connected device, leading to better network performance and less congestion.

5. Router:

A router operates at the network layer and is responsible for forwarding data between different networks. It uses IP addresses to determine the best path for data transmission. Routers enable internetworking by connecting networks with different IP subnets and facilitating data exchange between them.

6. Gateway:

A gateway is a device or software application that translates between different communication protocols or data formats. It enables communication between networks that use different protocols. Gateways are often used to connect local networks to the internet.

7. Modem:

A modem (modulator-demodulator) is a device that converts digital data from a computer into analog signals suitable for transmission over analog communication channels such as telephone lines. At the receiving end, the modem converts the analog signals back into digital data. Modems are commonly used to provide internet connectivity over phone lines.

ADDRESSING IN IPV4:

IPv4 (Internet Protocol version 4) uses a 32-bit address format, which is typically represented in dotted-decimal notation (e.g., 192.168.1.1).

An IPv4 address is divided into two main parts: the network portion and the host portion.

1. Network Portion: This part of the address identifies the network to which the device belongs. All devices within the same network share the same network portion of the address.

2. Host Portion: This part of the address identifies the specific device within the network. Each device within the same network has a unique host portion of the address.

IPv4 addressing includes concepts like classes (A, B, C, D, E), public and private addresses, and subnet masks for defining the boundary between the network and host portions.

ADDRESSING IN IPV6:

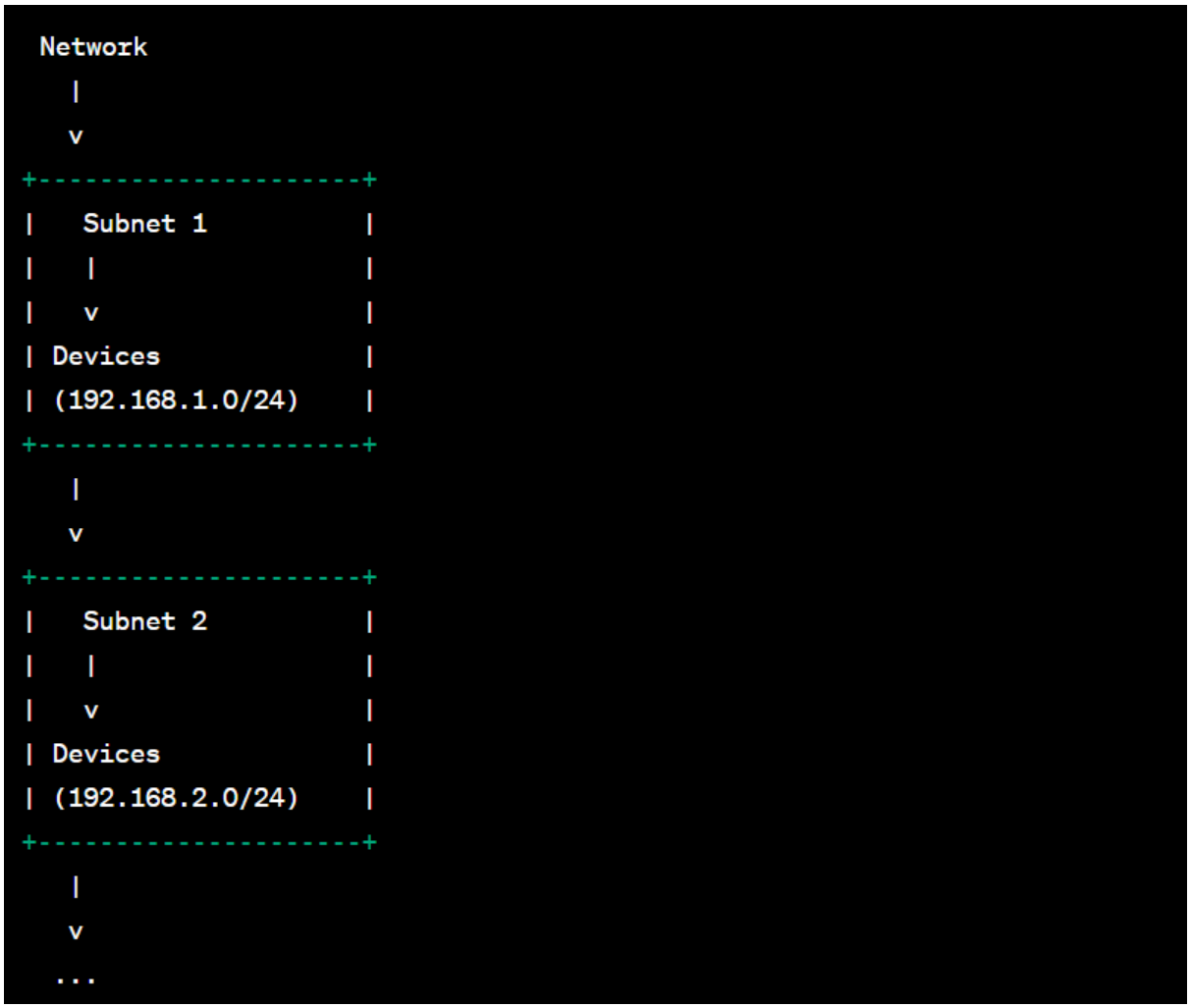
IPv6 (Internet Protocol version 6) was developed to address the limitations of IPv4, primarily the depletion of available addresses due to the rapid growth of the internet. IPv6 uses a 128-bit address format, often represented in hexadecimal notation (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). IPv6 addresses are designed to provide a significantly larger address space, ensuring the availability of unique addresses for countless devices.

IPv6 addresses have several types, including unicast (one-to-one communication), multicast (one-to-many communication), and anycast (nearest available instance). IPv6 also introduces concepts like prefix delegation for efficient address assignment and hierarchical addressing for better routing.

IPV4 SUBNETTING:

Subnetting in IPv4 allows a network to be divided into smaller sub-networks or subnets. This division enhances network management, optimizes routing, and helps allocate IP addresses more efficiently.

Block Diagram for IPv4 Subnetting:



In the block diagram:

- The main "Network" is divided into smaller "Subnets."

- Each subnet has its range of IP addresses (e.g., 192.168.1.0/24, 192.168.2.0/24).

- Devices within each subnet have unique IP addresses, typically assigned based on the subnet they belong to.

Subnetting allows efficient use of IP addresses, better management of network resources, and improved security through isolation.

ROUTING:

Routing is the process of determining the best path for data packets to travel from a source to a destination across an interconnected network. Routing protocols play a crucial role in making these decisions, ensuring efficient and reliable data delivery.

UNICAST ROUTING PROTOCOLS:

Unicast routing protocols are used to determine the best path for data packets from one source to one destination. Let's delve into three prominent unicast routing protocols:

1. RIP (Routing Information Protocol):

- Distance Vector Protocol: RIP is a distance vector routing protocol that uses hop count as its metric. Each router maintains a routing table containing the distance (hop count) to reach different networks.

- Routing Updates: RIP routers periodically exchange routing updates with their neighbors. If a router receives an update with a shorter path to a destination, it updates its routing table accordingly.

- Convergence: RIP uses a split-horizon mechanism to prevent routing loops. It has slower convergence compared to other modern routing protocols.

- Limitations: RIP has limitations in terms of scalability and support for more complex network topologies.

- Advantages: Simple to configure and implement, suitable for small networks.

- Disadvantages: Converges slowly in large networks, limited scalability due to frequent

2. OSPF (Open Shortest Path First):

- Link-State Protocol: OSPF is a link-state routing protocol that uses more advanced algorithms than distance vector protocols. It calculates the shortest path based on link costs rather than hop count.

- Link-State Advertisements (LSAs): OSPF routers exchange LSAs to build a database of the network topology. Routers then run the Dijkstra algorithm to determine the shortest path.

- Areas: OSPF divides networks into areas, reducing the size of the LSAs and improving scalability. Each area has its own routing table, and routers in different areas exchange summarized routing information.

- Fast Convergence: OSPF provides faster convergence compared to RIP due to its link-state nature and efficient routing updates.

- Advantages: Fast convergence, supports VLSM (Variable Length Subnet Masking), and offers better scalability for larger networks.

- Disadvantages: Requires more configuration and resources compared to RIP.

3. BGP (Border Gateway Protocol):

- Path Vector Protocol: BGP is a path vector protocol used in the internet's core routing. It doesn't rely solely on hop count or link metrics; it considers multiple attributes (such as AS-path, next hop, and MED) to determine the best path.

- Autonomous Systems (AS): BGP routers are organized into autonomous systems, which are collections of routers under the control of a single organization or service provider.

- Policy-Based Routing: BGP allows administrators to apply routing policies to control how routes are advertised and selected. This feature is important for maintaining control over network traffic.

- Internet Core Routing: BGP is crucial for inter-domain routing in the internet, enabling communication between networks operated by different organizations.

- Advantages: Extremely scalable, supports policy-based routing, ideal for large and complex networks.

- Disadvantages: Complex to configure, slower convergence compared to interior gateway protocols.

Comparison:

Protocol	Type	Metric	Convergence	Scalability
RIP	Distance Vector	Hop Count	Slower	Limited
OSPF	Link-State	Link Costs	Faster	Better
BGP	Path Vector	Multiple Factors	Slower	Excellent

ROUTING METHODS:

1. Static Routing:

Static routing involves manually configuring the routing tables of routers to determine the paths that data packets should take. Network administrators explicitly define the routes and destinations, and these routes remain unchanged unless manually updated. Static routing is suitable for small networks with simple and predictable topologies. It doesn't adapt well to changes in network conditions and requires manual intervention for updates.

2. Dynamic Routing:

Dynamic routing uses routing protocols to automatically determine the best paths for data packets based on network conditions. Routers exchange routing information, and as network topology changes, routers update their routing tables accordingly. Dynamic routing is suitable

for larger and more complex networks as it adapts to changes, provides faster convergence, and reduces administrative overhead.

BASIC ROUTING COMMANDS:

Routing commands vary depending on the router's operating system. Here, we'll cover some common routing commands in Cisco's IOS (Internetwork Operating System):

1. Viewing Routing Table:

To view the routing table on a Cisco router:

```
show ip route
```

2. Adding a Static Route:

To add a static route in Cisco IOS:

```
ip route <destination-network> <subnet-mask> <next-hop-ip>
```

3. Removing a Static Route:

To remove a static route:

```
no ip route <destination-network> <subnet-mask> <next-hop-ip>
```

4. Enabling a Routing Protocol:

To enable a dynamic routing protocol (e.g., OSPF):

```
router ospf <process-id>
```

5. Configuring Dynamic Routing Protocol Parameters:

To configure parameters for a dynamic routing protocol (e.g., OSPF):

```
router ospf <process-id>
network <network-address> <wildcard-mask> area <area-id>
```

6. Viewing Dynamic Routing Information:

To view dynamic routing protocol information (e.g., OSPF):

```
show ip ospf
```

7. Clearing Routing Table:

To clear the routing table and recompute routes (use with caution):

```
clear ip route *
```

These commands provide a starting point for configuring and managing routing on Cisco routers. Keep in mind that the exact commands and syntax might vary based on the router's operating system and the routing protocol being used.

DISTANCE VECTOR PROTOCOL:

Distance vector protocols are a type of routing protocol used in computer networks to determine the best path for data packets based on the number of hops (distance) to a destination. These protocols operate by periodically exchanging routing updates with neighbouring routers and making routing decisions based on the information in those updates. The most well-known distance vector protocol is RIP (Routing Information Protocol).

Key Characteristics:

- Hop Count: Distance vector protocols measure distances in terms of hop counts. Each router maintains a routing table containing the number of hops required to reach various network destinations.

- Periodic Updates: Routers exchange routing updates at regular intervals to keep each other informed about network changes. These updates contain information about the reachable destinations and their associated hop counts.

- Routing Table: Routers use the information from routing updates to update their routing tables and determine the best paths for data packets.

- Convergence: Distance vector protocols have slower convergence times compared to link state protocols because routers must wait for updates and recalculations to occur.

- Count-to-Infinity Problem: Distance vector protocols are susceptible to the count-to-infinity problem, where incorrect routing information can lead to routing loops and slow convergence.

LINK STATE PROTOCOL:

Link state protocols are a type of routing protocol that focuses on the state of individual links and routers in a network. Instead of simply counting hops, link state protocols gather detailed information about network topology, link costs, and link statuses. OSPF (Open Shortest Path First) is a prominent example of a link state protocol.

Key Characteristics:

- Link State Advertisements (LSAs): In link state protocols, routers exchange LSAs, which describe the state of links and routers in the network. These LSAs are used to build a database of network topology.

- Dijkstra's Algorithm: Link state protocols use Dijkstra's shortest path algorithm to calculate the best path from each router to all other routers in the network. This algorithm considers link costs when making routing decisions.

- Routing Table Calculation: Routers use the information from the LSAs and the results of Dijkstra's algorithm to calculate their routing tables. This process allows routers to determine the shortest paths based on actual link costs.

- Areas: Link state protocols divide networks into areas to improve scalability and manageability. Routers exchange summarized information about their areas, reducing the amount of routing information that needs to be exchanged across the entire network.

- Fast Convergence: Link state protocols offer faster convergence times compared to distance vector protocols. They achieve this by quickly disseminating network changes and recalculating routes based on updated link state information.

UNIT-IV

TRANSPORT LAYER:

The Transport layer is the fourth layer of the OSI Model and plays a critical role in ensuring reliable communication between devices across different networks. It provides end-to-end communication services, such as error detection, data segmentation, flow control, and multiplexing/demultiplexing.

FUNCTIONS OF THE TRANSPORT LAYER:

1. Segmentation and Reassembly: The Transport layer breaks down large data streams into smaller segments for efficient transmission. Upon reception, these segments are reassembled into the original data stream.

2. Flow Control: Flow control ensures that data is transmitted at a rate that the receiver can handle. It prevents overwhelming the receiver with more data than it can process, thereby avoiding data loss or congestion.

3. Error Detection and Correction: The Transport layer detects errors in data transmission and may provide mechanisms for error correction through checksums, acknowledgments, and retransmissions.

4. Multiplexing and Demultiplexing: Multiplexing allows multiple applications or sessions to share the same network connection, while demultiplexing ensures that data gets delivered to the appropriate application or session at the receiving end.

5. Connection Management: The Transport layer manages the establishment, maintenance, and termination of connections between devices. This process involves negotiation and synchronization between sender and receiver.

TRANSPORT LAYER PROTOCOLS:

Two prominent transport layer protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol):

1. TCP (Transmission Control Protocol):

- Reliable and connection-oriented.
- Provides error detection, correction, and retransmission of lost or corrupted segments.
- Ensures data delivery in the correct order.
- Supports flow control and congestion control mechanisms.
- Widely used for applications like web browsing, file transfer, and email.

2. UDP (User Datagram Protocol):

- Connectionless and less reliable than TCP.

- Faster data transmission since there's no connection setup.

- Suitable for applications where speed is more important than reliability, such as video streaming and online gaming.

- Does not provide error correction, retransmission, or guaranteed delivery.

CONNECTION MANAGEMENT:

TCP uses a three-way handshake for connection establishment and termination:

1. Connection Establishment:

1. The client sends a SYN (synchronize) segment to the server.

2. The server responds with a SYN-ACK segment, acknowledging the client's request and sending its own synchronization request.

3. The client acknowledges the server's SYN-ACK segment, completing the connection establishment.

2. Connection Termination:

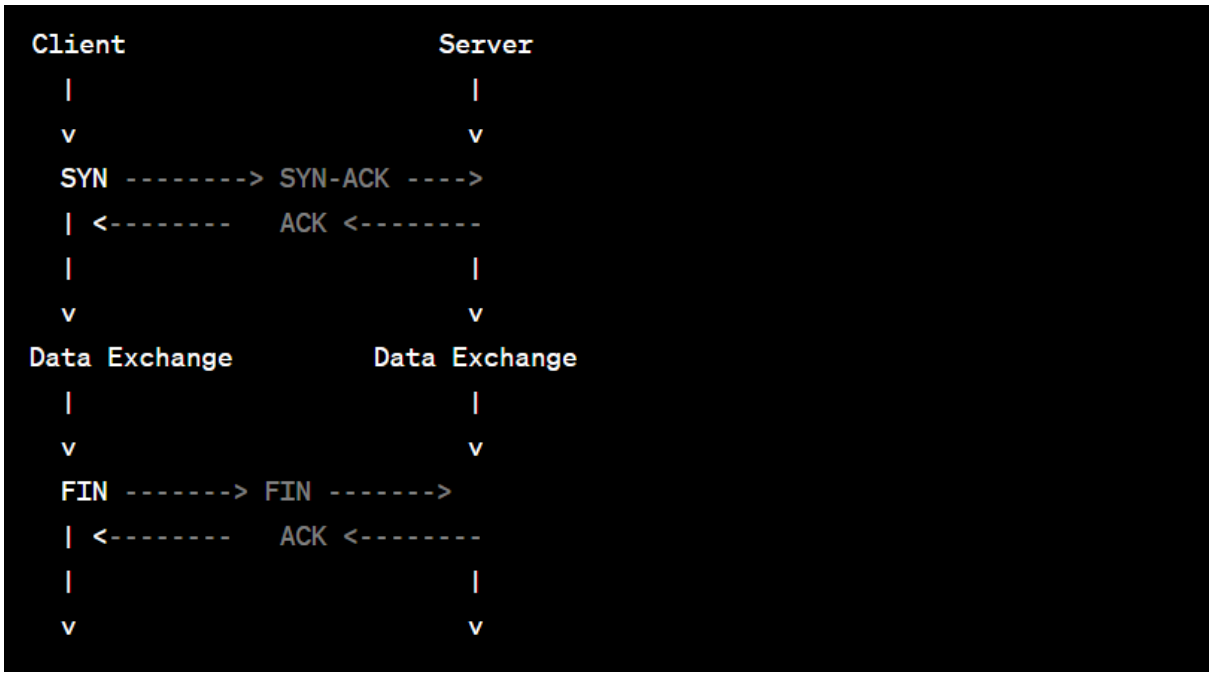
1. The client sends a FIN (finish) segment to the server, indicating its intention to close the connection.

2. The server acknowledges the client's FIN segment.

3. The server sends its own FIN segment to the client.

4. The client acknowledges the server's FIN segment, completing the connection termination.

Block Diagram for Connection Management:



In the block diagram:

- The client initiates the connection by sending a SYN segment to the server.

- The server responds with a SYN-ACK segment, and the connection is established.

- Data exchange occurs between the client and server.

- Either party can initiate connection termination by sending a FIN segment.

- Both parties acknowledge each other's FIN segments, and the connection is terminated.

SESSION LAYER:

The Session Layer is the fifth layer of the OSI Model, responsible for establishing, maintaining, and terminating communication sessions between applications on different devices. It ensures reliable data exchange and manages synchronization between the sender and receiver.

FUNCTIONS OF THE SESSION LAYER:

1. Session Establishment: The Session Layer establishes a logical connection between applications by negotiating session parameters, such as synchronization points and data exchange modes.

2. Session Maintenance: It manages and monitors the ongoing communication session, ensuring that data arrives in the correct order and that lost or duplicate data is handled appropriately.

3. Dialog Control: The Session Layer controls the flow of data between applications, enabling full-duplex or half-duplex communication and handling issues like token management to avoid conflicts.

4. Data Synchronization: The Session Layer provides mechanisms for synchronization between sender and receiver, ensuring that data is exchanged in a coherent manner.

5. Checkpointing and Recovery: It allows applications to set checkpoints during data exchange. If a failure occurs, the Session Layer enables the recovery of data from the last checkpoint.

PRESENTATION LAYER:

The Presentation Layer is the sixth layer of the OSI Model, responsible for translating, encrypting, and compressing data exchanged between applications. It ensures that data from one application can be understood by another application, even if they use different data formats or encoding schemes.

FUNCTIONS OF THE PRESENTATION LAYER:

1. Data Translation: The Presentation Layer translates data between different character sets, formats, or data structures to ensure compatibility between communicating applications.

2. Data Encryption and Decryption: It provides security by encrypting data before transmission and decrypting it upon reception. This ensures confidentiality and data integrity.

3. Data Compression: The Presentation Layer reduces the size of data for more efficient transmission. Compression algorithms are used to minimize bandwidth usage.

4. Data Syntax Conversion: The layer converts data between different data formats, such as from binary to ASCII, to facilitate interoperability between systems with varying data representations.

APPLICATION LAYER:

The Application Layer is the topmost layer of the OSI Model, directly interacting with end-users and applications. It provides a user interface and network services, allowing users to access network resources and communicate over the network.

FUNCTIONS OF THE APPLICATION LAYER:

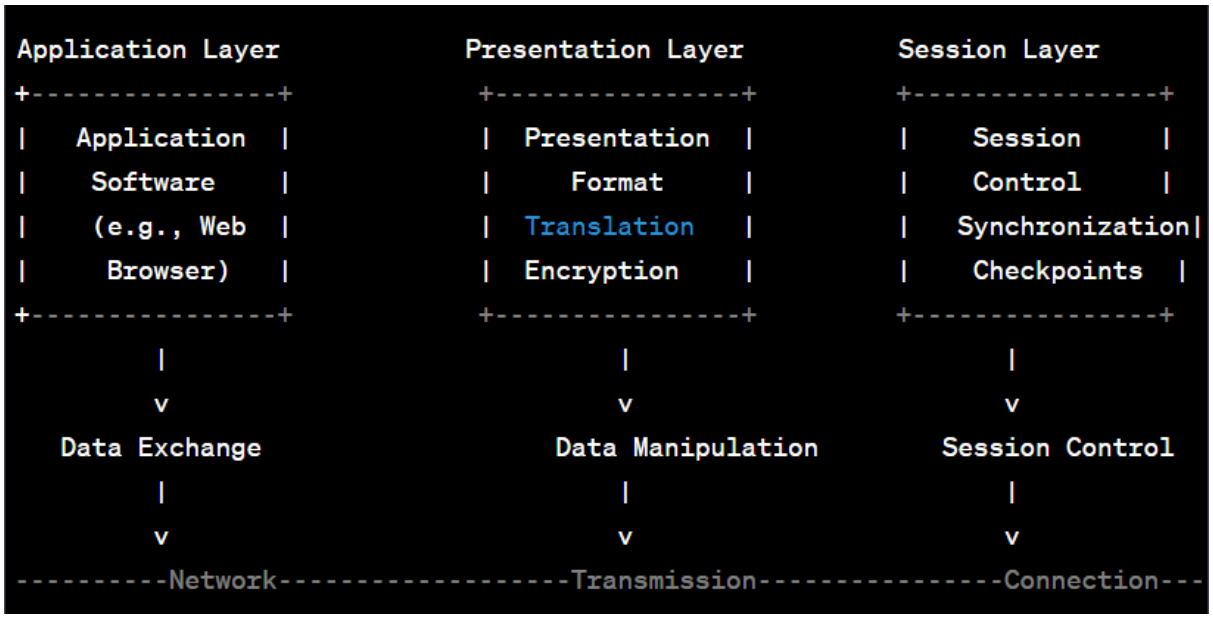
1. Network Services: The Application Layer provides a variety of network services that applications can use, such as email (SMTP), file transfer (FTP), remote access (SSH), and web browsing (HTTP).

2. User Interface: It offers a user-friendly interface for users to interact with applications and services over the network.

3. Data Exchange: The Application Layer manages the exchange of data between different devices and software applications, providing seamless communication between users.

4. Authentication and Authorization: It includes mechanisms for user authentication and authorization, ensuring secure access to network resources.

Block Diagram:



In the block diagram:

- The Application Layer interacts with user applications and provides network services.

- The Presentation Layer performs data translation, encryption, and compression.

- The Session Layer manages synchronization and session control between applications.