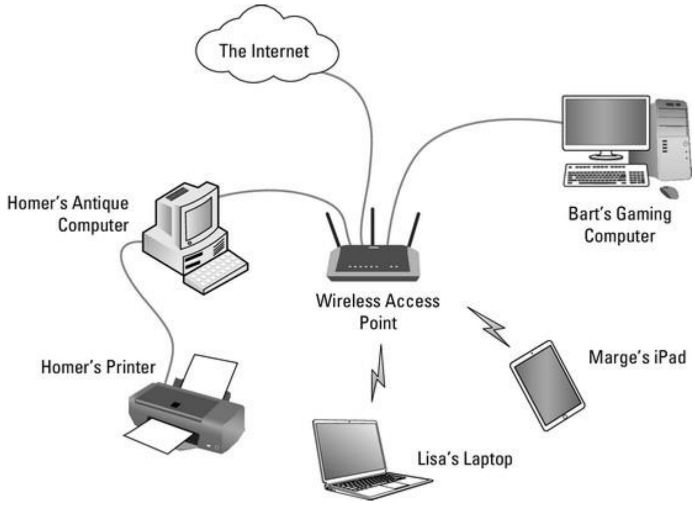
EXPERIMENT-1

AIM- Demonstration and study about different physical equipment used for networking NIC (Network Interface Card), types of cable, Fiber Optics.

Computer Network: A computer network is a **system that connects two or more computing devices** to enable communication, data sharing, and resource sharing.

Exemple - Devices like computers, smartphones, tablets, and servers to connect and communicate with each other.



Computer Network

NIC (Network Interface Card) is a hardware component that enables a computer to connect to a network, allowing it to send and receive data.

1. Wired NICs (Ethernet):

- **Function**: Connect to a network using physical cables, typically Ethernet cables (RJ45 connectors).
- **Types:**
  - **Standard Ethernet**: Uses twisted-pair cables for data transmission.
  - **Fiber Optic:** Transmits data via fiber optic cables, supporting longer distances and higher speeds.

- **Advantages:** Reliable, high speed, and secure**.**
- **Disadvantages**: Requires physical cables, can be less portable**.**

2. Wireless NICs (Wi-Fi):

- **Function:** Connect to a network using radio frequencies via an antenna.

NIC (Network Interface Card)

- **Types:**
    - Wi-Fi: Follows the IEEE 802.11 wireless communication standards.
    - Bluetooth: Enables devices to communicate via Bluetooth.
    - Cellular Network Cards: Connect to mobile networks through cellular standards.
- **Advantages:** Portable, flexible, and can cover larger distances.
- **Disadvantages:** Can be less reliable and secure than wired connections, and susceptible to interference.

3. Other NIC Types:

- **USB NICs:**

Provide network connections through a device plugged into a USB port, ideal for portable computers or devices without built-in NICs.

- **PCI/PCIe NICs:**

Older types of NICs that connect to the computer's motherboard via PCI or PCIe slots.

- **Internal vs. External NICs:**

Internal NICs are built into the device (e.g., laptops), while external NICs are separate devices (e.g., USB NICs).

.

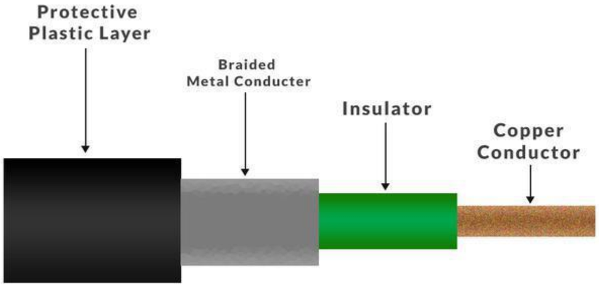
Types of Cables

Mainly there are three types of ethernet cables used in LANs.

- Coaxial Cables
- Twisted Pair Cables
- Fiber optic Cables

Coaxial Cable

A type of electrical cable consisting of an **inner conductor surrounded by a concentric conducting shield, separated by a dielectric (insulating material)**, and often protected by an outer sheath.



Coaxial Cable

- **Structure:**
  - **Inner Conductor:** A central wire, usually made of copper or aluminum, that carries the signal.
  - **Dielectric:** An insulating material (like plastic or foam) that separates the inner conductor from the outer shield.
  - **Outer Shield (Conducting):** A metal tube or braid that surrounds the dielectric, acting as a shield against electromagnetic interference and acting as a return path for the signal.
  - **Outer Sheath:** A protective layer, often made of plastic or rubber, that covers the entire cable.
- **Function:**

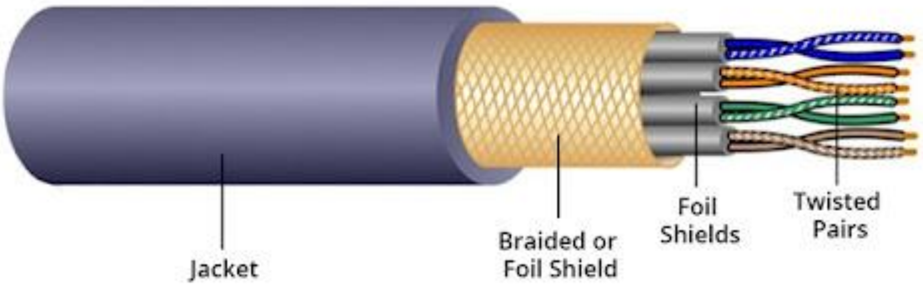
Coaxial cables are designed to efficiently transmit high-frequency signals with minimal signal loss and interference.

- **Common Uses:**
    - Cable television and satellite installations.
    - Connecting antennas to transmitters and receivers.
    - Data and video transmission.
    - Radio frequency applications.
- **Types:**

Different types of coaxial cables are identified by their RG (Radio Guide) number, such as RG-6, RG-59, and RG-8.

Twisted Pair Cables

A twisted pair cable is a type of communication cable where **two insulated copper wires are twisted together** to reduce electromagnetic interference and crosstalk.



Twisted Pair Cables

- **Purpose:**

The twisting of the wires helps minimize electromagnetic radiation and resist external interference, improving signal quality and reliability.

- **Construction:**

Twisted pair cables consist of one or more pairs of copper wires that are insulated and twisted around each other.

- **Types:**

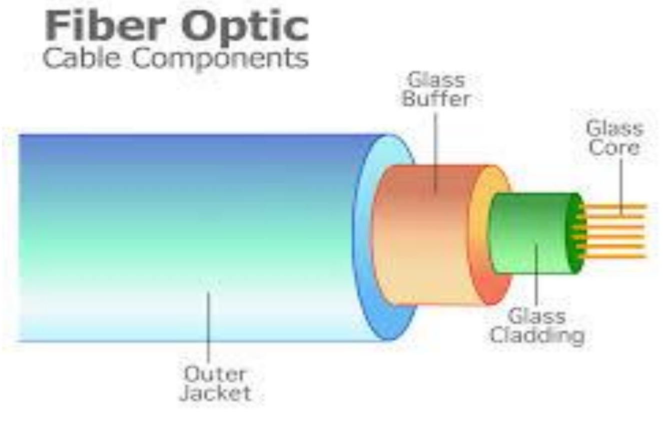
    - **Unshielded Twisted Pair (UTP):** The most common type, where the wires are twisted but not shielded.
    - **Shielded Twisted Pair (STP):** Features an additional shield around the twisted pairs to provide better protection against electromagnetic interference.
- **Applications:**

Twisted pair cables are widely used in various applications, including:

    - **Networking:** Ethernet cables, which are used to connect devices in a local area network (LAN).
    - **Telecommunications:** Telephone lines.
- **Benefits:**
    - **Reduced Electromagnetic Interference (EMI):** The twisting of the wires helps cancel out electromagnetic signals, reducing interference.
    - **Lower Cost:** Compared to other cable types like fiber optic, twisted pair cables are generally more affordable.
    - **Ease of Installation:** Twisted pair cables are relatively easy to install and terminate.

Fiber Optic Cable

A fiber optic cable is a type of communication cable that **transmits data as light signals through thin, flexible strands of glass or plastic** called optical fibers, offering high bandwidth and speed compared to traditional copper cables.



Fiber Optic Cable

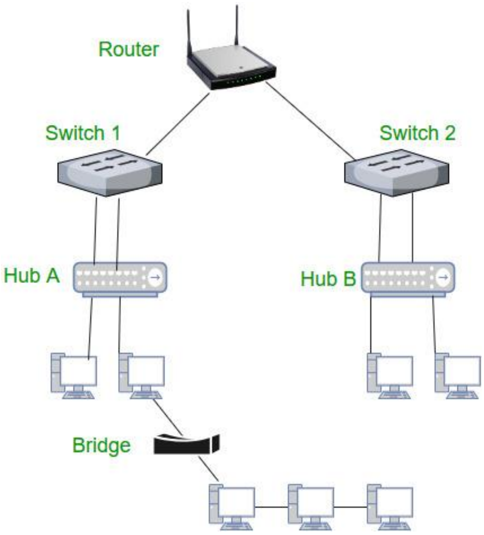
- **Types of Fiber:**
    - **Multimode:** Uses multiple light paths (modes) for data transmission, suitable for shorter distances.

    - **Single-mode:** Uses a single light path, ideal for long-distance communication.
- **Advantages:**
    - **High Bandwidth:** Fiber optic cables can transmit significantly more data than copper cables.
    - **High Speed:** Data transfer speeds are extremely fast, reaching gigabit speeds.
    - **Long Distance:** Light signals can travel long distances with minimal signal loss.
    - **Low Interference:** Fiber optic cables are less susceptible to electromagnetic interference compared to copper cables.
- **Applications:**
    - **Telecommunications:** Internet, telephone, and television services.
    - **Data Networking:** High-speed data transmission in businesses and homes.
    - **Medical Imaging:** Used in endoscopes and other medical devices.
    - **Industrial Applications:** Used in sensors, lasers, and other industrial equipment.

EXPERIMENT – 2

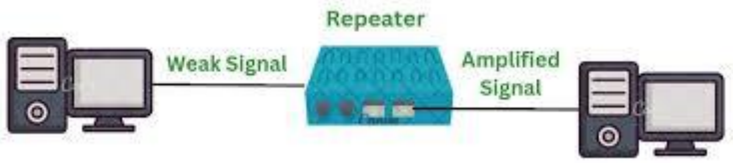
AIM – Demonstration and study different internetworking devices in a computer network; Repeater, Bridge, Router, Gateway, Hubs, Switchs.

Internetworking devices - Network devices are **physical devices** that allow hardware on a **computer network to communicate and interact** with each other. Network devices like hubs, repeaters, bridges, switches, routers, gateways, and brouter help manage and direct data flow in a network.



Internetworking devices

Repeater- In computer networks, a repeater is a network device that **amplifies or regenerates incoming signals** before retransmitting them, **extending the range** of a network and ensuring consistent, reliable communication.



Repeater

- **Function:**

Repeaters receive a network signal, regenerate it to its original strength, and then retransmit it, effectively extending the distance over which data can be transmitted safely.

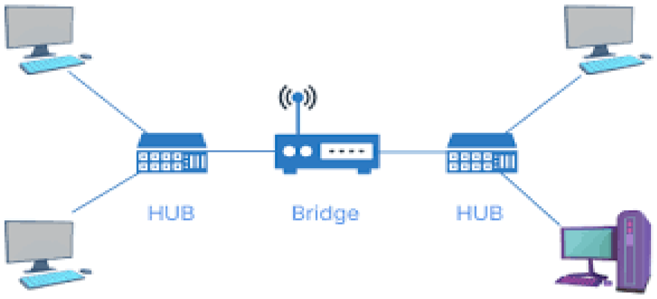
- **Purpose:**
  - Extend Network Reach: Repeaters are used when the distance between network devices exceeds the limitations of the physical media (e.g., Ethernet cables).
  - Restore Weak Signals: They can also restore signals that have become weak or distorted due to distance or interference.
  - Connect Different Networks: In some cases, repeaters can be used to connect networks that use different physical media.
- **How it Works:**
  - Repeaters work at the physical layer, meaning they deal with the raw electrical or optical signals, not the data content.
  - They simply regenerate the signal, not making any decisions about routing or data content.
- **OSI Model Layer:**

Repeaters operate at the physical layer (Layer 1) of the OSI model.

- **Examples:**
  - Hubs: Multiport Ethernet repeaters are often referred to as hubs.
  - Wireless Repeaters: Wireless repeaters (also called extenders) are used to extend the range of Wi-Fi networks.
- **Limitations:**
  - While repeaters extend network reach, they don't increase bandwidth or data transfer speed.
  - Too many repeaters in a network can introduce latency and slow down the network.

Bridge - A bridge is a network device that **connects multiple subnetworks** to create a single network. It provides **interconnection with other computer networks** that use the same protocol. Through a bridge, multiple LANs can be connected to form a larger and extended LAN.

a bridge is a device that connects two or more Local Area Networks (LANs) into a single, larger LAN, operating at the data link layer (Layer 2) of the **OSI model**. It acts as a "repeater" with the added functionality of filtering content by reading **MAC addresses**, deciding whether to forward or **filter data packets**.



Bridge

How does a bridge work?

- A bridge connects multiple subnetworks to create a single network.
- It connects multiple LANs to form a larger LAN.
- It inspects incoming traffic to determine if it should be filtered or forwarded.
- It can filter content by reading the MAC addresses of the source and destination.

Benefits

- It makes multiple networks appear as a single network.
- It allows multiple LANs to be connected to other computer networks that use the same protocol.

Standardized

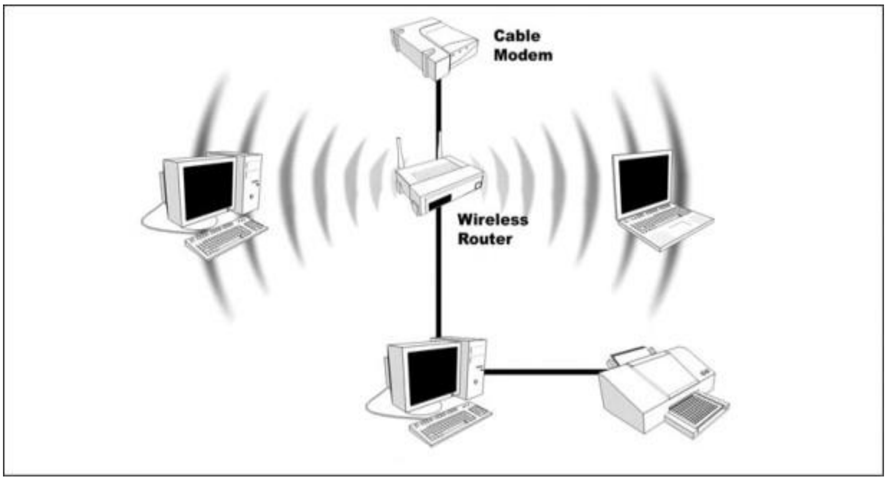
- The Institute of Electrical and Electronics Engineers (IEEE) standardizes bridges in the IEEE 802 family.
- Modern multi-port bridges are often called Layer 2 switches because they perform similar functions.

Some things to consider when using a bridge

- Ensure there are no duplicate IP addresses within the bridged network segments.

Router – A router is a **device that connects two or more networks**, forwarding data packets to their intended destination **based on IP addresses**, and allowing multiple devices to share the same internet connection.

It serves two primary functions: **managing traffic between these networks** by forwarding data packets to their intended IP addresses, and multiple devices.



Router

- **Connecting Devices:**

Routers act as a central hub, allowing multiple devices (computers, smartphones, tablets, etc.) to share a single internet connection and communicate with each other within a local network.

- **Directing Traffic:**

Routers intelligently forward data packets (small units of data) to their intended destinations by examining the IP addresses (unique identifiers for devices on a network).

- **Enabling Communication:**

Routers facilitate communication between different networks, such as a home network and the internet, or between different parts of a larger network.

- **Security Features:**

Many routers include built-in security features, such as firewalls, to protect the network from unauthorized access and potential threats.

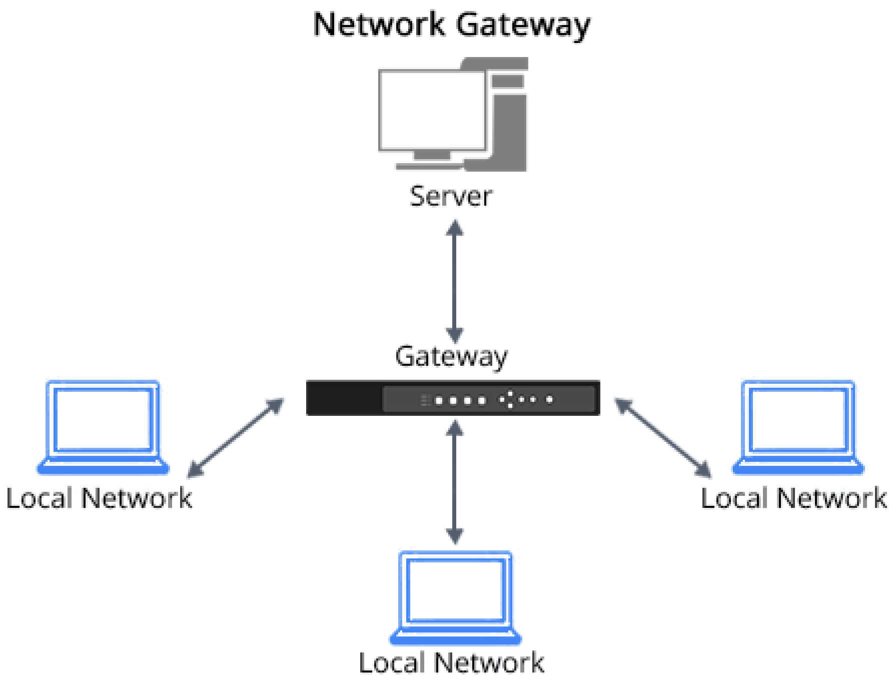
- **Wireless and Wired Connections:**

Routers can support both wireless (Wi-Fi) and wired (Ethernet) connections, allowing devices to connect to the network in various ways.

- **Modem vs. Router:**

While routers connect devices to a network and direct traffic, a modem connects your network to the internet service provider (ISP) and establishes the internet connection. Many devices combine both router and modem functions into a single unit.

Gateway - A gateway acts as a bridge or interface between different networks or applications that use different protocols, **facilitating communication and data transfer** between them.



Gateway

- **Function:**

  Gateways translate data formats (protocols) from one network to another, enabling devices on different networks to communicate.

- **Examples:**
  - **Internet Gateway:** Your home router acts as a gateway, allowing your local network to connect to the internet.
  - **Cloud Storage Gateway:** Facilitates access to cloud storage from on-premises applications without moving those applications to the cloud.
  - **IoT Gateway:** Collects and translates data from IoT devices, enabling communication with cloud networks.
- **Types:**
  - **Unidirectional Gateway:** Allows data to flow in one direction.
  - **Bidirectional Gateway:** Allows data to flow in both directions.

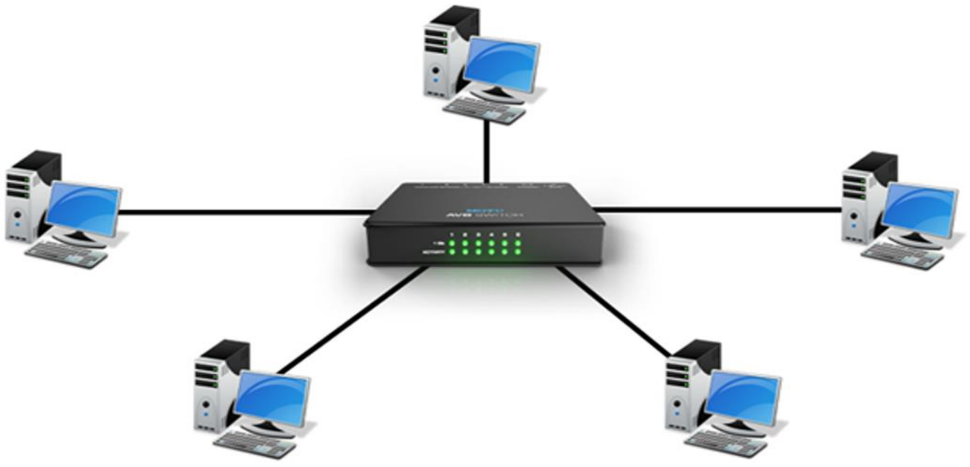
- **Difference between Gateway and Router:**

While both connect networks, a router typically delivers data within a network, while a gateway is more specialized and handles data conversion between different types of networks.

- **Default Gateway:**

It is the access point between your home network and the rest of the internet.

Hub- A hub is a simple device that **connects multiple devices to a single network**, broadcasting data received on **one port to all other ports**, essentially acting as a multi-port repeater.



Hub

- **Function:**

A hub acts as a central point for connecting devices in a local area network (LAN).

- **Data Transmission:**

When a data packet arrives at one port of the hub, it's copied and sent out to all other ports, allowing all connected devices to receive the data.

- **Lack of Intelligence:**

Hubs don't analyze or manage the data they transmit; they simply broadcast it to every connected device.

- **Obsolete Technology:**

Due to their lack of intelligence and the potential for increased network traffic and collisions, hubs are less common today than switches and routers.

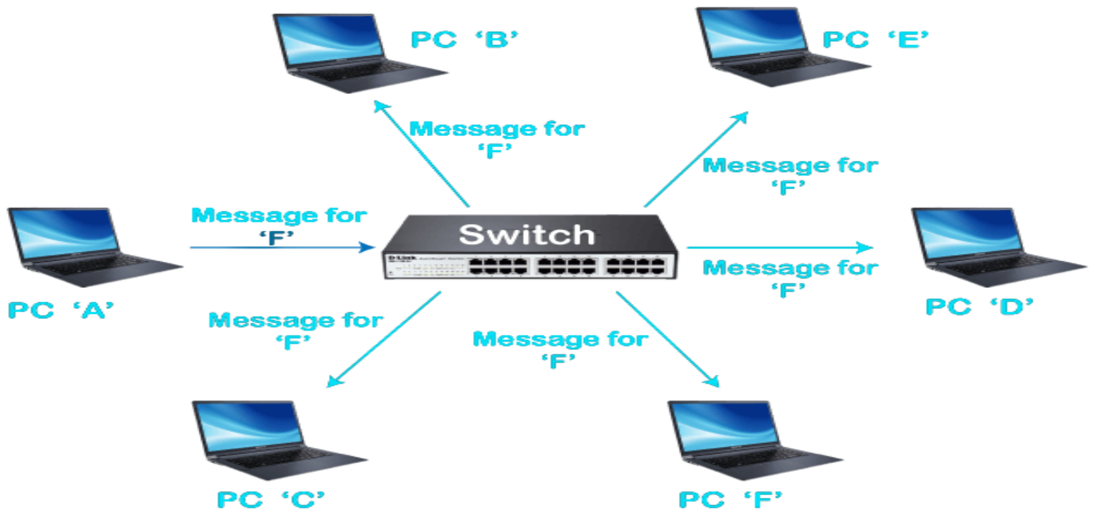
- **Types of Hubs:**
    - **Active Hub:** These hubs have their own power supply and can clean, boost, and relay the signal along with the network.
    - **Passive Hub:** These hubs collect wiring from nodes and power supply from the active hub, relaying signals onto the network without cleaning or boosting them.
    - **Intelligent Hub:** These hubs work like active hubs and include remote management capabilities, flexible data rates, and the ability for an administrator to monitor traffic and configure ports.
- **Comparison to Switches:**

While both hubs and switches connect devices, switches are more intelligent and can filter and forward data based on the destination MAC address, leading to more efficient and less congested networks.

- **Hubs vs. Switches:**
    - **Hubs:** operate at the physical layer (layer 1 of the OSI model), broadcast data to all ports, and are less expensive.
    - **Switches:** operate at the data link layer (layer 2 of the OSI model), filter data based on MAC addresses, and are more expensive.

Switchs - A switch is a networking device that **connects multiple devices**, like **computers and printers, on the same network**, enabling them **to communicate and share information** efficiently by forwarding data packets to the intended recipient.

In a network, enabling them to communicate by forwarding data packets between them, typically based on MAC addresses.



Switch

- **Connecting Devices:**

Switches act as central hubs, connecting various network devices, such as computers, servers, printers, and wireless access points, within a local area network (LAN).

- **Data Forwarding:**

When a device sends data, the switch receives the data packet and forwards it only to the specific device that is the intended recipient, rather than broadcasting it to all connected devices.

- **Packet Switching:**

Switches use packet switching, a method of data transmission where data is broken down into small packets, each containing addressing information, which are then transmitted independently and reassembled at the destination.

- **Layer 2 Operation:**

Switches operate at the data link layer (Layer 2) of the OSI model, using MAC addresses (Media Access Control addresses) to identify and forward data packets.

Types of Switches:

- **Unmanaged Switches:**

These are the simplest and most basic types of switches, often used in home networks or small businesses, requiring minimal configuration and offering plug-and-play functionality.

- **Managed Switches:**

Managed switches provide more advanced features and control, allowing network administrators to configure and monitor network traffic, prioritize data flow, and implement security measures.

- **Smart Switches:**

These switches offer some advanced features beyond unmanaged switches, but are less feature-rich than fully managed switches, making them suitable for small to medium-sized networks.

- **PoE (Power over Ethernet) Switches:**

These switches can deliver both data and electrical power to connected devices over Ethernet cables, eliminating the need for separate power sources for devices like IP phones and wireless access points.

Benefits of Using Switches:

- **Improved Network Performance:**

By forwarding data packets directly to the intended recipient, switches reduce network congestion and improve overall network performance.

- **Enhanced Security:**

Managed switches offer features like VLANs (Virtual LANs) and port security, enhancing network security and control.

- **Scalability:**

Switches allow for easy expansion of networks by connecting additional devices without disrupting existing network operations.

- **Cost-Effective:**

Switches are relatively inexpensive compared to other networking devices, making them a cost-effective solution for connecting multiple devices on a network.