3. Computer Networks

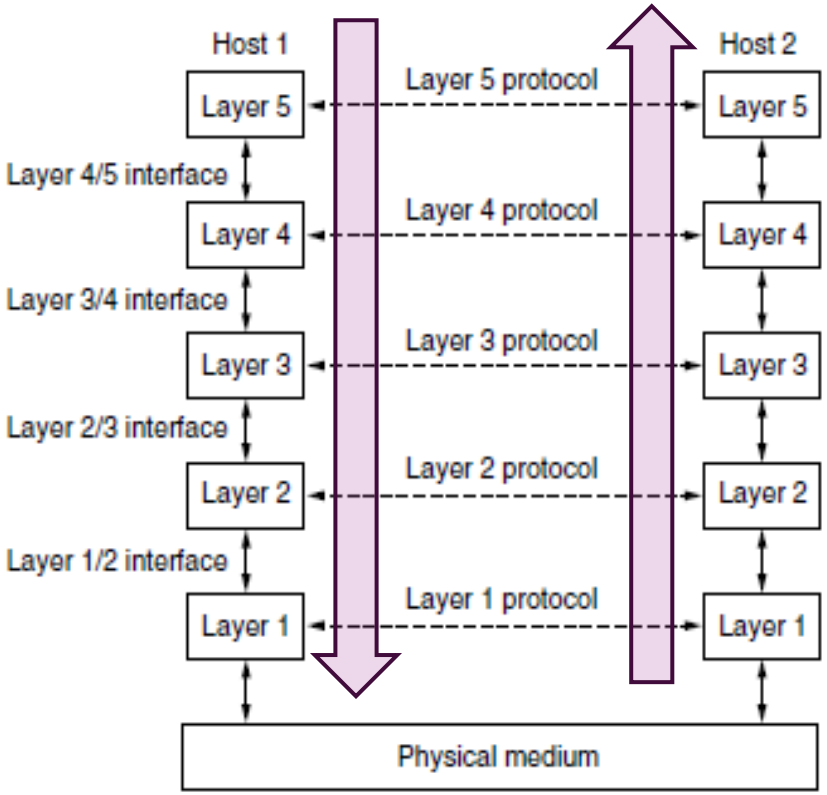
ISO/OSI Model, Physical Layer, Data Link Layer

Summary

- Network Architecture
- Network Ownership and Standards
- ISO/OSI Reference Model
- Physical Layer
- Frequency and Bandwidth
- Bandwidth-delay Product
- Data Link Layer
- Logical Link Control (LLC)
- Media Access Control (MAC)
- Network Switch

Network Architecture

The **network architecture** is a framework that outlines the **structure** and **operation** of a network, consisting of a **set of layers** and **protocols** that dictate how data is transmitted and received.



Network Ownership and Standards

- **Network Ownership:**

Networks where the design and operational decisions are independently made by the manufacturer.

Choices are arbitrary and can vary widely between manufacturers.

- **Standard de facto:**

Public domain specifications widely accepted and used by the industry (TCP/IP model).

- **Standard de iure:**

Specifications approved by international standardization organizations and are in the public domain (ISO/OSI model).

ISO/OSI Reference Model - Introduction

The **OSI (Open Systems Interconnection) model** was established in 1984 and is the result of work by the **ISO (International Organization for Standardization).** It is a **standard de iure**. Its purpose is to:

- Provide a **standard model** against which various network architectures can be compared.

The **ISO/OSI model** is an **abstract description** for layered communication and computer network protocol design. It divides the network architecture into **seven layers**.

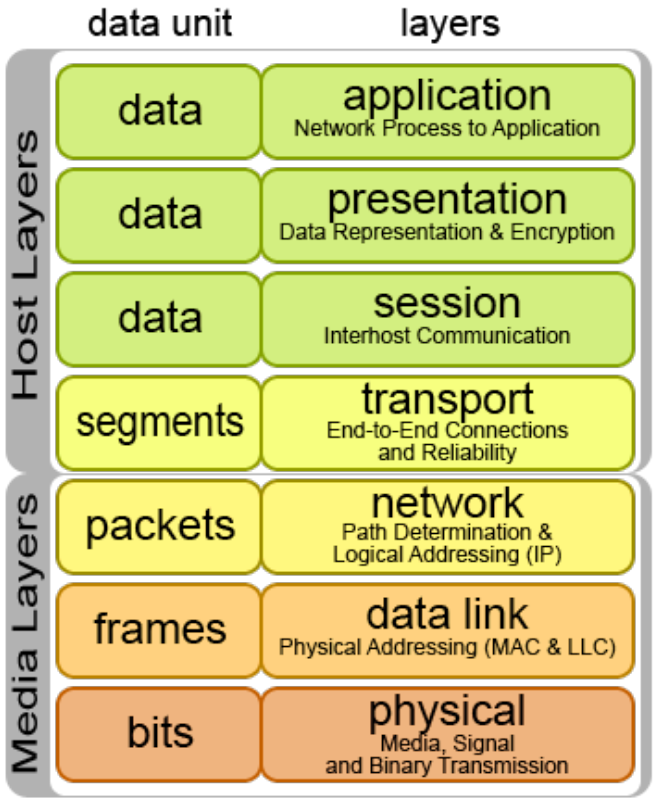
ISO/OSI model was designed according to following principles:

- Each layer must have a different **level of abstraction**;
- Each layer must have a **well-defined function**;

The choice of layers must:

- **Minimize** the information passing between layers;
- **Avoid** too many functions in one layer;
- **Avoid** too many layers.

ISO/OSI Reference Model

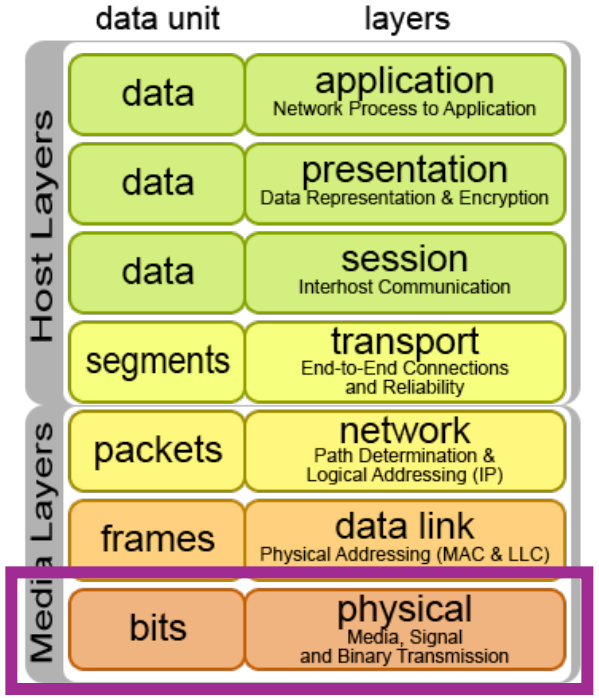


Physical Layer

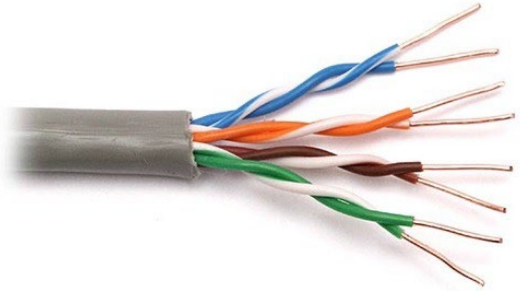
The **physical layer** is responsible for the **physical connection** between devices. It deals with the **transmission** and **reception** of **raw bitstreams** over a physical medium.

Main physical mediums:

- **Copper** cables (e.g., Ethernet, Coaxial cable);
- **Fiber** optic cables;
- **Radio** frequencies (e.g., Wi-Fi, Bluetooth).



Ethernet and Coaxial Cables

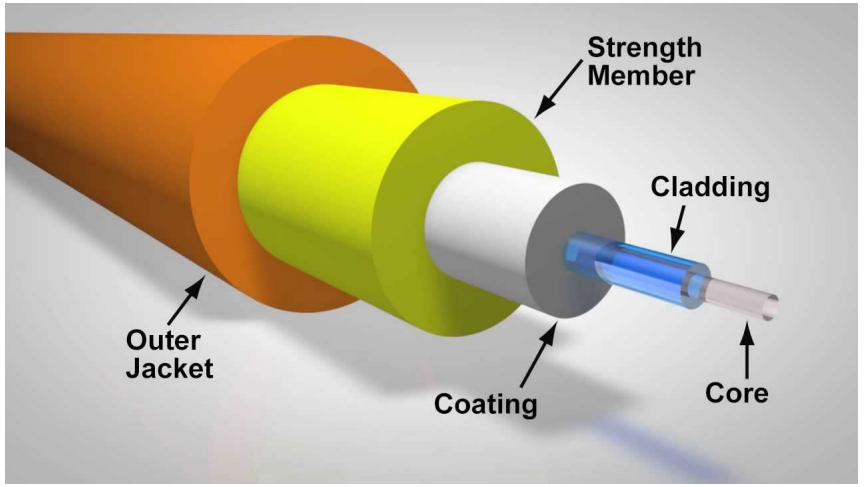


Ethernet cables are types of **electrical cables** used to connect devices within a **local area network (LAN)** for data transmission. They use **twisted pair** wiring to **reduce interferences** and **improve signal quality**.

Coaxial cable is a type of **electrical cable** consisting of a **central copper** conductor, an **insulating layer**, a **metallic shield**, and an **outer insulating layer**. This construction provides **excellent protection** against electromagnetic interferences, ensuring **signal integrity** over **long distances**. It also offers **higher** data transmission **speeds**.

Fiber Optic Cable

Fiber optic cable is a type of network cable that uses **light** to transmit data at **high speeds over long distances**. It consists of **strands of glass** or **plastic** fibers, each capable of carrying data signals in the form of **light pulses**. Fiber optic supports much **higher data rates** and is also **immune** to **electromagnetic interferences**, ensuring clean and reliable data transmission.



- **Core:** The central part of the fiber, made of glass or plastic, through which light signals travel.
- **Cladding:** Surrounds the core and reflects light back into the core, minimizing signal loss.
- **Coating:** Protects the fiber from damage and moisture.
- **Outer Jacket:** Provides additional protection against environmental factors.

Radio Frequencies (Wi-Fi, Bluetooth)

Radio frequency (RF) data transfer involves transmitting data wirelessly through **electromagnetic waves**. **Wi-Fi** and **Bluetooth** are two common technologies that use RF to enable **wireless communication** between devices.

- **Wi-Fi:**

Frequency Bands: Operates primarily in the 2.4 GHz and 5 GHz frequency bands, with newer standards also using the 6 GHz band.
Range: Typically covers a range of up to 100 meters indoors, depending on the environment and obstacles.
Network Type: Typically forms part of a local area network (LAN) where multiple devices connect to a central router or access point.
Applications: Internet access, streaming services, online gaming, smart home connectivity, and enterprise networking.

- **Bluetooth:**

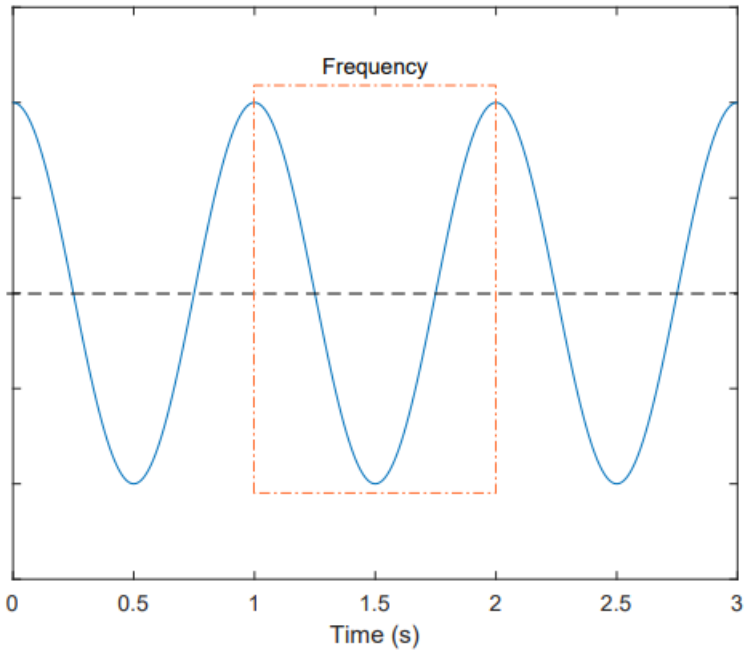
Frequency Bands: Operates in the 2.4 GHz ISM (Industrial, Scientific, and Medical) band.
Range: Typically covers a range of up to 10 meters, with some versions (Bluetooth 5) extending up to 100 meters.
Network Type: Typically forms a personal area network (PAN) where devices connect directly to each other or through a central device in a star topology.
Applications: Connecting peripherals (e.g., headphones, keyboards), file transfer between mobile devices, wireless audio streaming, and smart home device control.

Advantages of RF Data Transfer:

- Eliminates the need for physical cables, providing greater mobility and convenience.
- Simplifies the process of connecting and communicating between devices.

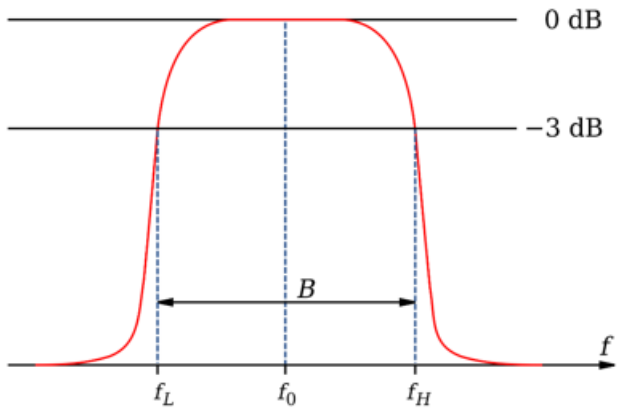
Frequency

Frequency refers to the **number of cycles (oscillations)** of the wave that pass a specific point in **one second**. It is measured in **Hertz (Hz)**, where one Hertz equals one cycle per second.



Bandwidth

Bandwidth is the **range of frequencies** within a given band that a signal occupies. It is the difference between the highest and lowest frequencies in the range and is measured in **Hertz (Hz)**.

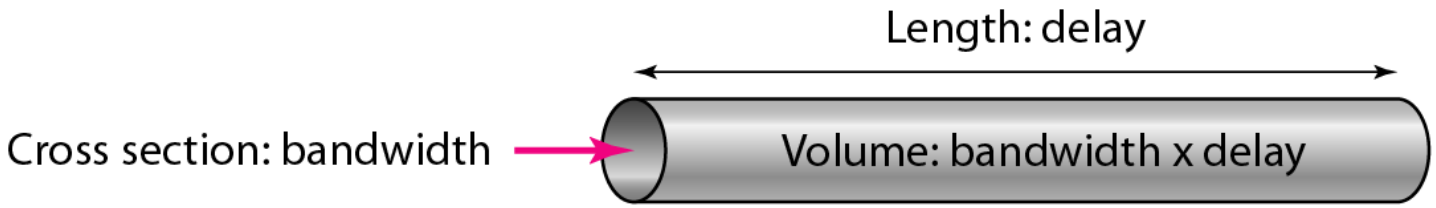


Bandwidth defines the **amount of data** that can be **transmitted** over a network connection in a **given amount of time**, typically measured in **bits per second (bps). Higher bandwidth** indicates a greater capacity to **carry more data**, resulting in **faster data transmission** and **higher performance** in network communications.

The **actual bandwidth** experienced by users can be **lower** due to factors like **network congestion**, **distance from the router**, **interference**, and **device capabilities**.

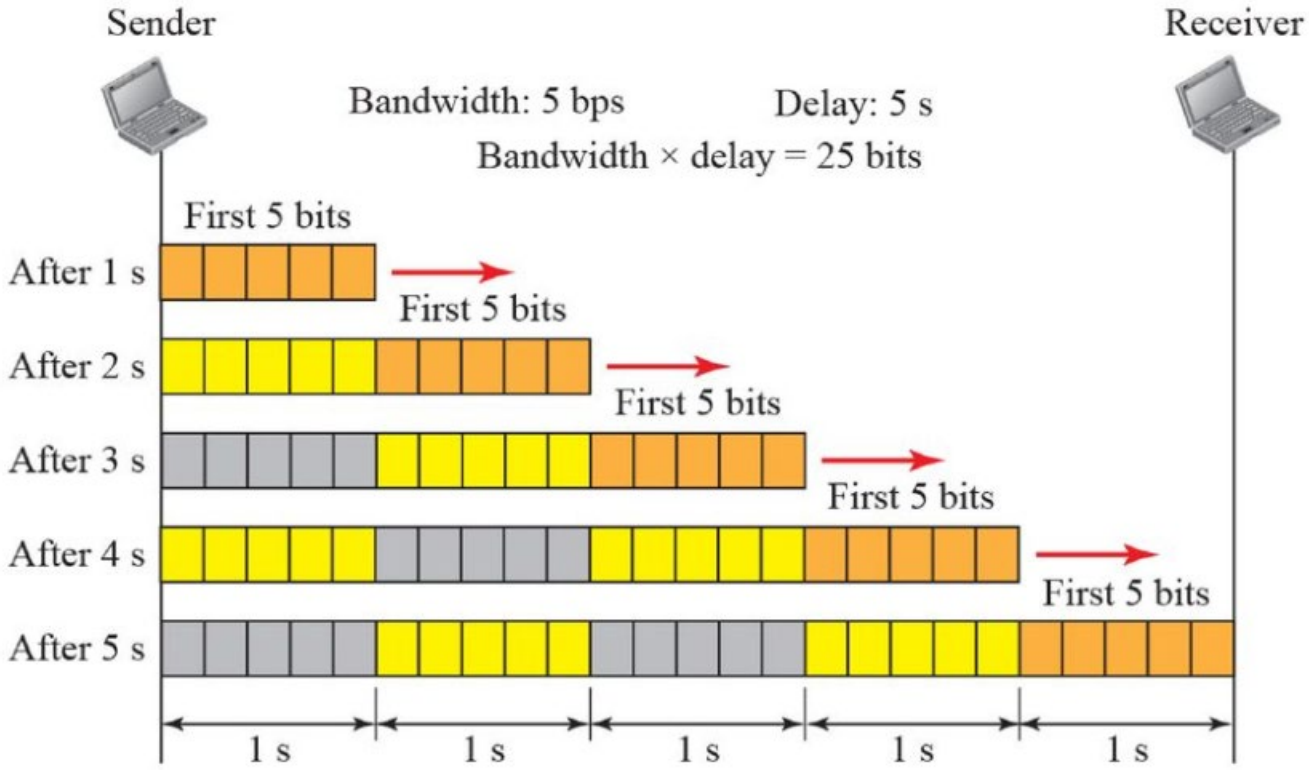
Bandwidth-delay Product/1

The **bandwidth-delay product** defines the **maximum amount of data (in bits)** that can be in **transit** in the network link at **any given time**.



- **Bandwidth:** The cross section of the pipe (how much data can flow through per unit of time).
- **Delay:** The length of the pipe (the time it takes for data to travel from one end to the other).
- **Bandwidth-Delay Product:** The volume of the pipe (total amount of data that can be in transit at any given time). The longer the pipe (greater delay), the longer it takes for data to travel through it.

Bandwidth-delay Product/2

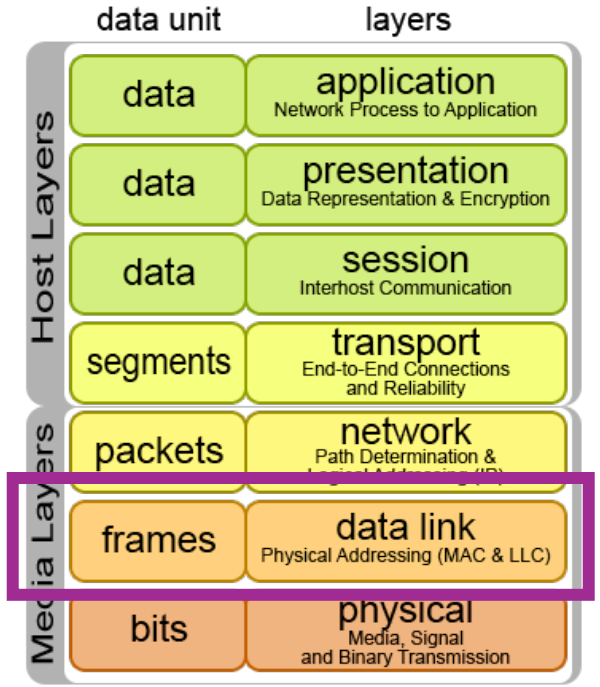


Data Link Layer

The **Data Link** layer is the second layer of the OSI model, responsible for **node-to-node data transfer** and **error detection** and **correction**.

Functions:

- **Establishes** and **terminates logical link** connections.
- Manages **data frames** between devices on the same network.



ICTAcademy
INFORMATION AND COMMUNICATIONS TECHNOLOGY

Functions of the Data Link Layer

- **Framing:**

Divides data into **frames** for easier transmission.

Adds headers and **trailers** to frames to facilitate communication.

- **Error Detection and Correction:**

Detects errors in transmitted frames using techniques like CRC (Cyclic Redundancy Check).

Corrects errors to ensure reliable data transfer.

- **Flow Control:**

Manages data **flow** to prevent congestion and data loss.

- **Addressing:**

Uses **MAC (Media Access Control)** addresses to **identify** devices on the network.

Sub-layers of the Data Link Layer

- **Logical Link Control (LLC):**

Handles **error checking** and **flow control**.

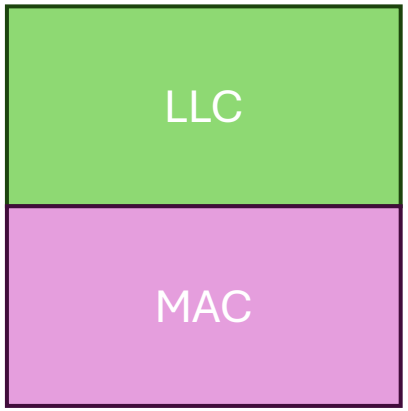
Divides data into **frames** for easier transmission.

Adds **headers** and **trailers** to frames to facilitate communication.

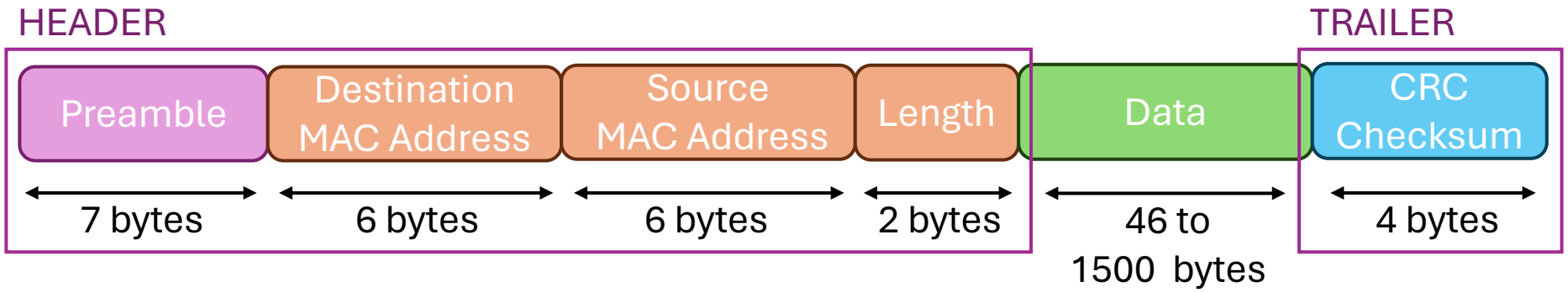
- **Media Access Control (MAC):**

Controls how **devices** on the network **gain access** to the medium.

Determines how data is placed on the medium.



LLC - Framing



- **Preamble:** The preamble is a series of bits that helps the receiving device get ready to understand the incoming data. It ensures both the sender and receiver are in sync before the actual message starts.
- **Destination MAC address:** the physical address of the destination device on the network.
- **Source MAC address:** the physical address of the sending device on the network.
- **Length:** the size of the data payload in the frame.
- **Data:** the field containing the actual payload being transmitted. It can include upper-layer headers.
- **CRC Checksum:** the checksum is a value calculated from the frame's contents to detect errors in transmission. If the calculated checksum at the receiving end does not match the transmitted checksum, it indicates that the frame has been corrupted

LLC - Flow Control Mechanisms

- **Stop-and-Wait**

Description: The sender transmits one frame and waits for an acknowledgment from the receiver before sending the next frame. This ensures that each frame is received and acknowledged before the next one is sent, preventing data overflow and ensuring orderly delivery.

Advantages: Simple and easy to implement.

Disadvantages: Inefficient for high-speed networks due to waiting time.

- **Sliding Window**

Description: Allows multiple frames to be sent before requiring an acknowledgment. The sender can transmit several frames specified by a "window" size. After sending these frames, the sender waits for acknowledgments. As acknowledgments are received, the window slides forward, allowing the sender to transmit more frames.

Advantages: More efficient use of network resources, better performance in high-speed networks.

Disadvantages: More complex to implement.

Media Access Control (MAC) Sub-layer

The **MAC sub-layer** controls how data is **placed onto** and **retrieved from** the network medium.

Functions:

- **Addressing:** Uses MAC addresses to identify sending and receiving devices on the network.
- **Access Control:** Determines how devices share the network medium to avoid collisions (when two devices try to send data simultaneously).

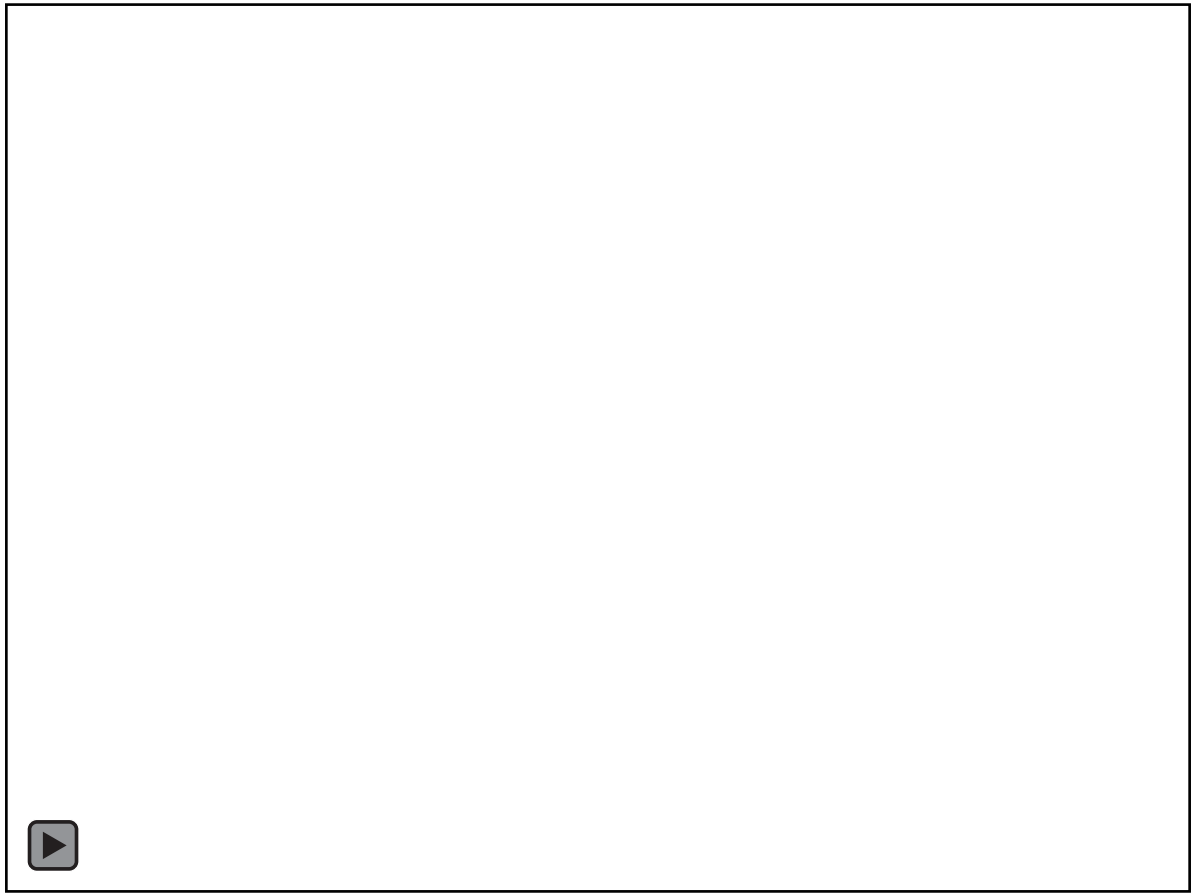
  Example methods:

  - **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):** Used in Ethernet networks to manage data transmission and detect collisions.

  - **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):** Used in Wi-Fi networks to avoid collisions by waiting for a clear channel before transmitting.

- **Frame Delimiting:** Defines the start and end of a frame, ensuring that data is correctly interpreted.

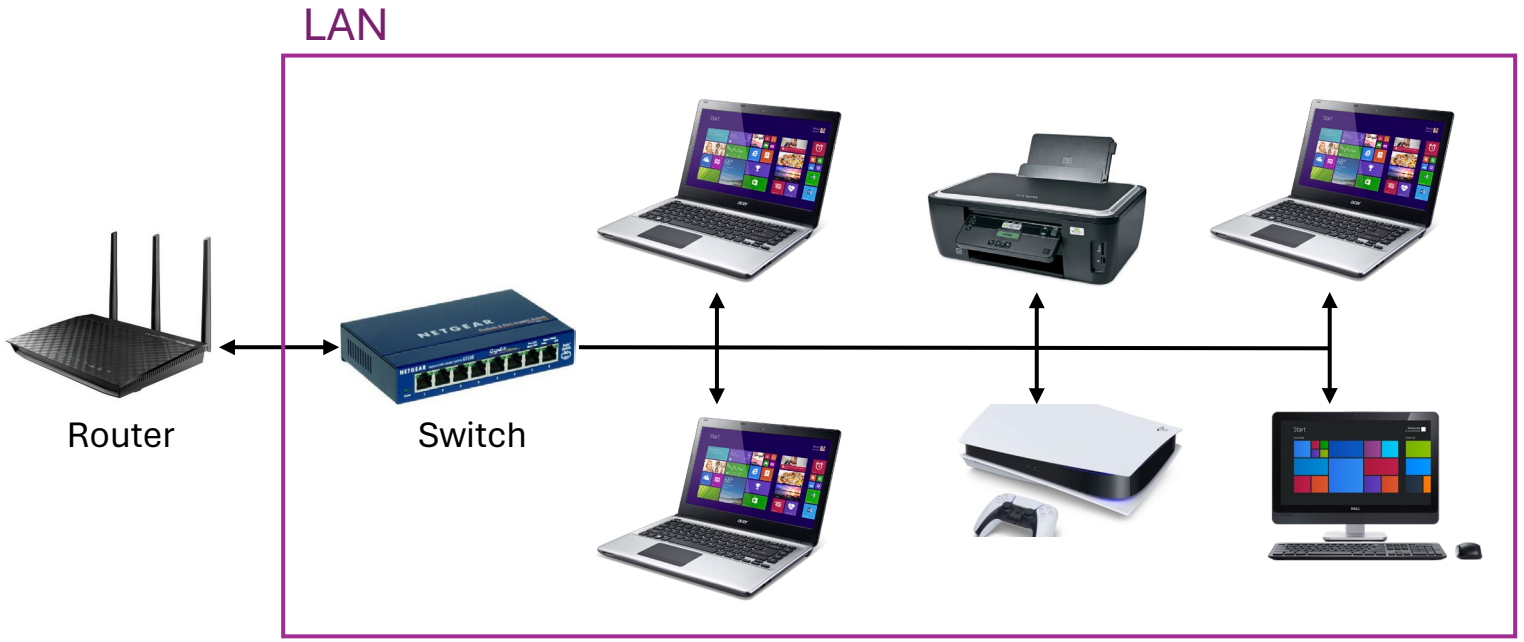
MAC - CSMA/CD and CSMA/CA



Network Switch

Network switches are fundamental devices in a **Local Area Network (LAN)**. They enable **communication** between different devices within the same network.

A **network switch** is a device that **receives**, **processes**, and **forwards** data to specific devices within a local network. It operates at the **Data Link Layer** of the **ISO/OSI model**.



Network Switch – Basic Operations

Basic Operation of a Switch:

- **Receives** a data frame from a connected device.
- **Reads** the destination MAC address of the frame.
- **Looks up** the MAC address in its MAC address table to determine the destination port.
  - The MAC address table maps MAC addresses to the switch port numbers.
  - It is dynamically built by learning MAC addresses from the frames passing through the switch.
- **Sends** the frame to the correct port to reach the destination device.