Computer Network Applications

Computer networks play a vital role in modern technology and are the foundation of many applications. These applications enable communication, data sharing, resource management, and much more. Here are the primary applications of computer networks:

1. Email and Messaging

- Description: Email is one of the earliest and most widely used applications of computer networks. Instant messaging (IM) and chat applications also rely on networks for real-time communication.
- Examples:
    - Email: Gmail, Outlook.
    - Messaging apps: WhatsApp, Telegram, Slack.

2. File Sharing and Cloud Storage

- Description: Computer networks enable the sharing and access of files between users, and with the advent of cloud storage, files can be stored and retrieved from remote servers.
- Examples:
    - File sharing: Google Drive, Dropbox, OneDrive.
    - Cloud storage: Amazon S3, Google Cloud Storage.

3. World Wide Web (WWW) and Browsing

- Description: The World Wide Web is the largest and most common application of computer networks, where users can access information and interact with websites.
- Examples:
    - Web browsing via HTTP/HTTPS protocols (Chrome, Firefox).
    - Web applications like online shopping (Amazon), e-learning (Coursera), and social media (Facebook, Twitter).

4. Remote Access and Teleworking

- Description: Computer networks enable users to remotely access other computers, servers, or systems, allowing people to work from anywhere.
- Examples:

    - Remote desktop applications: Microsoft Remote Desktop, AnyDesk, TeamViewer.
    - Virtual Private Networks (VPNs): Used for secure remote access to organizational networks.

5. Video Conferencing and Voice over IP (VoIP)

- Description: Networks support video conferencing and voice communication over the Internet (VoIP), enabling remote meetings and communication.
- Examples:
    - Video conferencing: Zoom, Microsoft Teams, Google Meet.
    - VoIP: Skype, WhatsApp calls, Google Voice.

6. Online Gaming

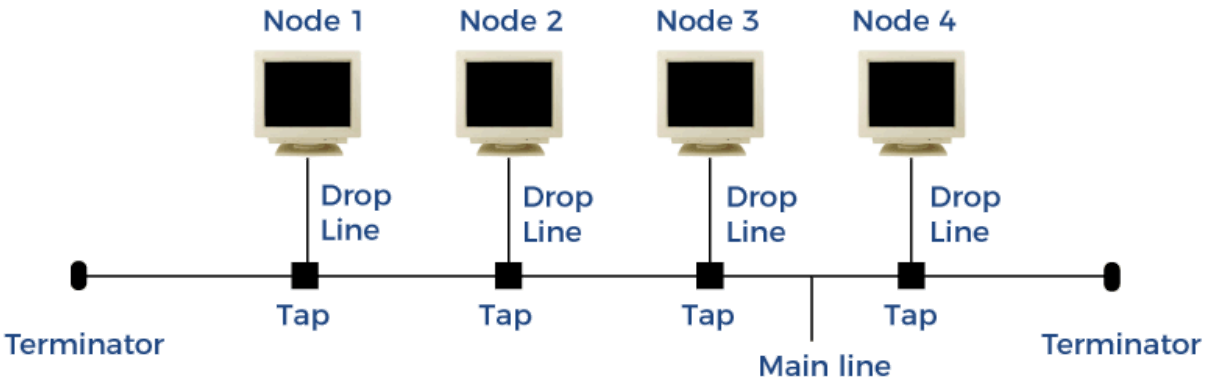
- Description: Multiplayer online games rely on computer networks to connect players from around the world in real time.
- Examples:
    - Online gaming platforms: Steam, Xbox Live, PlayStation Network.
    - Popular games like Fortnite, League of Legends, Call of Duty.

7. E-Commerce

- Description: E-commerce applications allow users to buy and sell goods and services over the Internet, and rely on secure computer networks for transactions.
- Examples:
    - E-commerce websites: Amazon, eBay, Alibaba.
    - Payment gateways: PayPal, Stripe.

TYPES OF NETWORK TOPOLOGIES , THEIR ADVANTAGES AND DISADVANTAGES

1. Bus Topology

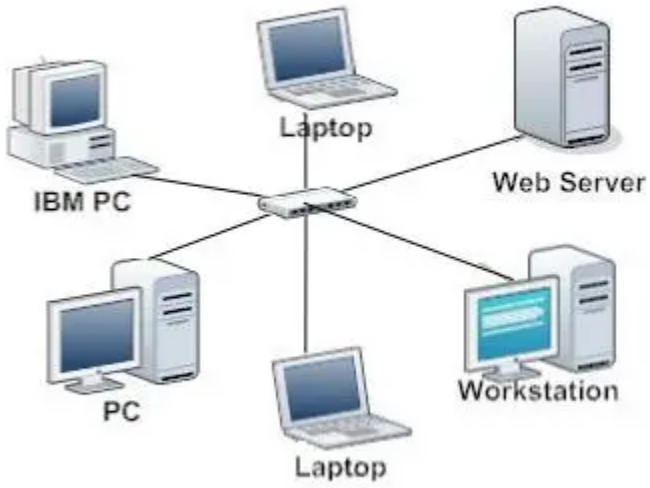


Bus Topology

- Description: All devices are connected to a single continuous cable (the "bus" or backbone). Data is sent from one device and travels along the bus to all other devices.
- Advantages:
    - Easy to set up and requires less cable than other topologies.
    - Suitable for small networks.
    - Cost-effective for small networks.
- Disadvantages:
    - Limited by cable length and the number of devices it can support.
    - A failure in the backbone cable brings down the entire network.
    - Troubleshooting can be difficult.
    - Performance degrades as more devices are added.
- Use Cases: Small networks, legacy systems, older Ethernet networks.

---

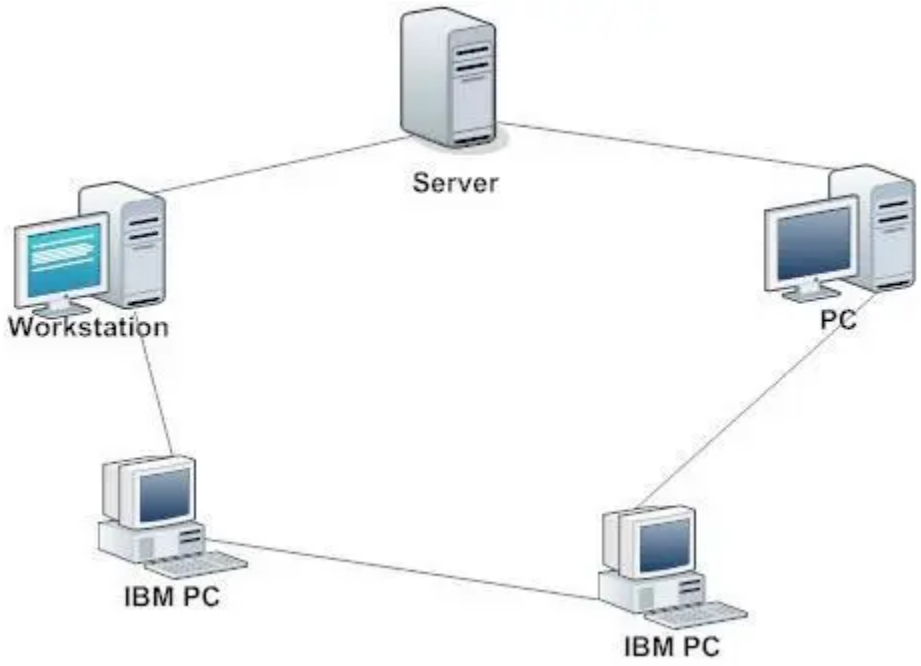
2. Star Topology



- Description: All devices are connected to a central hub or switch. Data passes through the hub before reaching its destination.
- Advantages:
    - Easy to install and expand.
    - Centralized management and troubleshooting.
    - If one device fails, the rest of the network is unaffected.
    - High performance with minimal data collisions.
- Disadvantages:
    - Requires more cables than bus topology (since each device has a dedicated connection to the hub).
    - If the central hub or switch fails, the entire network goes down.
    - Hub/switch adds cost to the network setup.
- Use Cases: Office networks, home networks, large organizations.

---

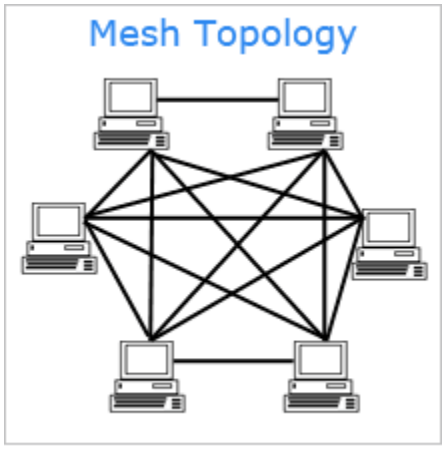
3. Ring Topology



- Description: Devices are connected in a circular fashion, where each device has exactly two neighbors for communication. Data travels in one or both directions around the ring.
- Advantages:
    - Equal access to the network for all devices.
    - Can handle high volumes of traffic (if using token-passing for data transmission).
    - Each device has a specific role, reducing data collisions.
- Disadvantages:
    - A break in the cable can disrupt the entire network.
    - Troubleshooting can be difficult.
    - Adding or removing devices disrupts the network.
- Use Cases: Token Ring networks, some metropolitan area networks (MANs), industrial applications.

---

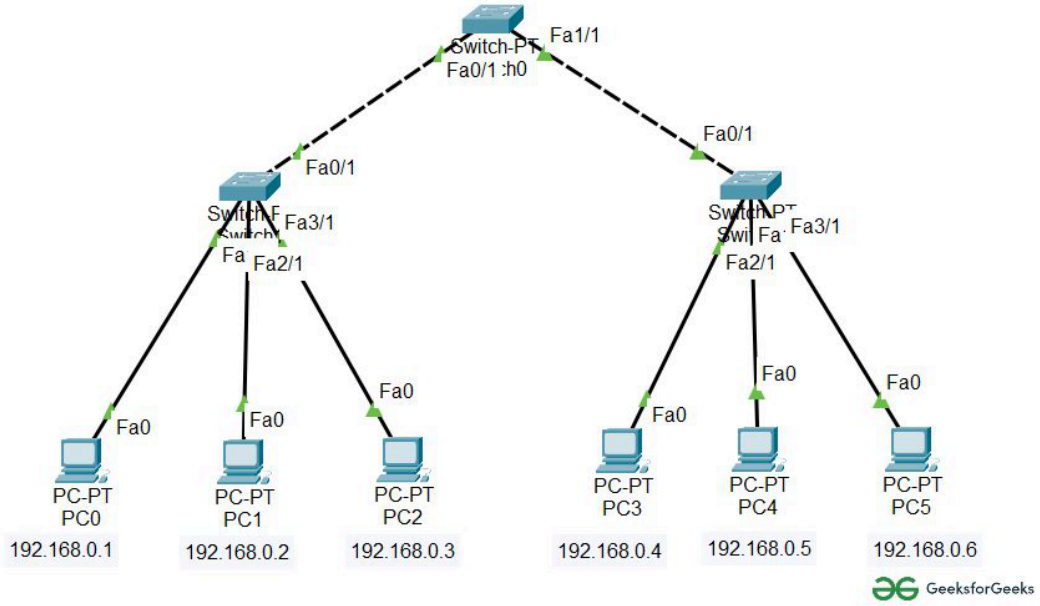
4. Mesh Topology



- Description: In a mesh topology, every device is connected to every other device. This creates a highly redundant network with multiple paths for data transmission.
- Two types:
    - Full Mesh: Every device is connected to every other device.
    - Partial Mesh: Some devices are fully connected, while others are only connected to certain devices.
- Advantages:
    - Highly reliable due to redundant paths. If one link fails, data can still be transmitted through another path.
    - Excellent for fault tolerance and high-performance networks.
    - Suitable for networks where uptime is critical (no single point of failure).
- Disadvantages:
    - Very expensive due to the high number of connections and cables required.
    - Difficult to set up and maintain, especially for large networks.
- Use Cases: Military applications, data centers, large industrial networks, and networks where reliability is critical.

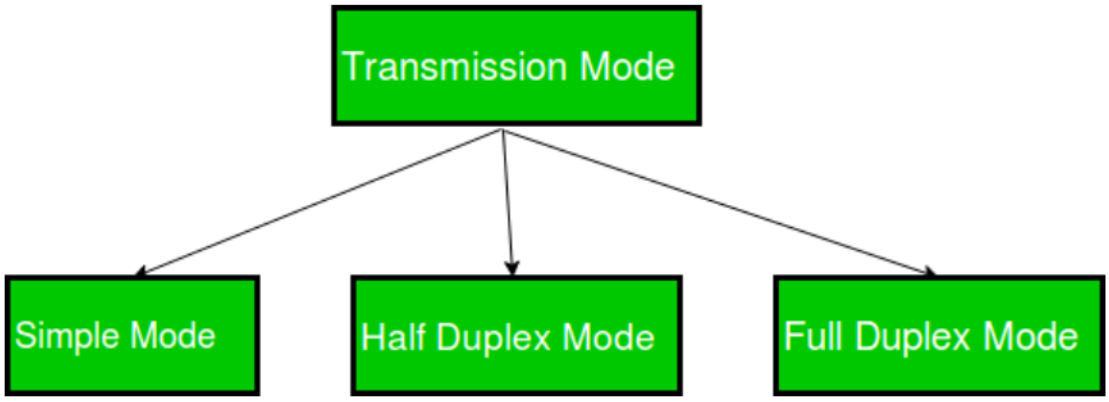
---

5. Tree Topology



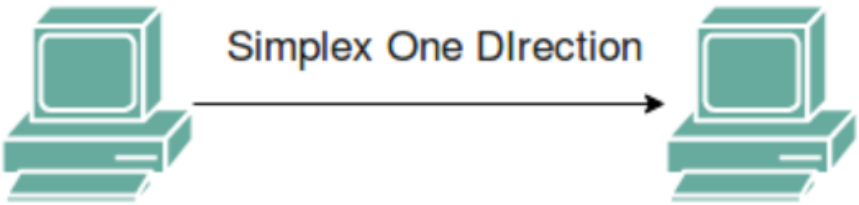
- Description: A hybrid topology that combines elements of both star and bus topologies. Devices are arranged in a hierarchical manner, with the central node being a hub or switch that connects to several branches (sub-networks) that have their own hubs or switches.
- Advantages:
    - Easy to expand by adding additional branches.
    - Centralized management and hierarchical structure.
    - If one branch goes down, the rest of the network is not affected.
- Disadvantages:
    - If the central hub or switch fails, the entire network segment is down.
    - Requires more cables and is more expensive compared to bus topology.
- Use Cases: Corporate networks, large university campuses, hierarchical office networks.

Types of Data Flow



In the context of computer networks, data flow refers to the direction in which data can travel between two communication devices or nodes. There are three primary types of data flow in networking:

1. Simplex Mode

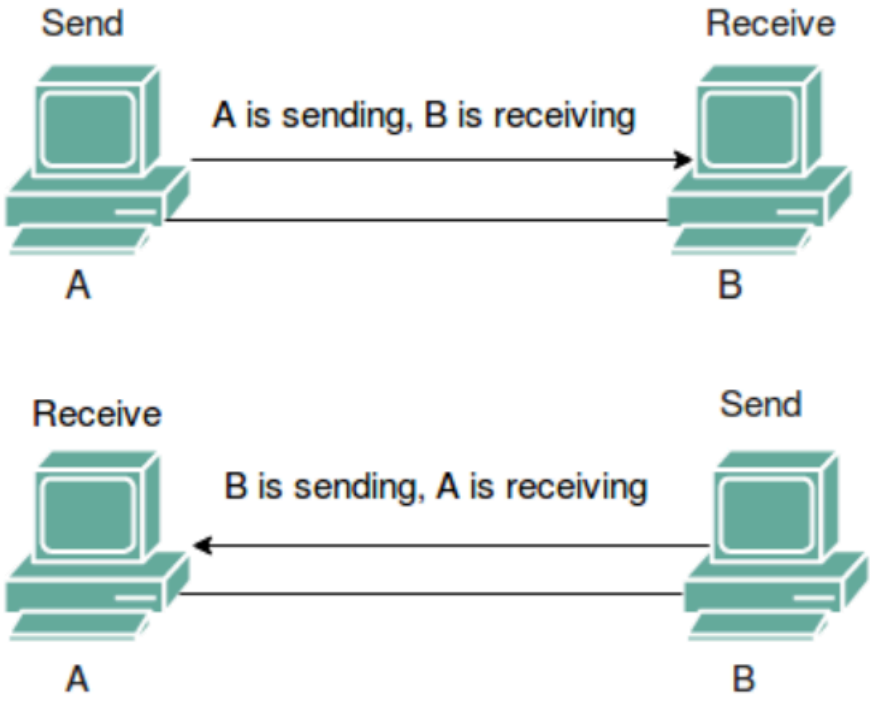


- Definition: In simplex mode, the data flows in one direction only, from a sender to a receiver. The sender can transmit data, but the receiver cannot send data back to the sender.
- Example:
    - A keyboard sending data to the computer.
    - A television broadcast where the signal is sent from the broadcaster to the TV, but no data is sent back from the TV to the broadcaster.
- Advantages:
    - Simple to implement.

    - Useful in scenarios where communication is one-way and feedback is not needed.
- Disadvantages:
    - No capability for two-way communication.
    - The receiver cannot send acknowledgments or feedback, which may be necessary in many systems.
- Use Cases: Broadcast systems, sensors, keyboards, and monitors.

---

2. Half-Duplex Mode

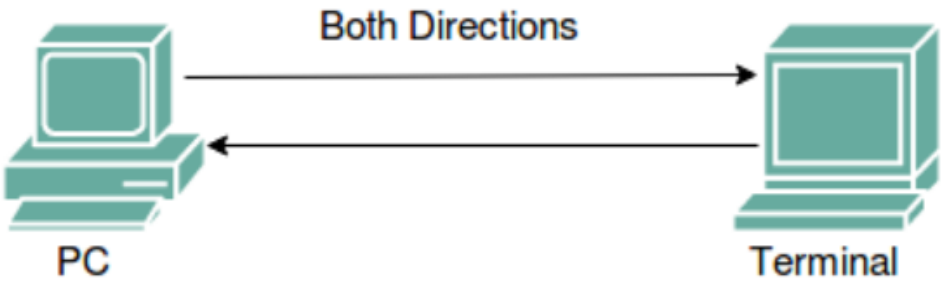


- Definition: In half-duplex mode, data can flow in both directions, but only one direction at a time. When one device is sending data, the other device must wait until the transmission is complete before it can send data back.
- Example:
    - Walkie-talkies, where one person talks and the other listens, and then they switch roles.
    - Ethernet networks operating in half-duplex mode, where data transmission occurs in one direction at a time.
- Advantages:
    - Allows two-way communication using a single communication channel.

    - More efficient than simplex in situations where bidirectional communication is needed, but simultaneous transmission is not required.
- Disadvantages:
    - Communication is not simultaneous, so it may introduce delays.
    - Only one party can send data at a time, which can be inefficient in high-traffic situations.
- Use Cases: Walkie-talkies, older Ethernet connections, and some communication protocols.

---

3. Full-Duplex Mode



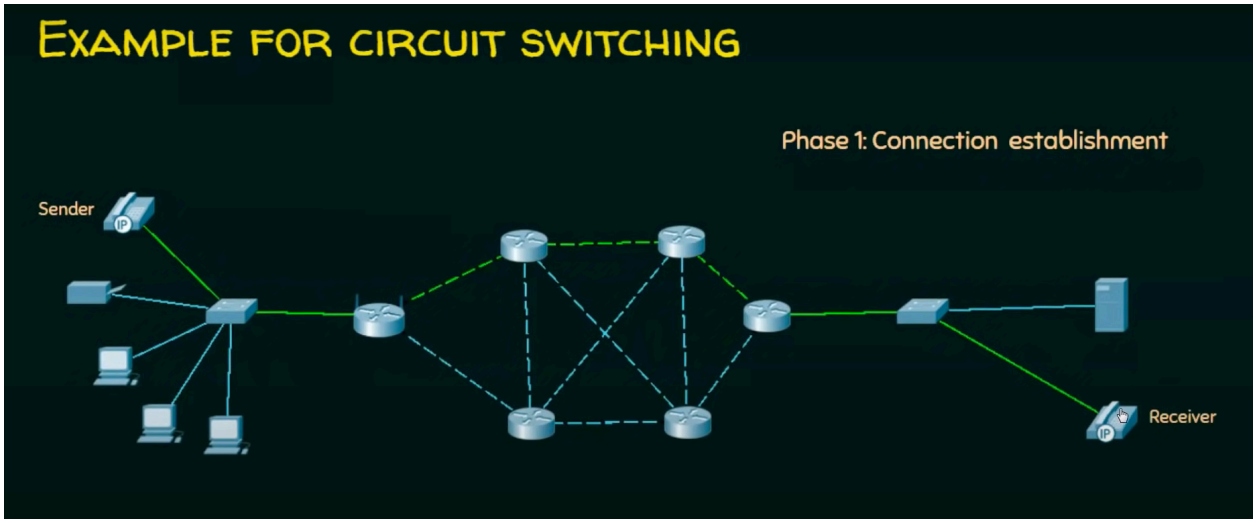
- Definition: In full-duplex mode, data can flow in both directions simultaneously. Both devices can send and receive data at the same time without any interference.
- Example:
    - Telephones, where both parties can talk and listen at the same time.
    - Modern Ethernet and Wi-Fi connections that allow simultaneous data transmission and reception.
- Advantages:
    - Efficient two-way communication with no delays caused by waiting for one device to finish transmitting.
    - Maximizes bandwidth usage since both directions are utilized at the same time.
- Disadvantages:
    - More complex and expensive to implement than simplex or half-duplex modes.
- Use Cases: Modern telecommunication systems, full-duplex Ethernet, Wi-Fi networks, and many real-time communication systems.

SWITCHING IN COMPUTER NETWORKS

In computer networking, Switching is the process of transferring data packets from one device to another in a network, or from one network to another, using specific devices called switches.

1. Circuit Switching

In **circuit switching**, a dedicated communication path or circuit is established between the sender and receiver for the entire duration of the communication.



Advantages:

- **Dedicated Connection**: Guarantees consistent and predictable communication since the entire bandwidth of the circuit is reserved.
- **Low Delay**: Once the circuit is established, there is no delay in transmission because of the dedicated path.
- **Reliable Data Transfer**: Ideal for real-time communications, like voice calls, where a constant and reliable connection is needed.

Disadvantages:

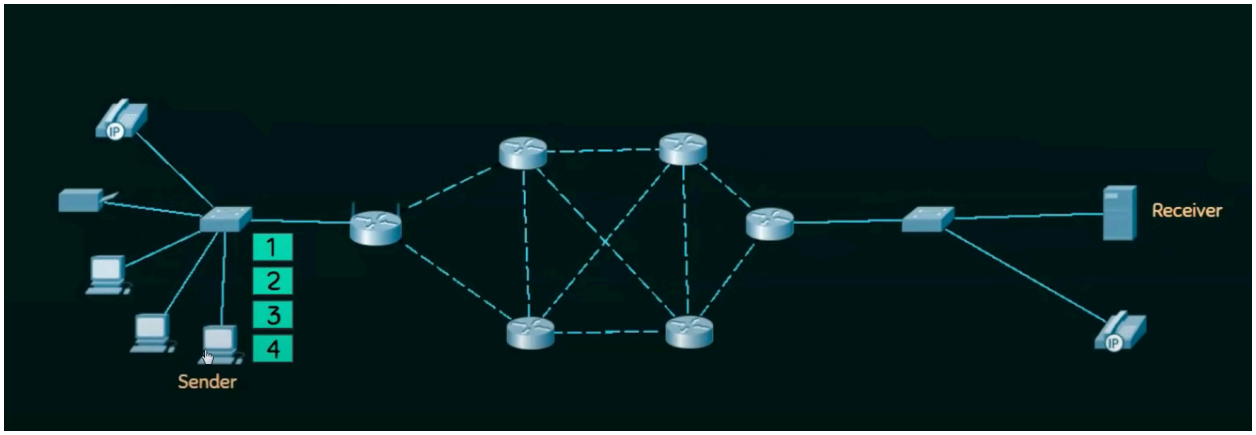
- **Inefficient Use of Resources**: The reserved circuit remains unused when no data is being transmitted, leading to inefficient bandwidth usage.
- **Setup Delay**: Setting up the circuit before communication can introduce delays.
- **Scalability Issues**: Maintaining dedicated circuits for multiple users simultaneously is difficult as network size increases.

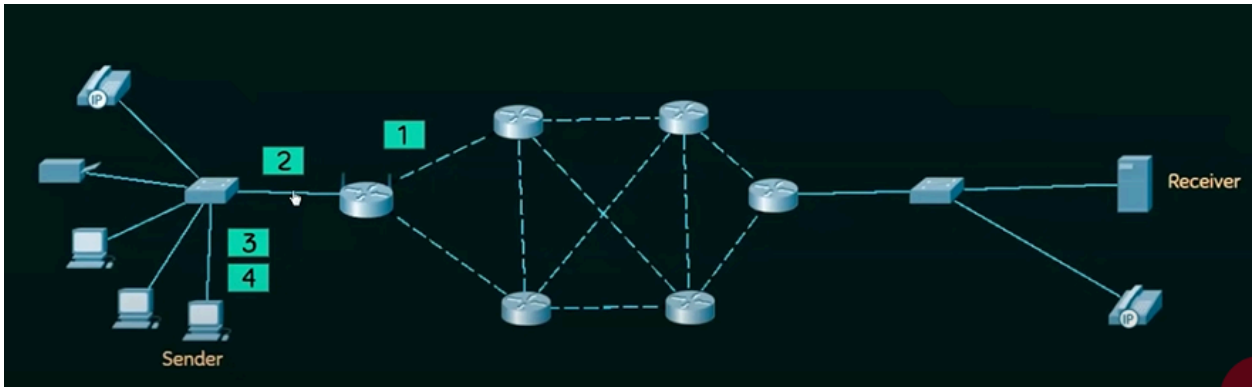
Example: Traditional telephone networks.

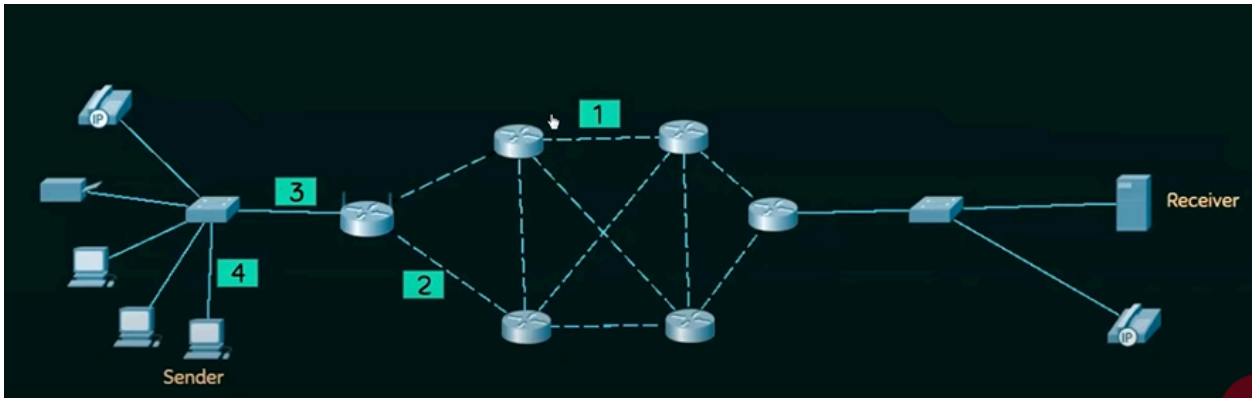
---

2. Packet Switching

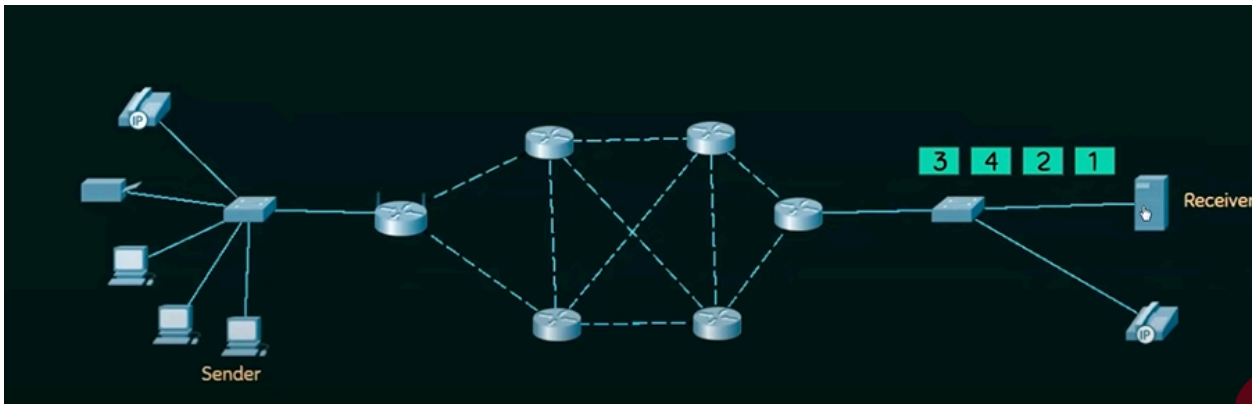
In **packet switching**, data is broken down into small packets, which are transmitted independently through the network and reassembled at the destination.







b



Advantages:

- **Efficient Use of Bandwidth**: Network resources are shared, and packets from different users can travel over the same links, making it more efficient.
- **Fault Tolerance**: If one path fails, packets can be rerouted through other available paths, enhancing reliability.
- **Scalable**: Easily scalable as the network grows, handling more traffic by using existing resources efficiently.

Disadvantages:

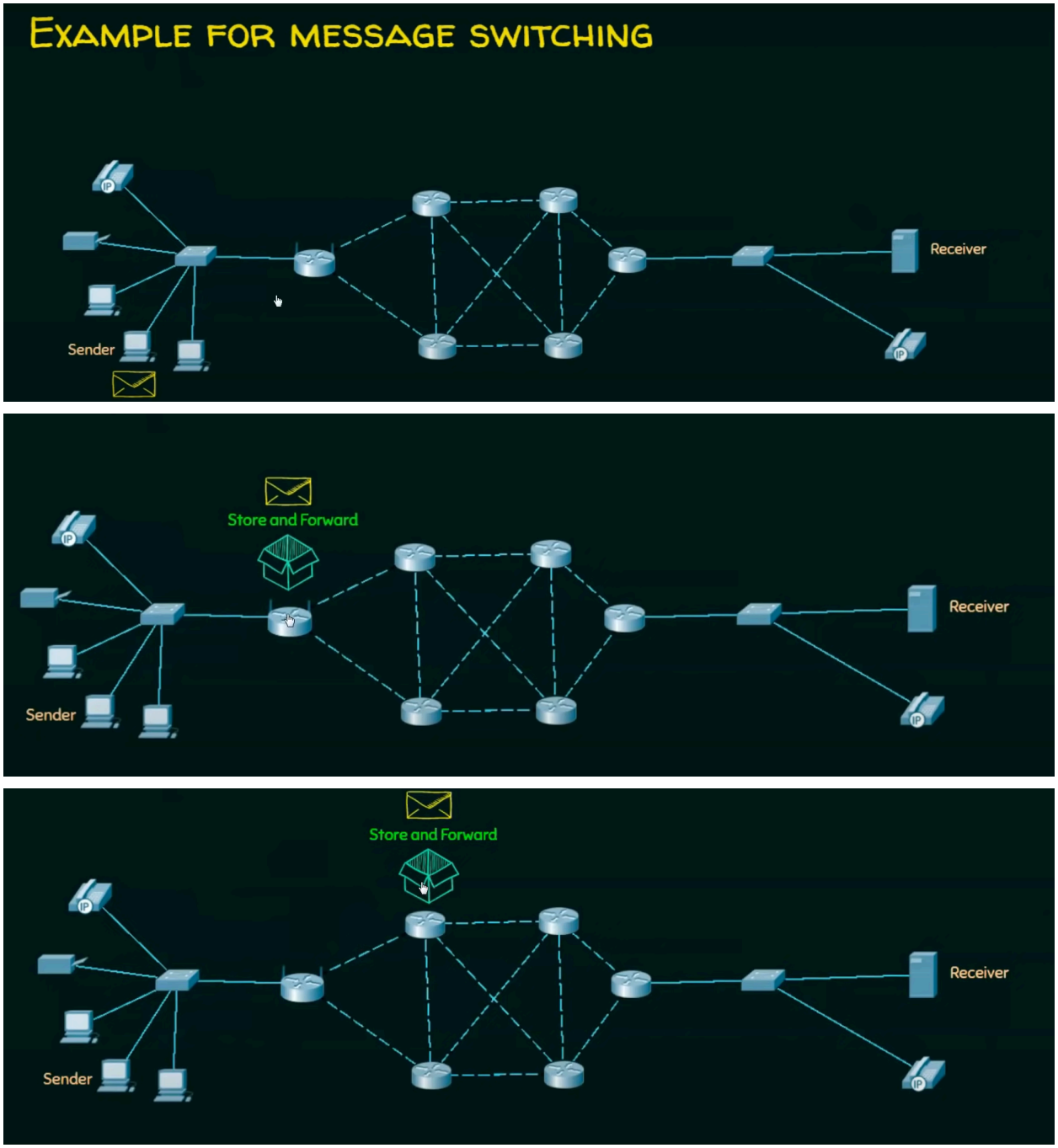
- **Variable Delay (Latency)**: Due to the dynamic routing of packets, they may take different paths, causing variable latency.

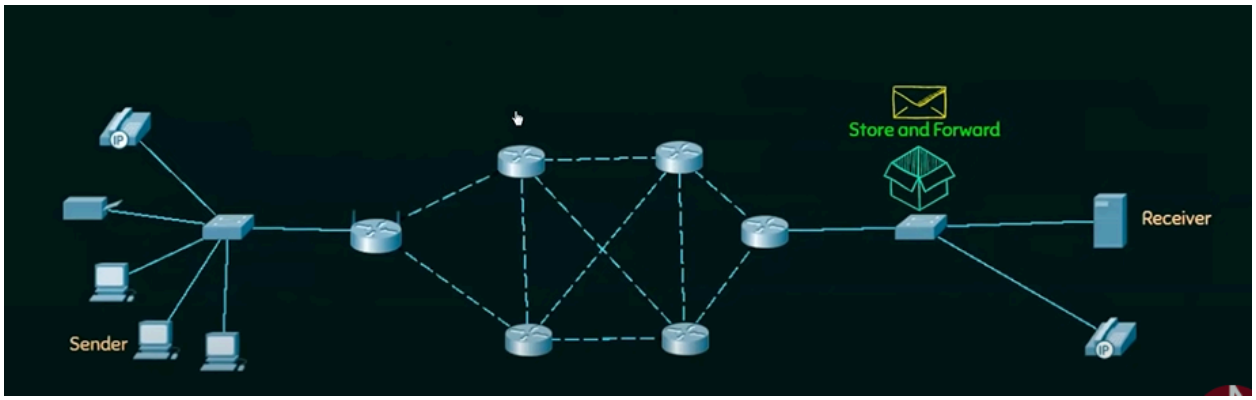
- **Packet Loss**: There's a chance that some packets may get lost, requiring retransmission, which affects data integrity.
- **Overhead**: Each packet carries addressing information, increasing overhead.

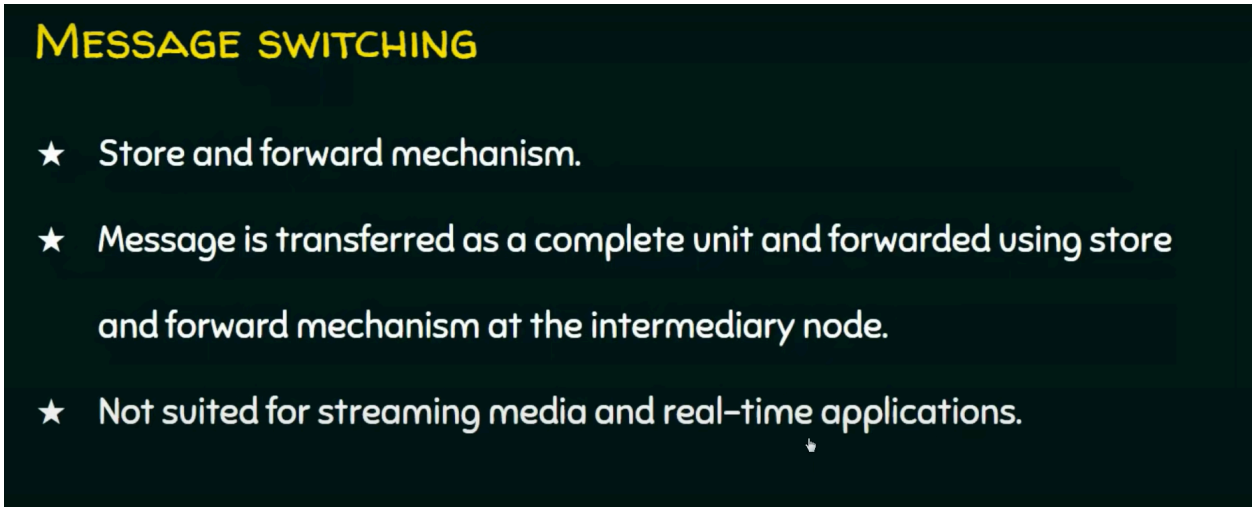
Example: The Internet, where data is transmitted in packets using the TCP/IP protocol.

---

3. Message Switching







In **message switching**, entire messages are transmitted, hop by hop, from one switch to another until they reach the destination. Each intermediate switch stores the complete message before forwarding it, known as the **store-and-forward** technique.

Advantages:

- **No Need for Dedicated Path**: No need for a dedicated connection between sender and receiver.
- **Efficient Bandwidth Usage**: Since data is transmitted as complete messages, network resources are used only when needed.

Disadvantages:

- **High Latency**: Each switch must store the entire message before forwarding, leading to significant delays.
- **Storage Overhead**: Each switch requires enough storage to store the entire message, which can be a limitation for large messages.
- **No Real-Time Communication**: The delay introduced by storing and forwarding makes it unsuitable for real-time applications like voice or video calls.

Example: Telegraph networks used in early communications, email systems.

Difference between Circuit switching and packet switching

Feature	Circuit Switching	Packet Switching
Definition	Establishes a dedicated communication path or circuit between two endpoints for the duration of the call or session.	Divides data into packets that are transmitted independently across the network without a dedicated path.
Connection	A connection is established before data transfer begins.	No prior connection establishment; packets are sent as needed.
Data Transmission	Continuous stream of data is sent over the established circuit.	Data is broken into packets that can take different routes to the destination.
Resource Allocation	Resources (bandwidth) are reserved for the entire duration of the call.	Resources are shared among users; bandwidth is allocated dynamically based on demand.
Delay	Low latency after the connection is established, as there is no waiting for packet routing.	Variable delay due to routing and potential congestion, as packets may take different paths.

Reliability	Highly reliable for real-time applications because the dedicated circuit minimizes data loss.	Packets can be lost or arrive out of order; protocols (like TCP) manage retransmission and order.
Efficiency	Inefficient use of bandwidth, as unused capacity remains allocated during silent periods (e.g., during a phone call).	More efficient use of bandwidth, as multiple users can share the same paths, and bandwidth is utilized only when packets are transmitted.
Scalability	Less scalable due to fixed paths for connections; adding more connections can lead to congestion.	Highly scalable, as new packets can be sent over any available route without congestion on a fixed path.
Best Suited For	Real-time communication applications, such as traditional voice calls and video conferencing.	Data-centric applications, such as the Internet, email, and file transfers, where real-time delivery is not critical.

Networking Parameters (Transmission Impairment, Data Rate and Performance)

Transmission Impairment

Transmission impairment refers to the degradation of signal quality as it travels through a medium. This degradation can affect the reliability and clarity of data transmission. The main types of transmission impairments include:

- **Attenuation**:
  - **Definition**: The reduction in signal strength as it travels over distance.
  - **Impact**: Causes loss of signal power, which may lead to increased errors if the signal is not amplified or regenerated.
- **Noise**:
  - **Definition**: Unwanted electrical signals that interfere with the transmitted signal.
  - **Types**:
    - **Thermal Noise**: Generated by the random motion of electrons in a conductor.
    - **Cross-talk**: Interference from signals in adjacent cables or circuits.

        - **Impulse Noise**: Sudden spikes in voltage that can disrupt signal transmission.
    - **Impact**: Can distort the signal, causing bit errors and requiring retransmission.
- **Distortion**:
    - **Definition**: The alteration of the signal waveform during transmission.
    - **Types**:
        - **Amplitude Distortion**: Changes in the amplitude of different frequency components.
        - **Phase Distortion**: Changes in the phase of the signal components.
    - **Impact**: Can lead to misinterpretation of the data received.

2. Data Rate

Data rate is the amount of data transmitted over a network in a given amount of time, usually measured in bits per second (bps). The data rate can be influenced by various factors, including:

- **Bandwidth**:
    - **Definition**: The maximum rate at which data can be transmitted over a communication channel, often measured in hertz (Hz).
    - **Impact**: Higher bandwidth allows for higher data rates, enabling more data to be sent simultaneously.
- **Latency**:
    - **Definition**: The time delay between the transmission and receipt of data.
    - **Impact**: High latency can reduce effective data transfer rates, especially in applications requiring quick responses, such as online gaming or video conferencing.
- **Protocol Overheads**:
    - **Definition**: Additional bits required for error checking, acknowledgment, and control information during data transmission.
    - **Impact**: Protocol overheads reduce the effective data rate, as not all transmitted bits represent actual user data.
- **Network Congestion**:

    - **Definition**: A situation where the network resources are insufficient to handle the volume of data being transmitted.
    - **Impact**: Can lead to reduced data rates due to increased delays and packet loss, requiring retransmission.

3. Performance

Performance in networking refers to how well a network meets its intended purpose, often measured by various metrics, including:

- **Throughput**:
    - **Definition**: The actual data rate achieved in a network, accounting for overhead, delays, and losses, typically measured in bps.
    - **Impact**: Indicates how much usable data is successfully delivered to the destination over time.
- **Latency**:
    - **Definition**: The time taken for a packet of data to travel from the source to the destination.
    - **Impact**: Lower latency improves performance, particularly in real-time applications.
- **Jitter**:
    - **Definition**: The variation in packet arrival times.
    - **Impact**: High jitter can affect the quality of real-time communications (e.g., VoIP and video calls) by causing interruptions and delays.
- **Error Rate**:
    - **Definition**: The percentage of packets that are lost or corrupted during transmission.
    - **Impact**: A high error rate necessitates retransmissions, reducing effective throughput and overall performance.

.

Data Link Layer	
3.1	Error Detection and Correction – Hamming Code, CRC, Checksum
3.2	Flow control mechanism – Sliding Window Protocol - GoBack - N - Selective Repeat
3.3	Multiple access Aloha - Slotted Aloha - CSMA, CSMA/CD
3.4	IEEE Standards (IEEE802.3 (Ethernet), IEEE802.11(WLAN))- RFID- Bluetooth Standards

The **Data Link Layer** is the **second layer** of the **OSI (Open Systems Interconnection)** model.
The **Data Link Layer** is responsible for **reliable data transfer** between two directly connected devices (nodes) over a physical link.
It ensures that data received at the destination is **error-free, properly ordered, and without duplication**.

Framing:

- Divides the data from the Network Layer into manageable units called **frames**.
- Adds headers and trailers to each frame for synchronization and error detection.

Error Detection and Correction:

- Detects and sometimes corrects errors that may occur during transmission.
- Uses techniques like **CRC (Cyclic Redundancy Check) ,Checksum, Hamming codeParity Bits.**

Flow Control:

- Ensures that a fast sender doesn't overwhelm a slow receiver with too much data.
- Example: Stop-and-Wait and Sliding Window protocols.

Access Control (MAC):

- Determines which device has permission to use the link at a given time, especially in shared media like LAN.
- Handled by **Media Access Control (MAC) sublayer**.

Acknowledgment and Retransmission:

- Confirms receipt of frames and retransmits lost or corrupted ones.

Flow control mechanism – Sliding Window Protocol - GoBack - N - Selective Repeat

Flow control is a technique used to regulate the rate of data transmission between two nodes (sender and receiver) in a network.
It ensures that the sender does not overwhelm the receiver by sending data faster than it can process or store.

🔹 **Why Flow Control is Required**

1. To Prevent Receiver Overload

- **The sender might transmit data at a high rate, but the receiver may have limited buffer capacity.**

- **Without flow control, the receiver's buffer could overflow, causing data loss or retransmissions.**
  ✅ ***Flow control ensures that the sender sends data only at a rate the receiver can handle.***

---

2. To Ensure Reliable Communication

- **Data may get lost if the receiver discards packets due to overflow.**

- **Flow control helps maintain data integrity and reliability, ensuring that every transmitted frame is correctly received and acknowledged.**

---

3. To Optimize Network Efficiency

- **If data packets are frequently lost and retransmitted, the network bandwidth is wasted.**

- **Proper flow control helps reduce retransmissions and improves the overall throughput of the network.**

---

4. To Synchronize Sender and Receiver Speeds

- **In real-world communication, devices have different processing speeds.**
  Example: A powerful server sending data to a slower personal computer.

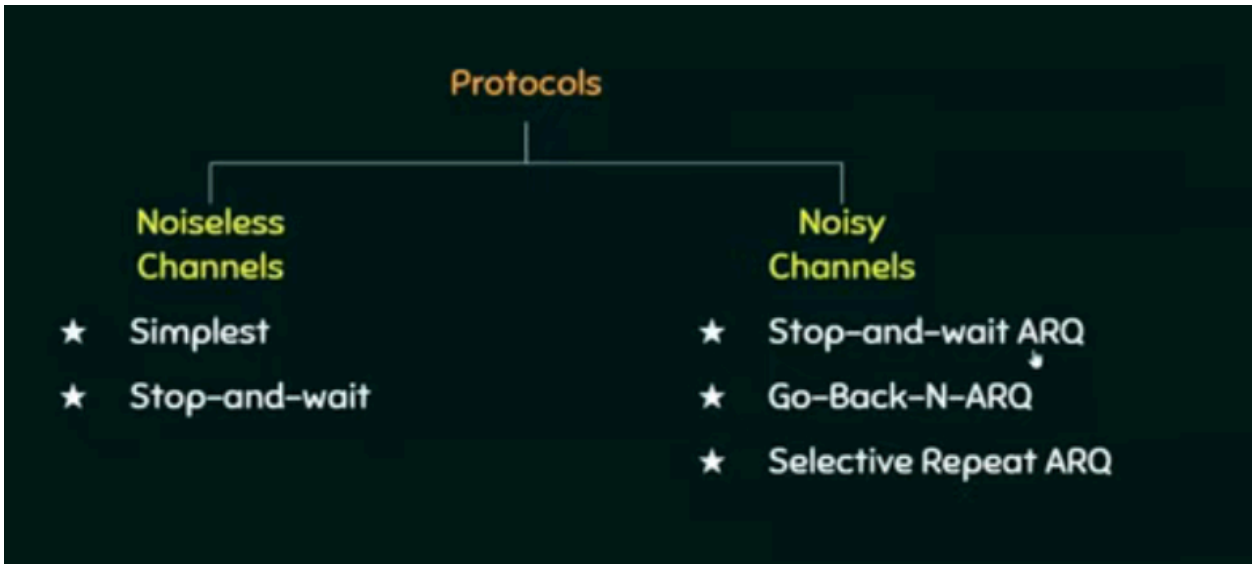
- **Flow control keeps both devices synchronized so that data flow matches the receiver's speed.**

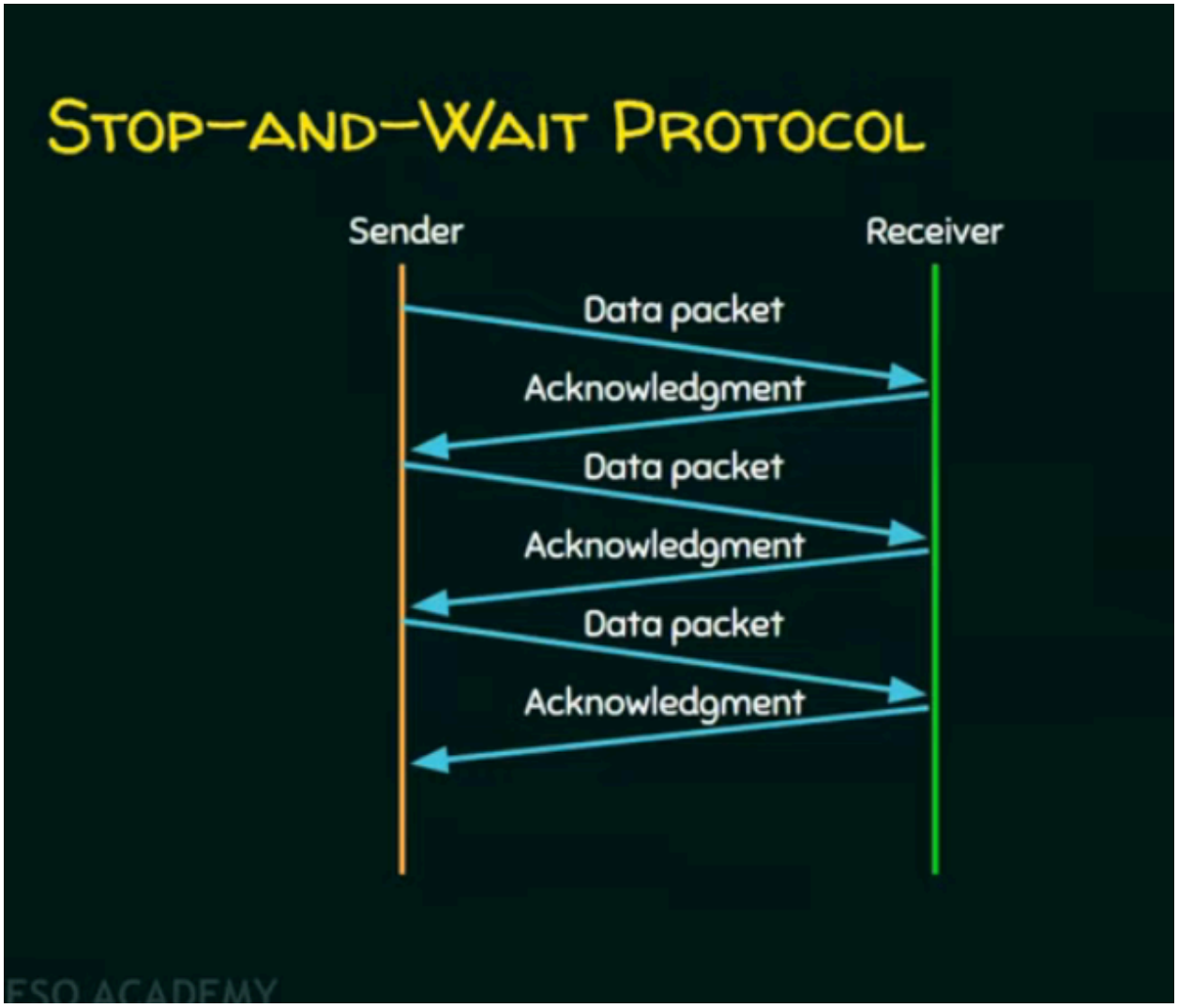
---

5. To Prevent Congestion

- **When many senders transmit data at high speeds, routers and switches can get congested.**

- **Flow control, along with congestion control, helps manage traffic and prevents network congestion.**



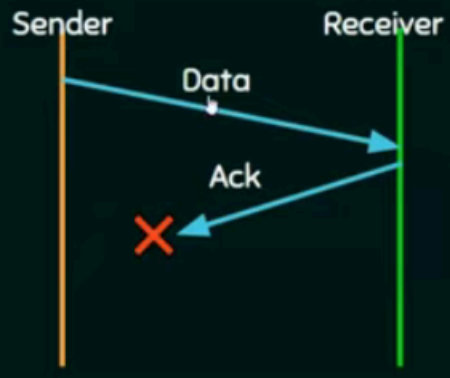

STOP-AND-WAIT PROTOCOL
Sender
Receiver
Data packet
Acknowledgment
Data packet
Acknowledgment
Data packet
Acknowledgment
ESO ACADEMY

Problems of Stop-and-Wait Protocol

1. Problems due to lost data.
   - ★ Sender waits for ack for an infinite amount of time.
   - ★ Receiver waits for data an infinite amount of time.

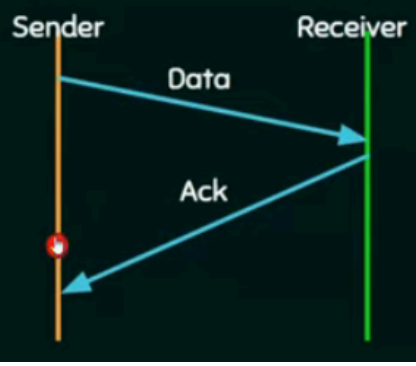
Problems of Stop-and-Wait Protocol

2. Problems due to lost ACK.
   - ★ Sender waits for an infinite amount of time for ack.

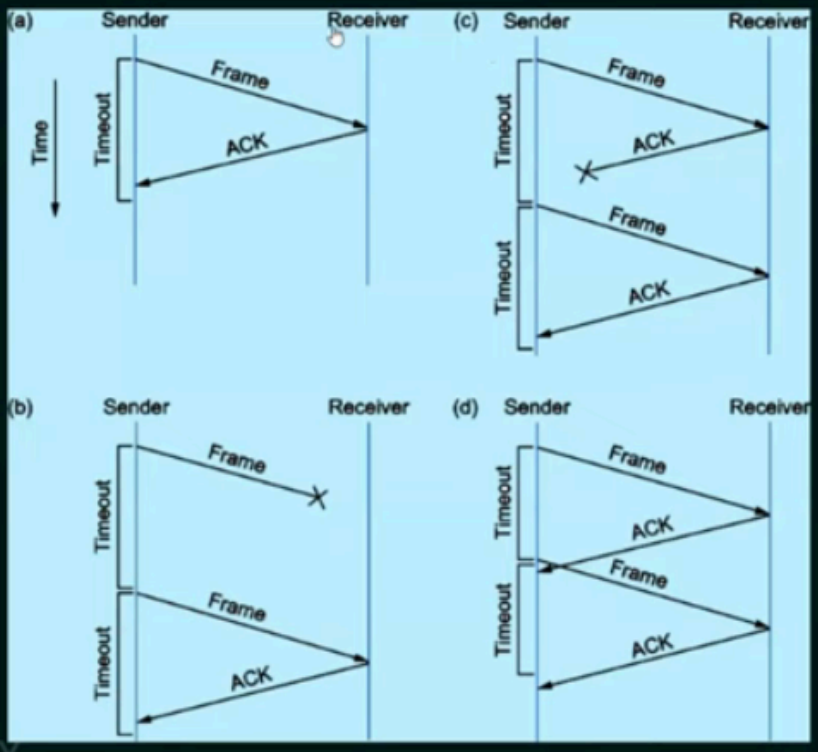


Problems of Stop-and-Wait Protocol

3. Problems due to delayed ACK/data.
   - ★ After timeout on sender side, a delayed ack might be wrongly considered as ack of some other data packet.



Stop-and-Wait ARQ Protocol



Stop-and-Wait ARQ – Drawbacks

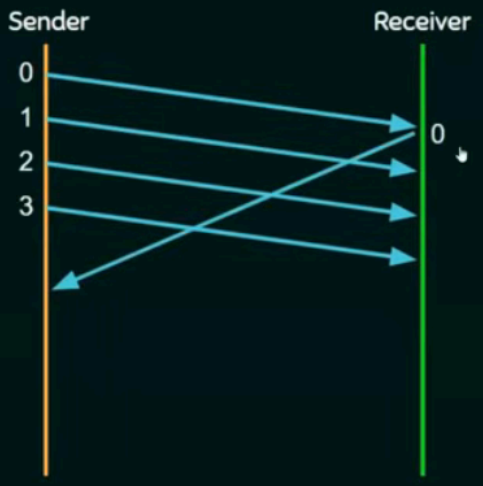
- ★ One frame at a time.
- ★ Poor utilization of bandwidth.
- ★ Poor Performance

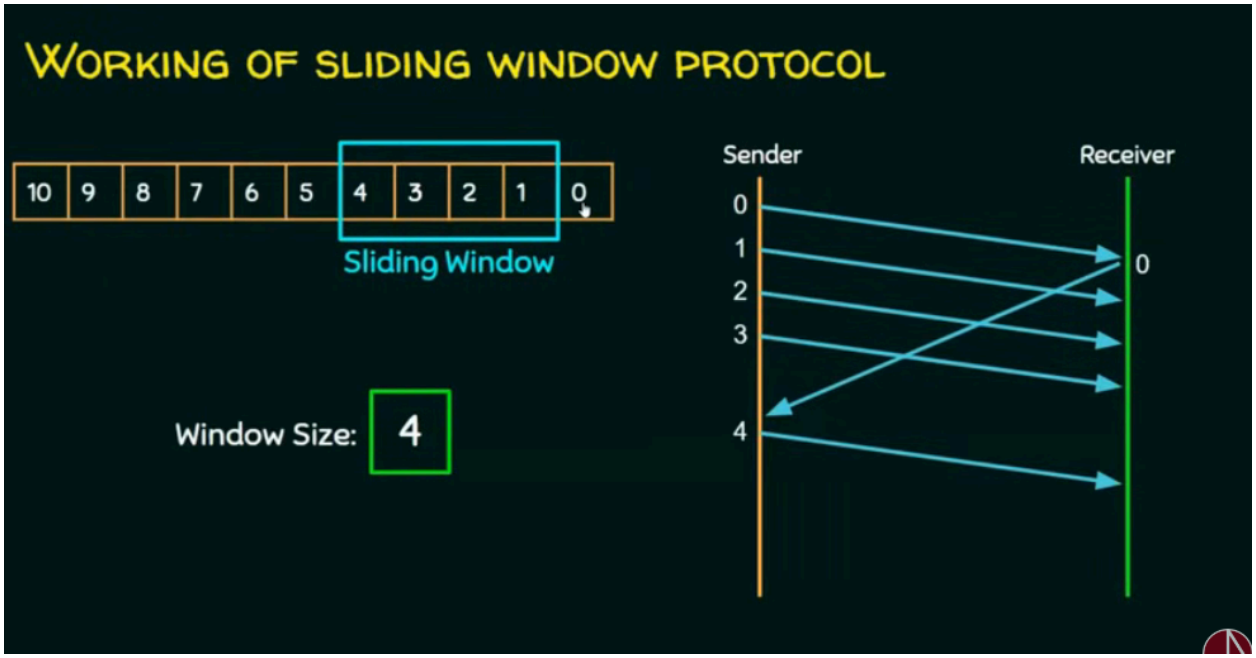
SLIDING WINDOW PROTOCOL

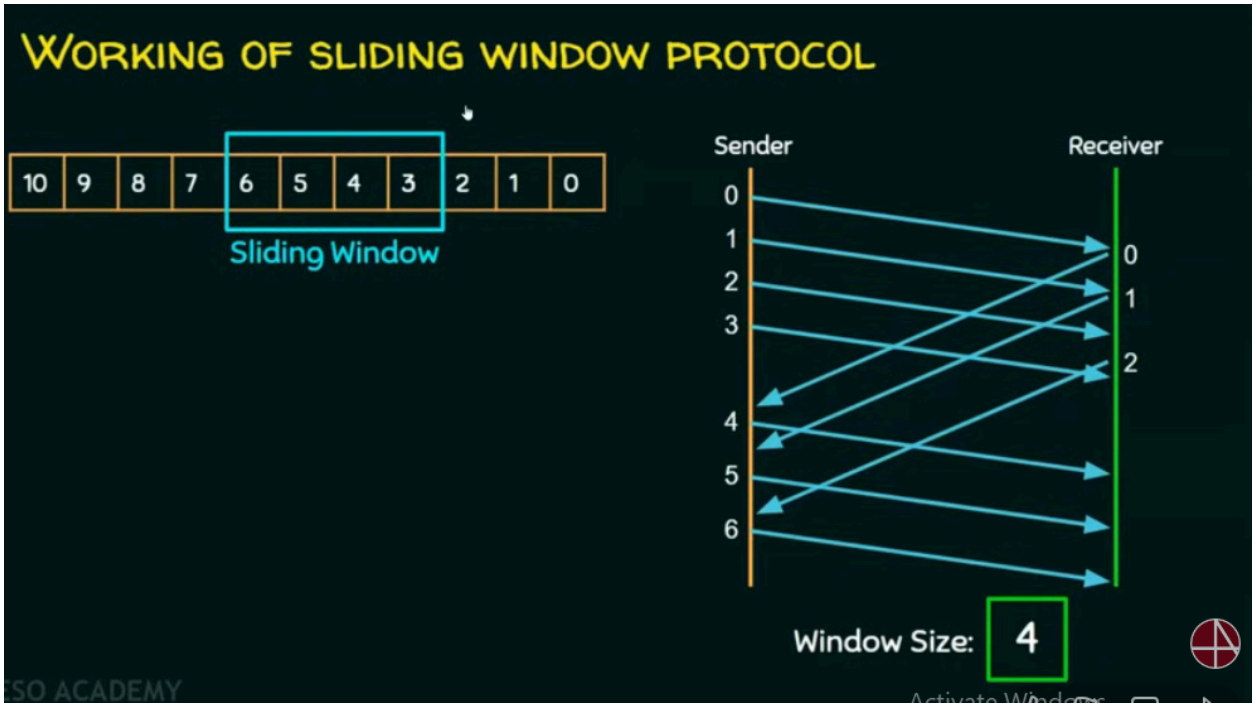
- ★ Send multiple frames at a time.
- ★ Number of frames to be sent is based on Window size.
- ★ Each frame is numbered -> Sequence number.

WORKING OF SLIDING WINDOW PROTOCOL

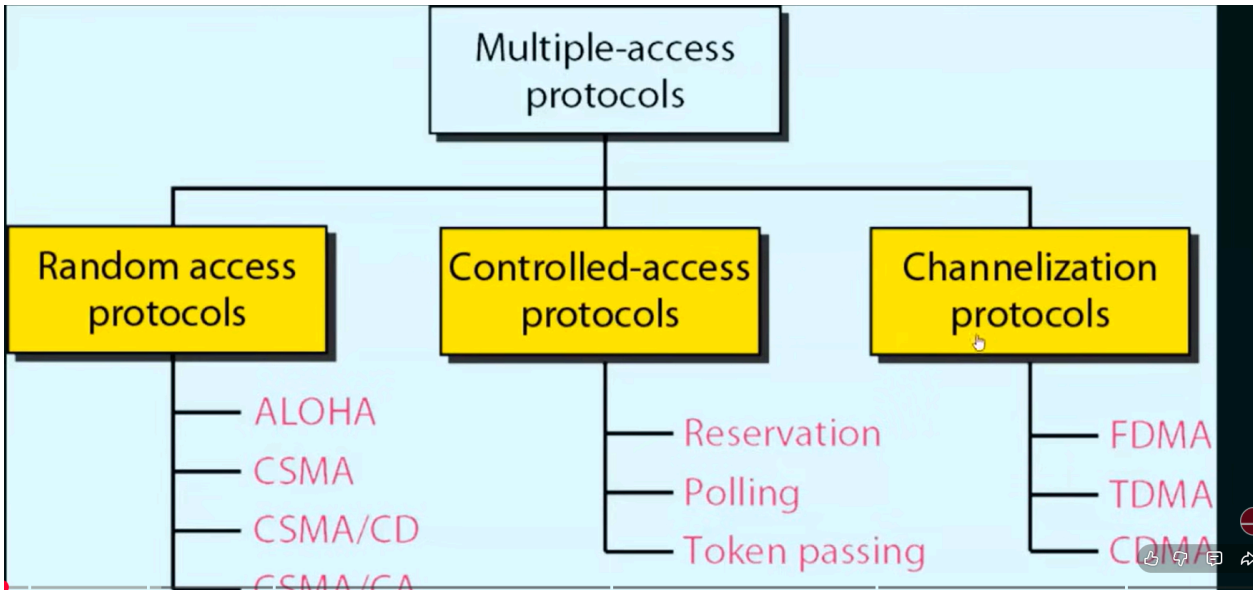
Window Size: 4




WORKING OF SLIDING WINDOW PROTOCOL
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0
1
2
3
4
0


WORKING OF SLIDING WINDOW PROTOCOL
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Sender
Receiver
0
1
2
3
4
5
6
0
1
2
Window Size: 4

A Multiple Access Protocol is a set of rules that allows multiple devices (nodes) to share and use the same communication channel without interfering with each other.



ALOHA in Computer Networks

ALOHA is a random access protocol where each device transmits data whenever it wants, without checking if the channel is free.

If two devices transmit at the same time → collision occurs, and both must retransmit after a random time.

1️⃣ Random Access Protocols

Devices transmit whenever they want.

- **ALOHA**
- **Slotted ALOHA**

- **CSMA (Carrier Sense Multiple Access)**
- **CSMA/CD (Ethernet)**
- **CSMA/CA (Wi-Fi)**

2️⃣ Controlled Access Protocols

Access is controlled or scheduled.

- **Reservation**
- **Polling**
- **Token Passing**

3️⃣ Channelization Protocols

Channel is divided among users by time, frequency, or code.

- **TDMA (Time Division Multiple Access)**
- **FDMA (Frequency Division Multiple Access)**
- **CDMA (Code Division Multiple Access)**

🌟 Types of ALOHA

There are two main types:

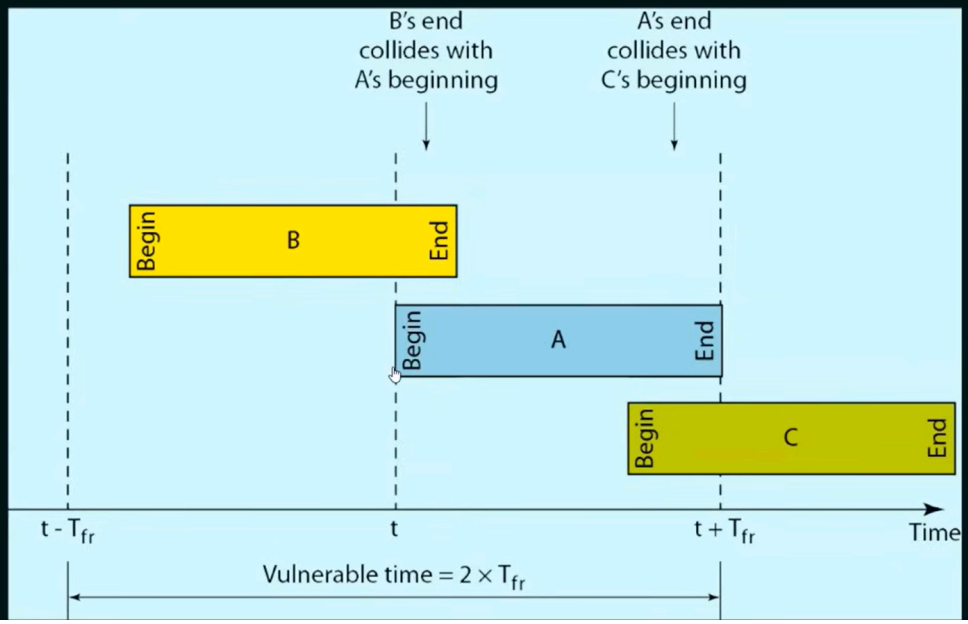
1️⃣ Pure ALOHA

- **Stations send data as soon as they have data.**
- **No checking of the channel before sending.**
- **High chance of collisions.**
- **Maximum efficiency: 18%**

PURE ALOHA

- ★ Pure ALOHA allows stations to transmit whenever they have data to be sent.
- ★ When a station sends data it waits for an acknowledgement.
- ★ If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data.

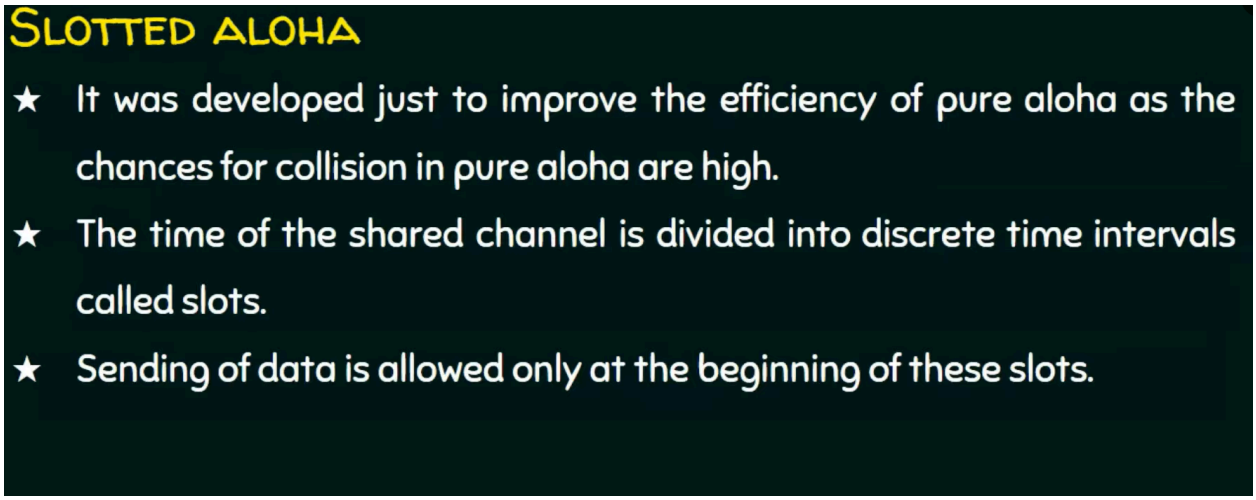
PURE ALOHA



2 Slotted ALOHA

- **Time is divided into fixed slots.**
- **Stations send data only at the beginning of a time slot.**
- **Lower collision probability.**

- **Maximum efficiency: 36%**



📌 Where ALOHA Is Used

- **Wireless communication systems**
- **Satellite communication**
- **RFID systems**
- **Early Wi-Fi concepts (influenced CSMA/CD)**

Pure Aloha	Slotted Aloha
Any station can transmit the data at any time.	Any station can transmit the data at the beginning of any time slot.
The time is continuous and not globally synchronized.	The time is discrete and globally synchronized.
Vulnerable time in which collision may occur = $2 \times T_{Fr}$	Vulnerable time in which collision may occur = T_{Fr}
Probability of successful transmission of data packet= $G \times e^{-2G}$	Probability of successful transmission of data packet= $G \times e^{-G}$
Maximum efficiency = 18.4% (Occurs at G = 1/2)	Maximum efficiency = 36.8% (Occurs at G = 1)

1.2 CSMA (Carrier Sense Multiple Access)

CSMA listens to the channel before sending.

Types of CSMA:

- **1-persistent CSMA: Keep listening; send immediately when channel is free.**
- **Non-persistent CSMA: If channel busy, wait a random time before checking again.**
- **P-persistent CSMA: Used in slotted channels; send with probability *p*.**

1.3 CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Used in Ethernet (wired LAN).
Stations sense the channel before transmitting and also detect collisions while transmitting.

Process:

1. **Sense the medium**
2. **If free → transmit**
3. **If collision occurs → detect it → stop transmission → send jamming signal**

4. **Backoff and retransmit**

---

2. IEEE Standards

2.1 IEEE 802.3 (Ethernet)

- **Standard for wired LANs**
- **Uses CSMA/CD**
- **Data rates: 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 40/100 Gbps**
- **Uses RJ-45 connectors and twisted-pair cables**
- **Frame structure includes: Preamble, MAC addresses, Type/Length, Data, CRC**

2.2 IEEE 802.11 (WLAN / Wi-Fi)

- **Standard for wireless LANs**
- **Uses CSMA/CA (Collision Avoidance)**
- **Data rates: 802.11b (11 Mbps), 802.11g (54 Mbps), 802.11n (300 Mbps+),**
  802.11ac (1 Gbps+), 802.11ax (Wi-Fi 6)

Features:

- **Operates on 2.4 GHz & 5 GHz**
- **Supports roaming**
- **Uses access points and authentication mechanisms**

---

3. RFID (Radio Frequency Identification)

Technology for automatic identification using radio waves.

Components:

- **RFID Tag (active / passive)**
- **Reader**
- **Backend database**

Uses:

- **Inventory tracking**
- **Access control**
- **Asset management**
- **Supply chain management**

---

4. Bluetooth Standards

Used for short-range wireless communication.

Specifications:

- **Operates at 2.4 GHz**
- **Range: 10–100 meters**
- **Speeds:**
    - **Bluetooth 3.0: 24 Mbps**
    - **Bluetooth 4.0 (BLE): Low energy, 1 Mbps**
    - **Bluetooth 5.0: Range + speed improved**

Applications:

- **Wireless headphones**
- **IoT devices**
- **File transfer**
- **Wearables**