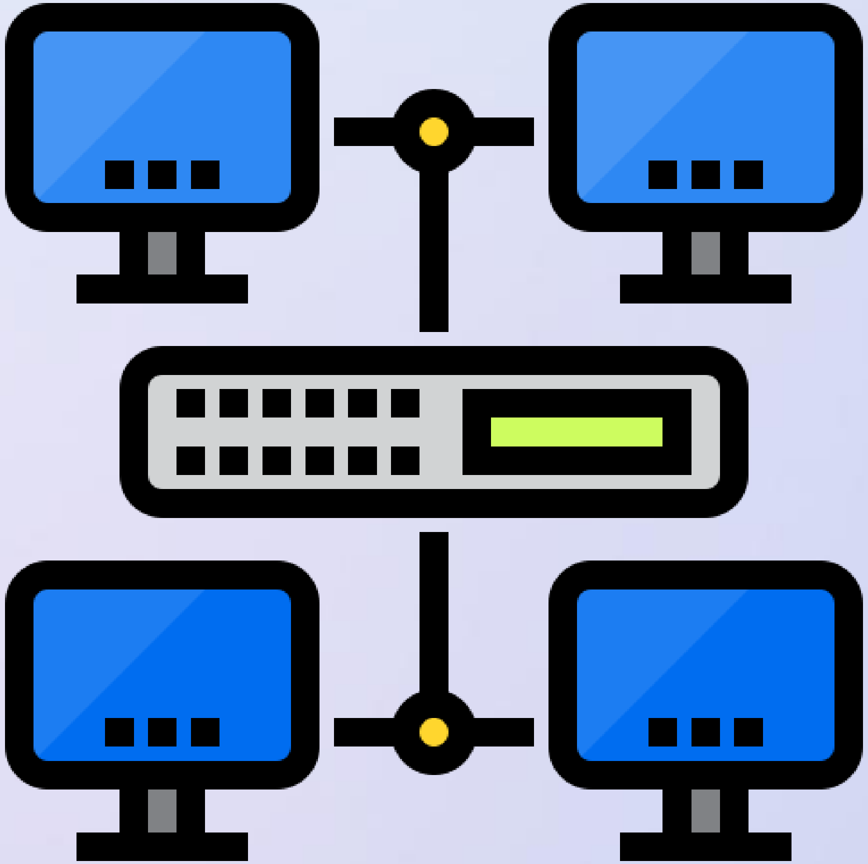
UNIVERSITY OF AL-AMEED COLLEGE OF PHARMACY

NETWORK FUNDAMENTALS

Exploring Networking, Networking Types, Connection Methods

NETWORK AND SECURITY FUNDAMENTALS

This presentation provides a comprehensive overview of networking and security essentials, focusing on various types of networks, methods of connection, and key security practices necessary to protect information and ensure efficient data communication.



WHAT IS NETWORKING?

- **Definition**: A network is a collection of interconnected devices that communicate and share resources.
- **Purpose**: Facilitates data sharing, resource access, and communication between devices.
- **Types vary** based on scale, purpose, and technology.

BASIC TERMINOLOGIES OF COMPUTER NETWORKS

Network: A group of connected computers and devices that can communicate and share data with each other.

Node: Any device that can send, receive, or forward data in a network. This includes laptops, mobiles, printers, earbuds, servers, etc.

Networking Devices: Devices that manage and support networking functions. This includes routers, switches, hubs, and access points.

Transmission Media: The physical or wireless medium through which data travels between devices.

Wired media: Ethernet cables, optical fiber.

Wireless media: Wi-Fi, Bluetooth, infrared

Service Provider Networks: Networks offered by external providers that allow users or organizations to lease network access and capabilities. This includes internet providers, mobile carriers, etc.

HOW DOES A COMPUTER NETWORK WORK

Basics building blocks of a Computer network are Nodes and Links.

Network Node: Any device in a network, such as a modem, router, or computer, that sends or receives data.

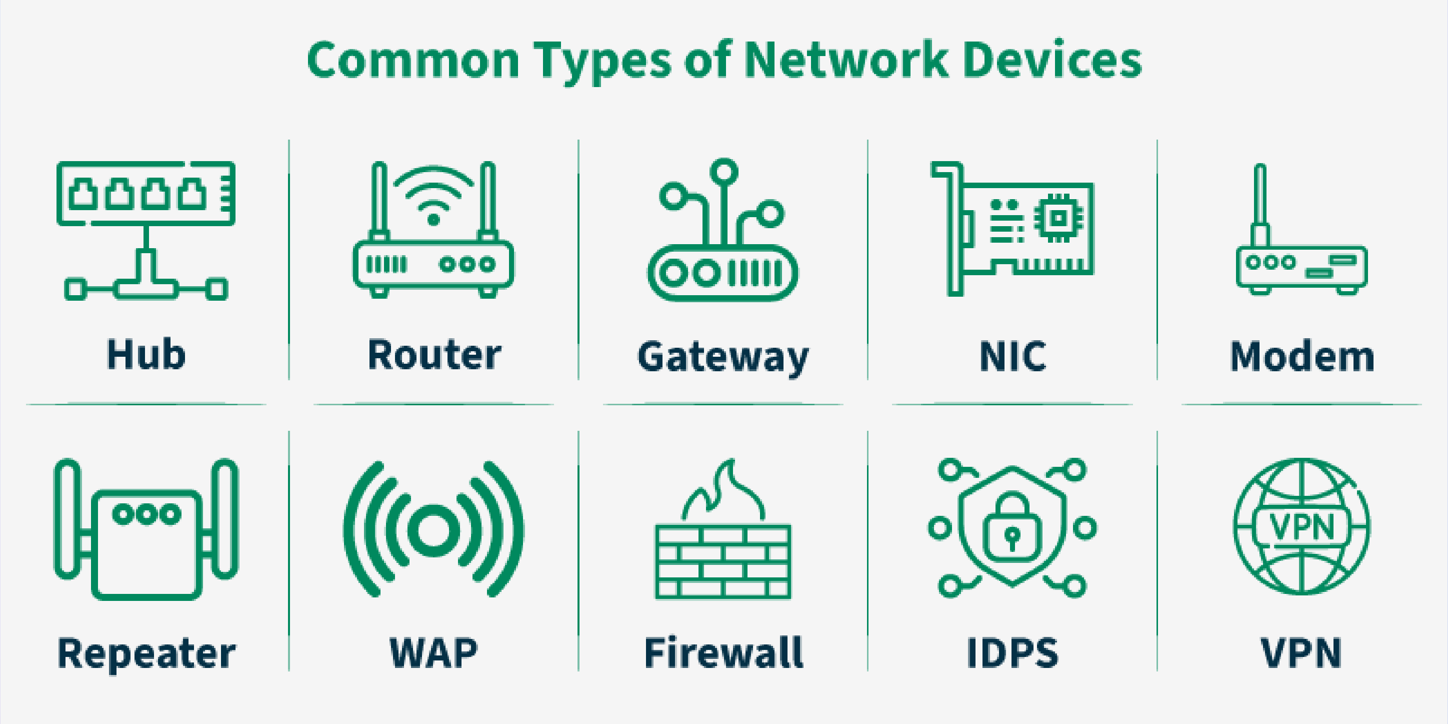
Link: The medium that connects nodes, like cables, wires, or wireless signals.

Working: Networks use rules called protocols to send and receive data between devices. Each device is identified by a unique IP Address.

Firewall: A security tool (hardware or software) that monitors traffic. Based on set rules, it either allows, blocks, or drops data.

NETWORK DEVICES

An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.



NETWORK DEVICES

1. Router

- Connects multiple networks (like home network to the internet).
- Directs data packets to their correct destination.

2. Switch

- Connects devices within a network (like computers in an office).
- Forwards data only to the specific device it is meant for.

3. Hub

- Basic device that connects multiple devices in a network.
- Sends data to all devices (less efficient than a switch).

4. Bridge

- Connects and filters traffic between two networks or segments.
- Helps reduce network traffic.

5. Gateway

- Connects two different types of networks.
- Translates data between different protocols.

6. Access Point (AP)

- Provides wireless connectivity to devices.
- Extends a wired network into a Wi-Fi network.

7. Modem

- Converts digital data from a computer into signals for phone/cable lines and vice versa.
- Provides internet access.

8. Firewall

- Monitors and controls incoming and outgoing network traffic.
- Provides security by blocking unauthorized access.

GOALS OF NETWORKS

- **Convenience**: Make computer use easier for users.
- **Efficiency:** Manage hardware resources effectively for better performance.
- **Resource Management:** Allocate CPU, memory, I/O, and storage fairly and efficiently.
- **Security & Protection**: Protect data and resources from unauthorized access.
- **Reliability & Fault Tolerance:** Ensure system runs smoothly and recovers from failures.
- **Scalability:** Support growth in users, processes, and resources.

USES OF COMPUTER NETWORKS

- **Communication**: Email, chat, and video conferencing.
- **Resource Sharing**: Share printers, scanners, and files to save cost and effort.
- **Remote Access**: Access data and systems from anywhere.
- **Collaboration**: Work together on projects, share ideas, and review work.
- **E-commerce**: Enable online shopping and secure payments.
- **Education**: Support online learning, research, and student–teacher collaboration.

CHARACTERISTICS OF COMPUTER NETWORKS

1. Security

Protects data from unauthorized access, hacking, and viruses.

Uses tools like firewalls, encryption, and authentication to ensure safety.

2. Reliability

Ensures data and resources are always available.

Redundancy and backups keep the network running during failures.

3. Scalability

The ability to grow and handle more devices/users without performance loss.

Example: The internet supports millions of new users daily.

4. High Performance

Fast data transfer, low latency, and high throughput improve user experience.

Performance depends on bandwidth, response time, and processing power.

5. Quality of Service (QoS)

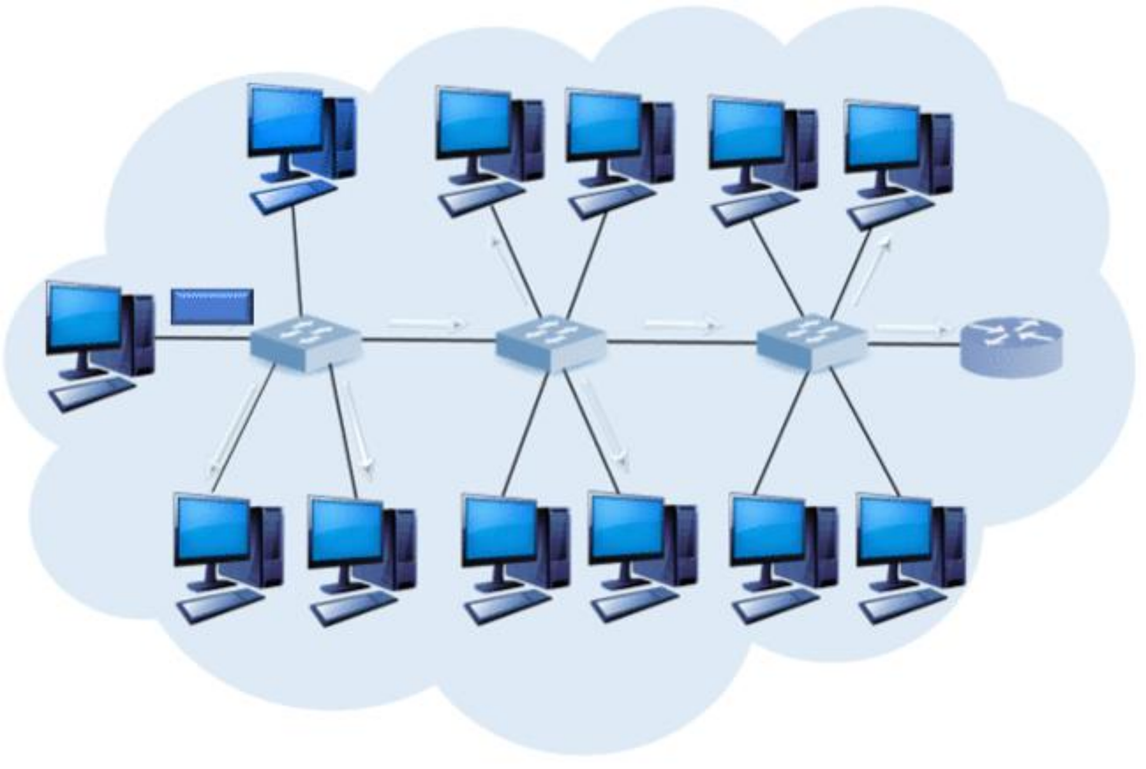
Prioritizes important data for faster delivery.

Ensures smooth communication, especially for streaming and video calls.

TYPES OF COMPUTER NETWORKS

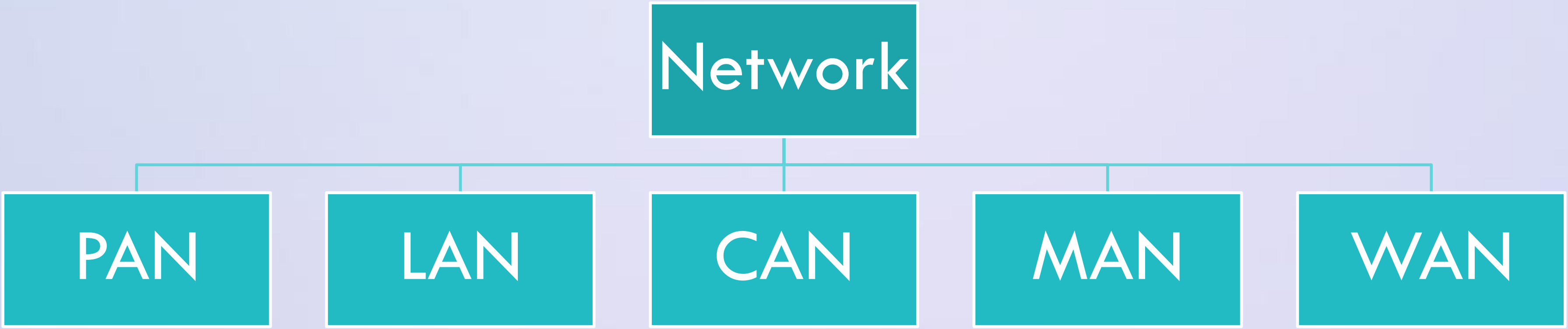
Computer networks are classified based on several factors, such as:

- Geographical area
- Ownership
- Architecture
- Topology
- Transmission technology



CLASSIFICATION BASED ON GEOGRAPHICAL AREA

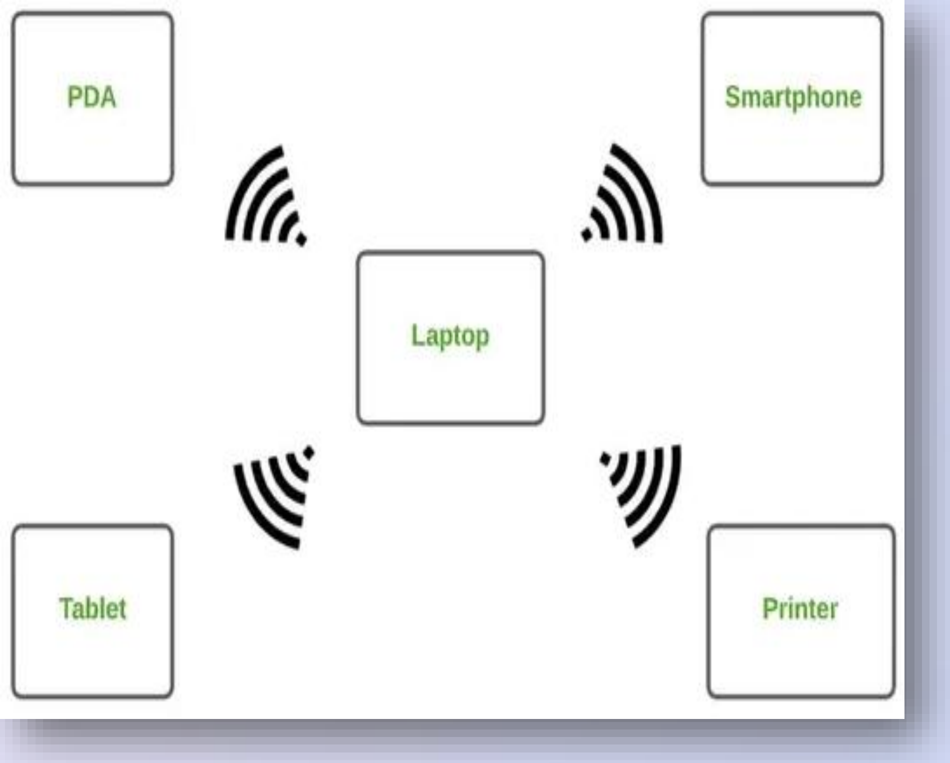
This is the most common way of classifying networks below are the different types :



PERSONAL AREA NETWORK (PAN)

PAN is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate and share data with each other. PAN offers a network range of 1 to 10 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost.

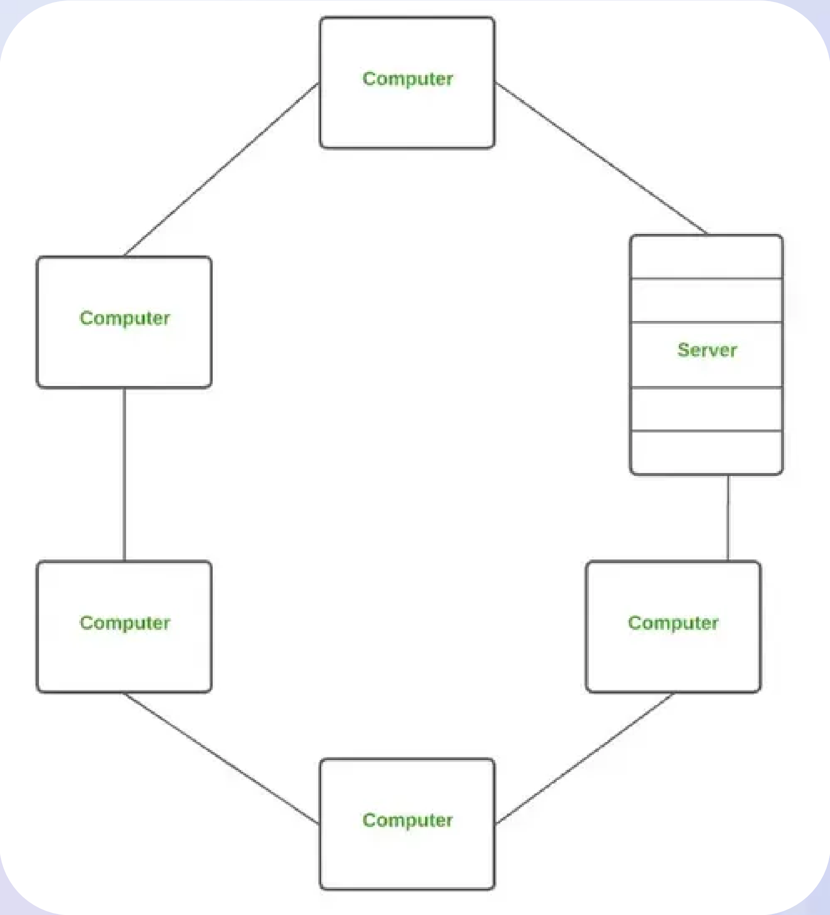
Examples of PAN are Bluetooth connection between a phone and wireless earbuds , Infrared communication between TV and remote, Smart Watch with Phone, etc.



LOCAL AREA NETWORK (LAN)

LAN is the most frequently used network. It is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi. It ranges up to 2km & transmission speed is very high with easy maintenance and low cost.

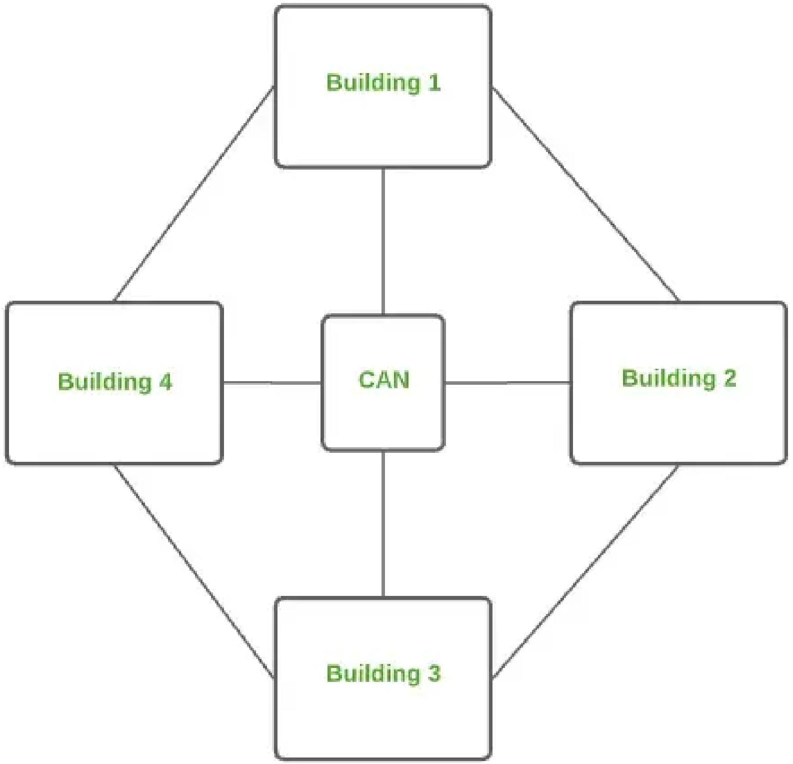
Examples of LAN are Wi-Fi in a home or school, wired LAN in a company's office.



CAMPUS AREA NETWORK (CAN)

CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network that is usually used in places like a school or colleges. This network covers a limited geographical area that is, it spreads across several buildings within the campus. CAN mainly use Ethernet technology with a range of few kilometers. Its transmission speed is very high with a moderate maintenance cost and moderate cost.

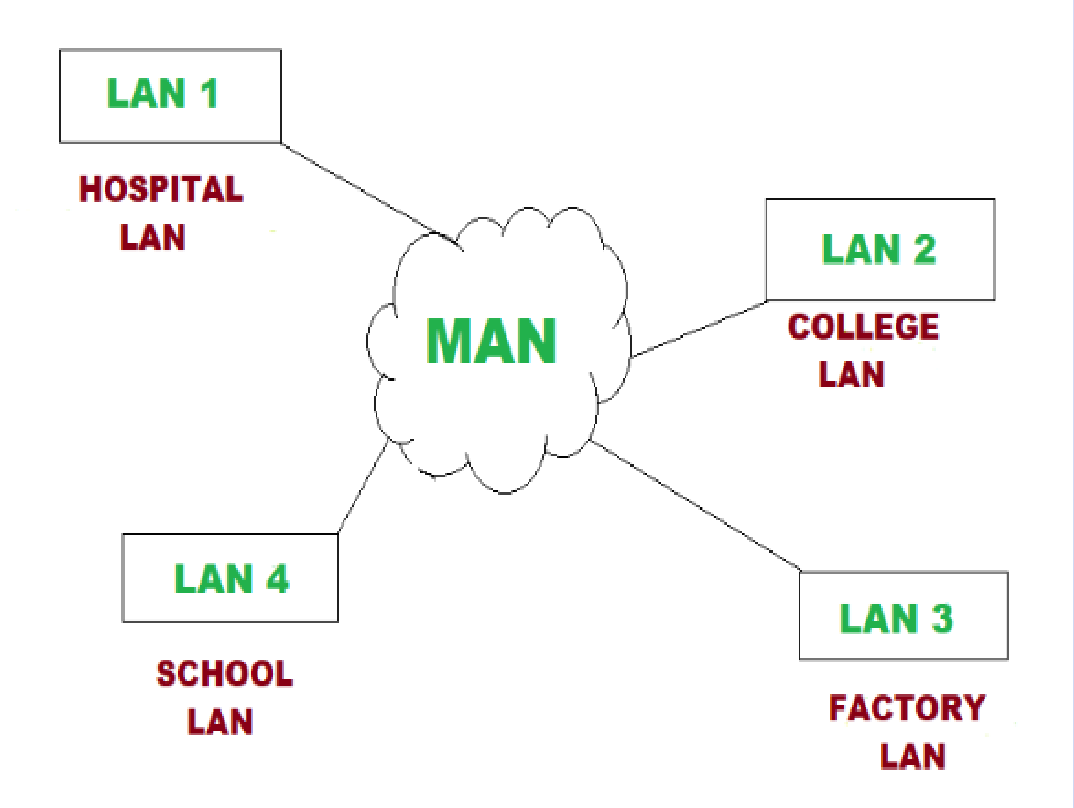
Examples of CAN are networks that cover schools, colleges, buildings, etc.



METROPOLITAN AREA NETWORK (MAN)

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost.

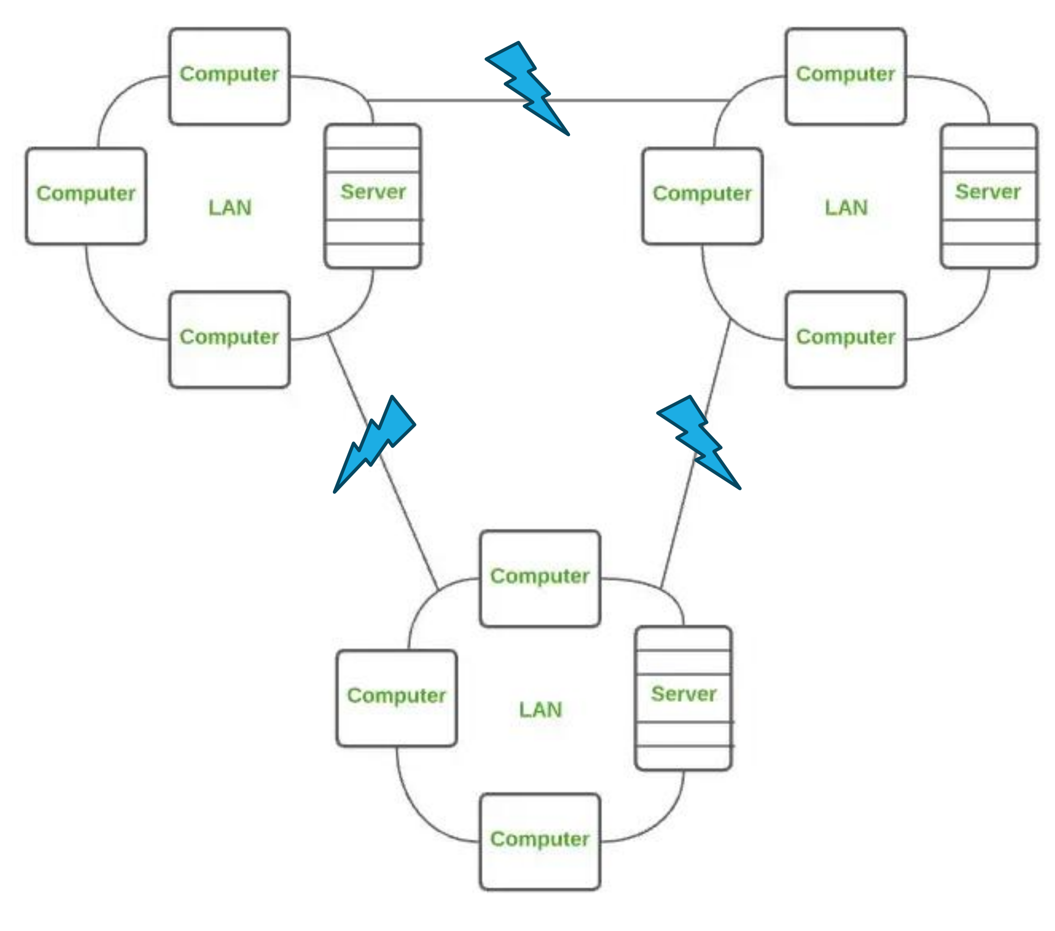
Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.



WIDE AREA NETWORK (WAN)

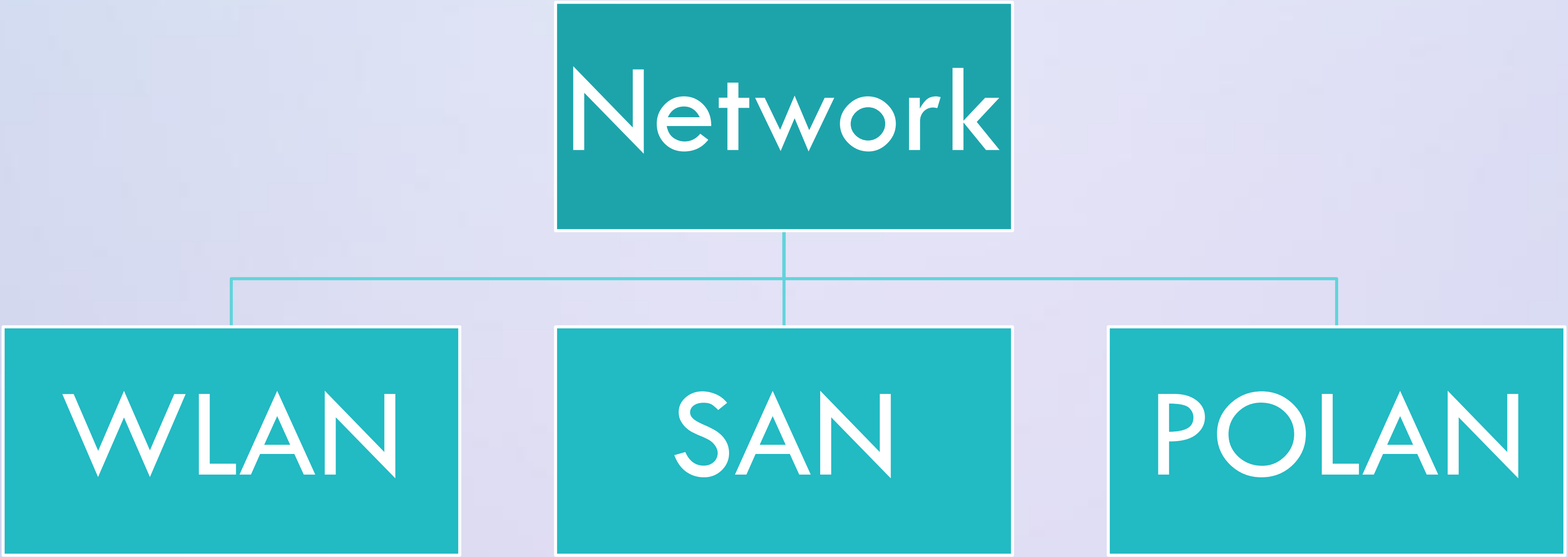
WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost.

Examples of WAN are the Internet (largest WAN), Banking networks linking global branches



CLASSIFICATION BASED ON TRANSMISSION TECHNOLOGY

This is the most common way of classifying networks below are the different types :



Network

WLAN

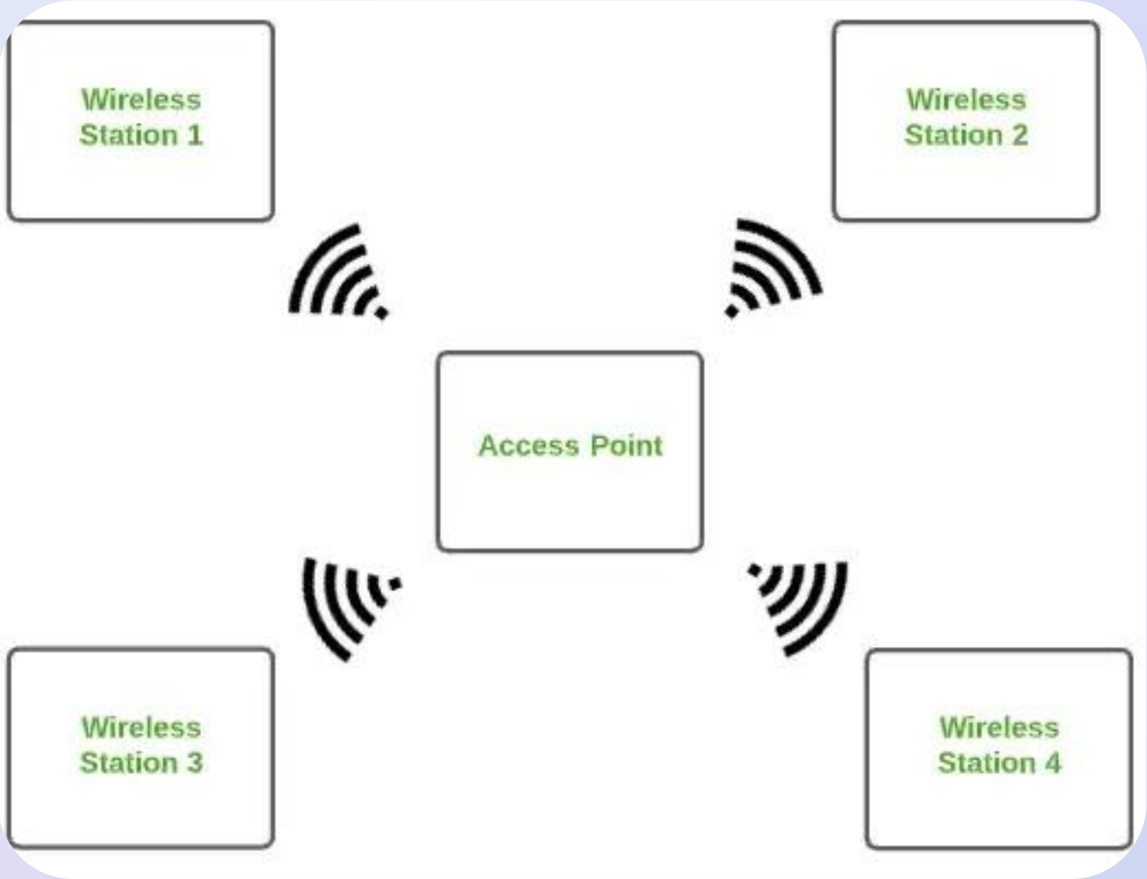
SAN

POLAN

WIRELESS LOCAL AREA NETWORK (WLAN) :

WLAN is a type of computer network that acts as a local area network but makes use of wireless network technology like Wi-Fi. This network doesn't allow devices to communicate over physical cables like in LAN but allows devices to communicate wirelessly.

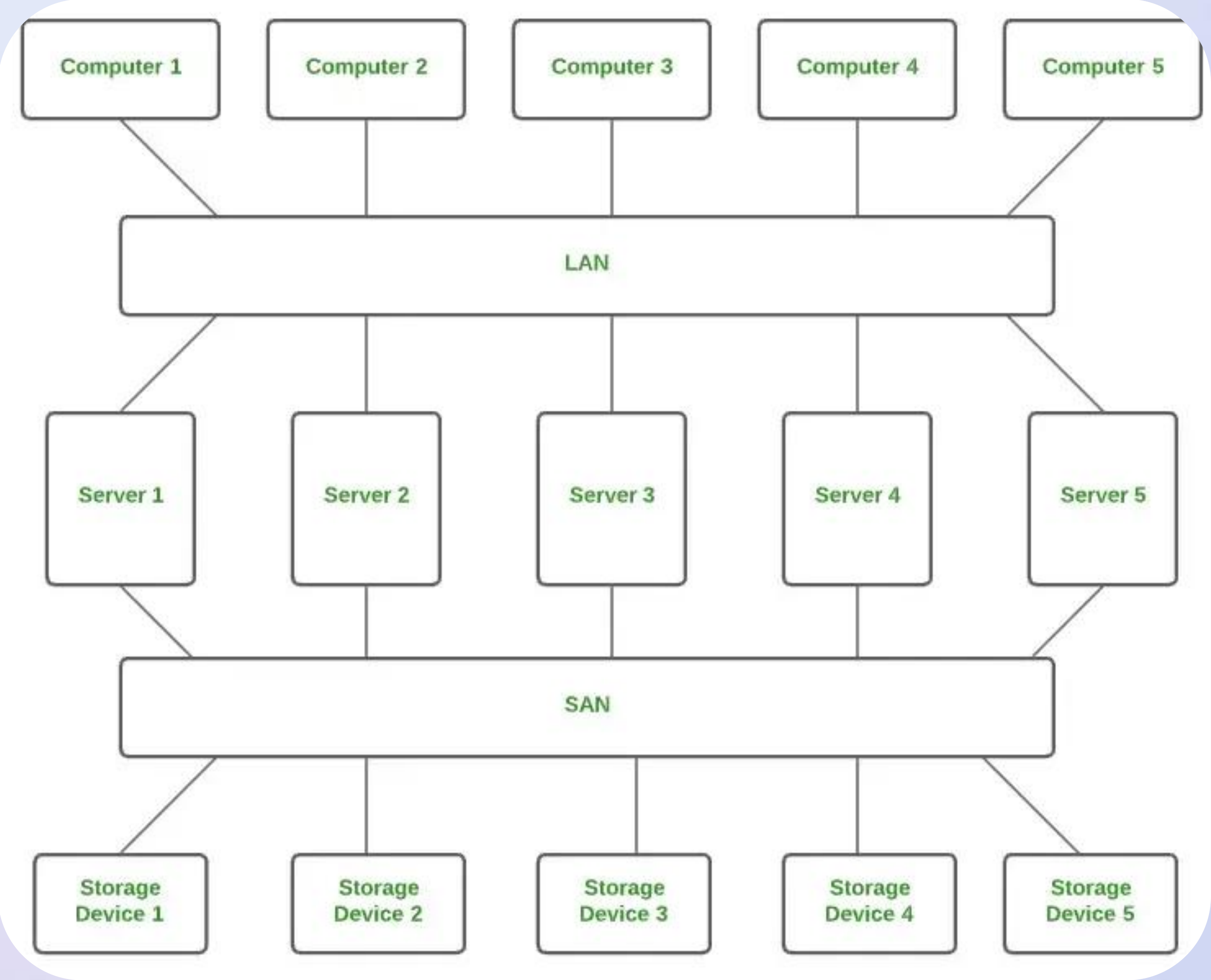
Most common example of WLAN is Wi-Fi.



SYSTEM AREA NETWORK (SAN)

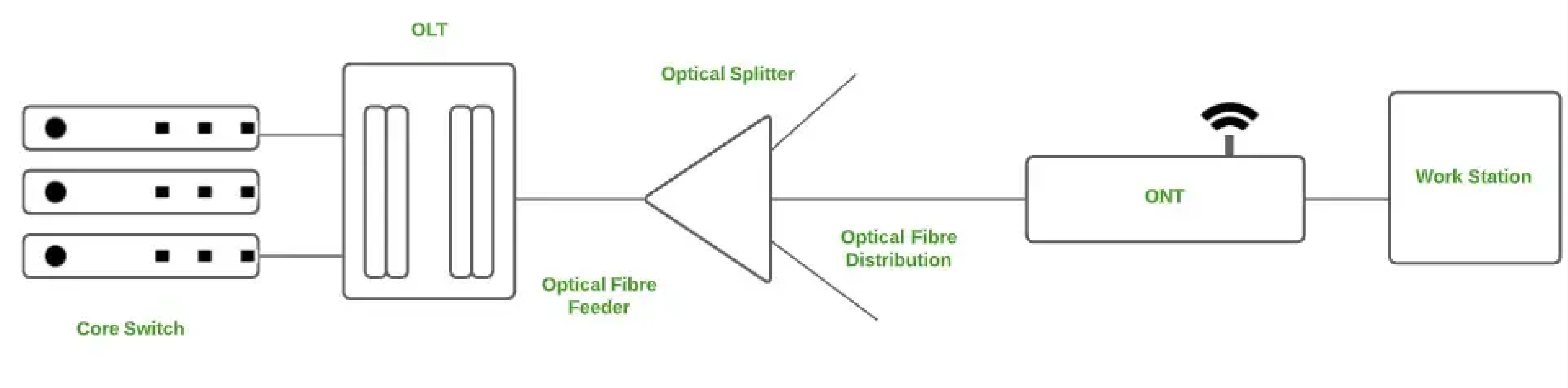
A System Area Network is designed to connect high-performance computers within a localized, high-speed environment, such as in data centers or supercomputing facilities. A SAN provides access to block-level data storage.

Examples of SAN are a network of disks accessed by a network of servers.



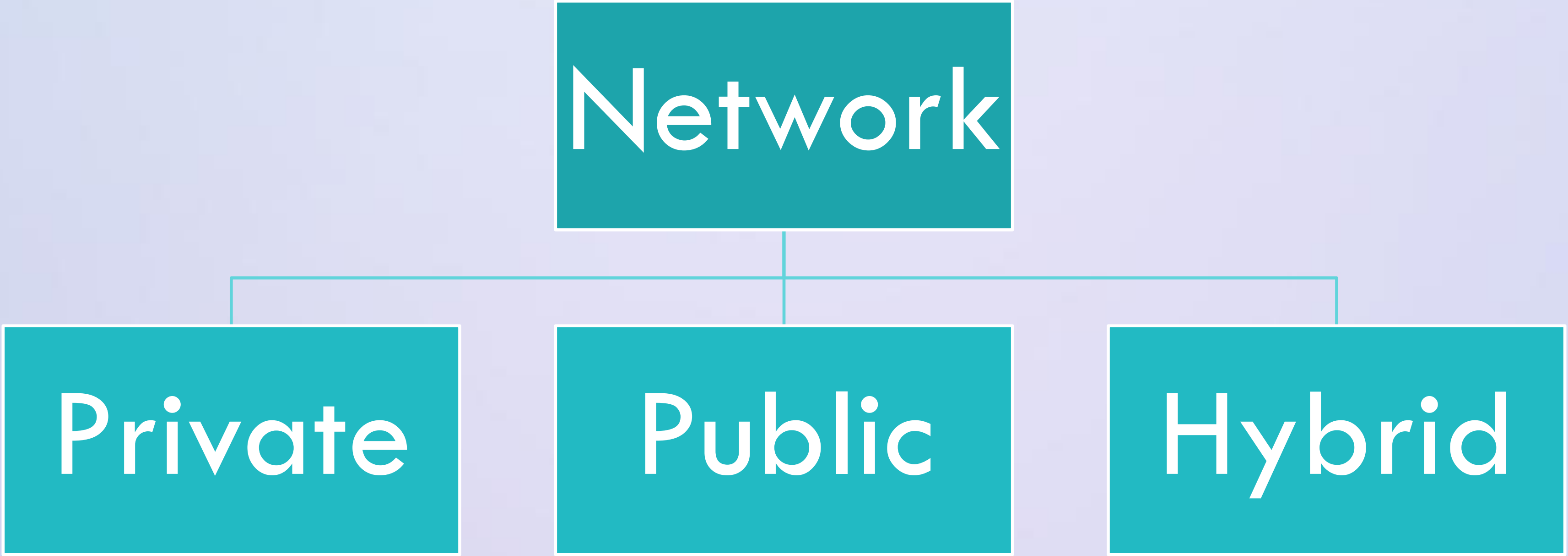
PASSIVE OPTICAL LOCAL AREA NETWORK (POLAN)

A POLAN is a type of computer network that is an alternative to a LAN. POLAN uses optical splitters to split an optical signal from a single strand of single-mode optical fiber to multiple signals to distribute users and devices. In short, POLAN is a point to multipoint LAN architecture.



CLASSIFICATION BASED ON OWNERSHIP AND ACCESS CONTROL

We can classify networks into three main types based on ownership and how access is controlled: **Private**, **Public**, and **Hybrid** networks.



PRIVATE NETWORK

These are networks completely owned and managed by a single organization or individual. The owner controls who can connect, what they can do, and how data moves within the network. Since there is no outside access, they are highly secure and reliable, often protected by firewalls and strict policies.

Examples: A company's internal office network (Intranet), School or college campus networks, Hospital systems storing patient data

PUBLIC NETWORK

These are networks open to the general public and are usually provided by Internet Service Providers (ISPs) or businesses in public places. They offer basic or no authentication, making them less secure and vulnerable to attacks if not used carefully.

Examples: Public Wi-Fi at cafes or airports, free hotspots in city centers, Internet (the largest public network).

HYBRID NETWORK

A hybrid network blends private and public access, offering flexibility and role-based access control. Some parts are restricted (like internal systems), while others are open (like guest Wi-Fi). This setup is useful in environments where different users need different access levels.

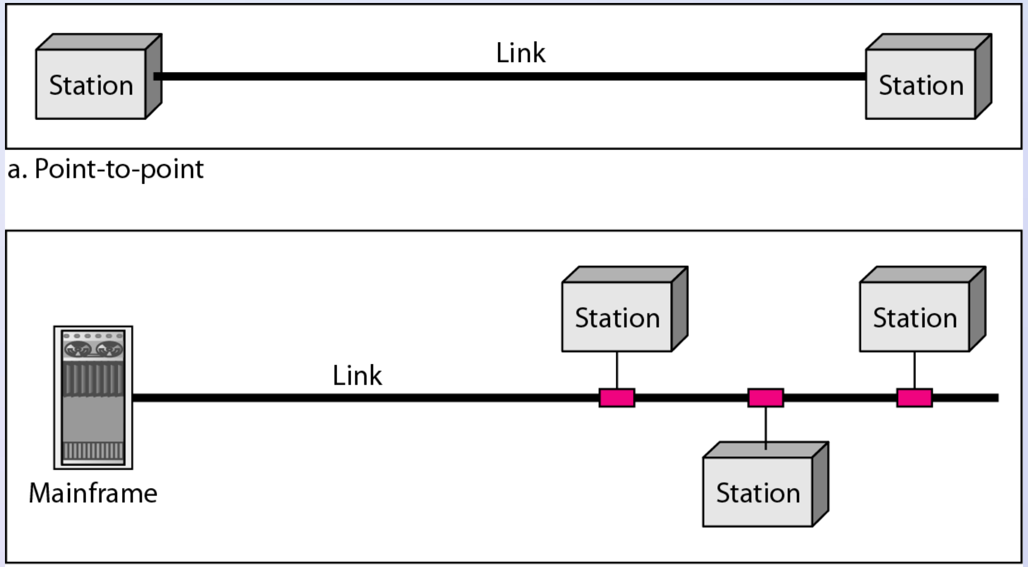
Example: A university network with private access for staff and students and limited access for guests.

TOPOLOGY

Network topology refers to the physical and logical arrangement of nodes and connections in a computer network, which governs how data flows between devices. Network topology impacts network performance, security and scalability, making it a crucial concept in network design and management.

PHYSICAL STRUCTURES

- **Type of Connection**
  - Point to Point - single transmitter and receiver
  - Multipoint - multiple recipients of single transmission

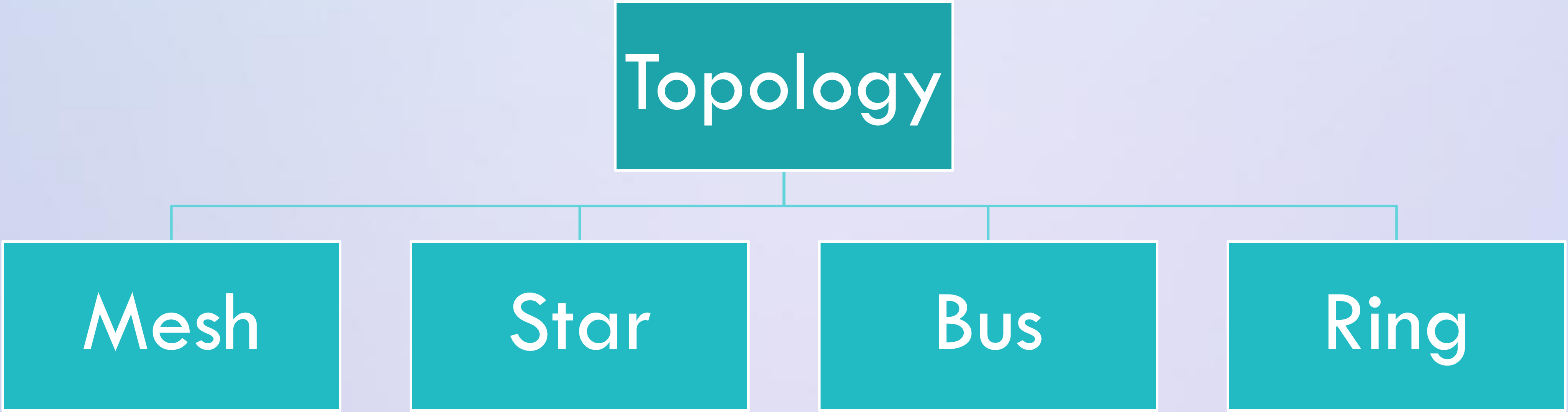


a. Point-to-point

b. Multipoint

- **Physical Topology**
  - Connection of devices
  - Type of transmission - unicast, multicast, broadcast

CATEGORIES OF TOPOLOGY



Topology

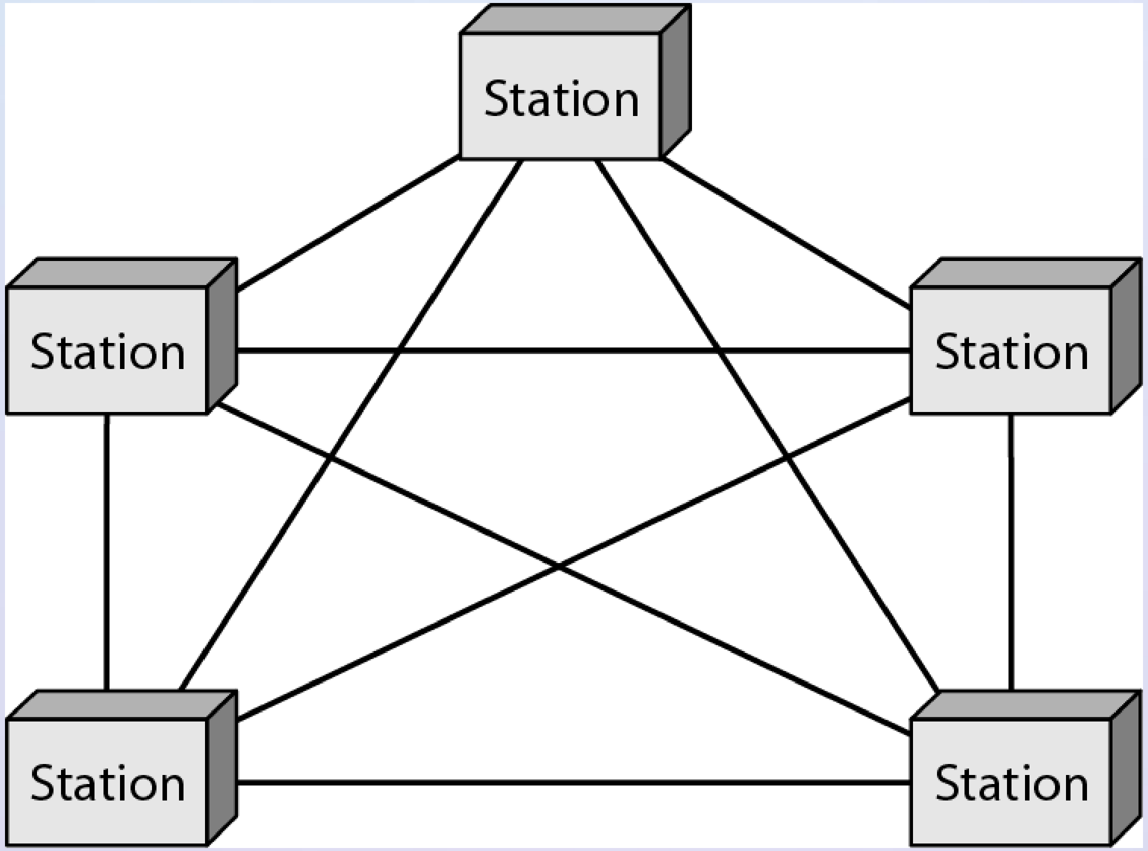
Mesh

Star

Bus

Ring

A FULLY CONNECTED MESH TOPOLOGY



In mesh topology, we need n(n -1) /2 duplex-mode links

ADVANTAGE OF MESH TOPOLOGY

1- Use of dedicated links guarantees that each connection can carry its own data load.

2- Robust. If one link becomes unusable, it does not incapacitate the entire system.

3- Security. When every message travels along a dedicated line, only the intended recipient sees it.

4- Point-to-point links make fault identification and fault isolation easy.

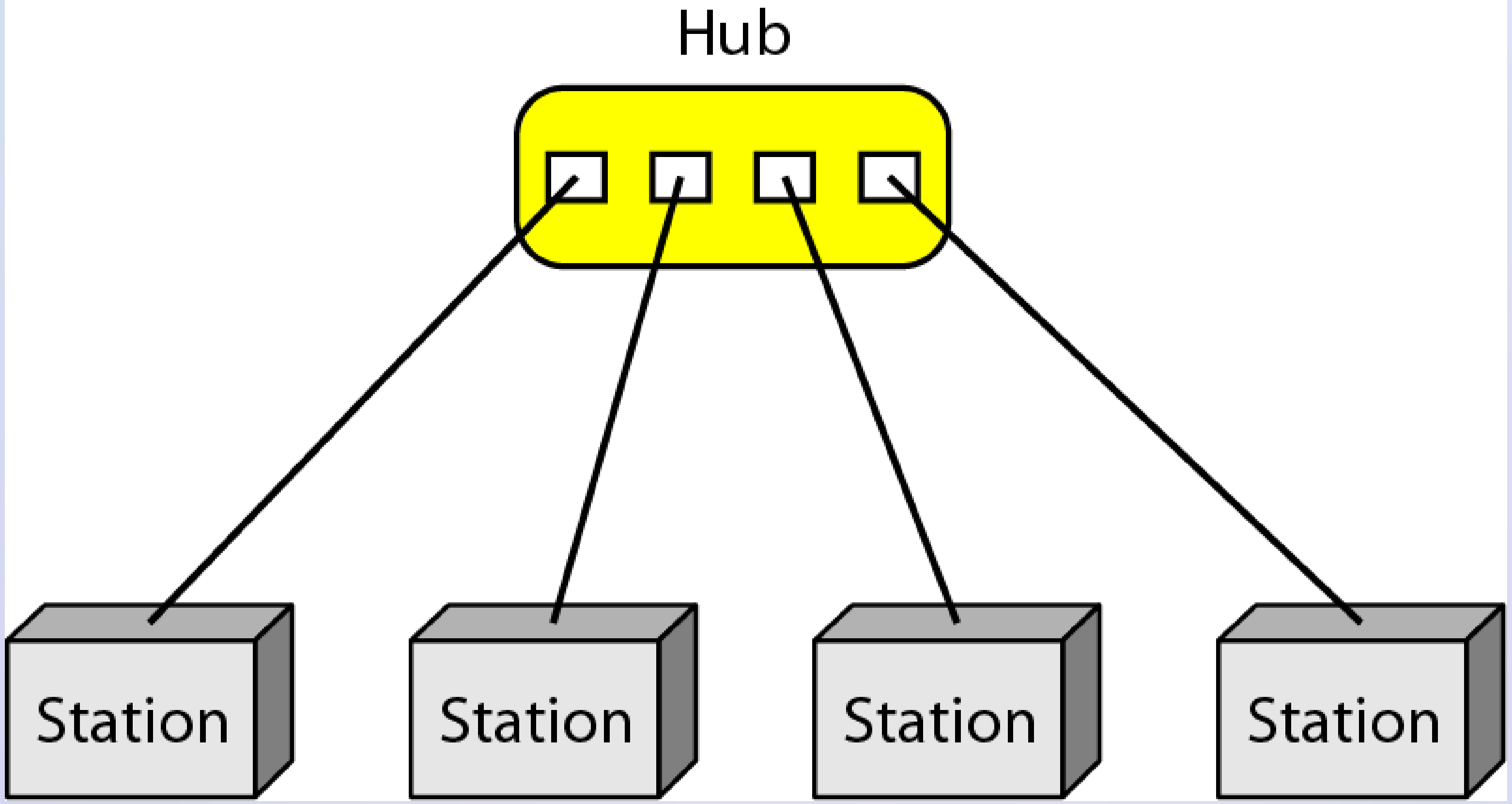
DISADVANTAGE OF MESH TOPOLOGY

1- The amount of cabling because every device must be connected to every other device.

2- The number of I/O ports required.

3- The hardware required to connect each link can be prohibitively expensive.

A STAR TOPOLOGY



STAR TOPOLOGY

Advantage of Star topology

1- Less expensive than a mesh topology.

2- Easy to install and reconfigure. Far less cabling needs to be housed.

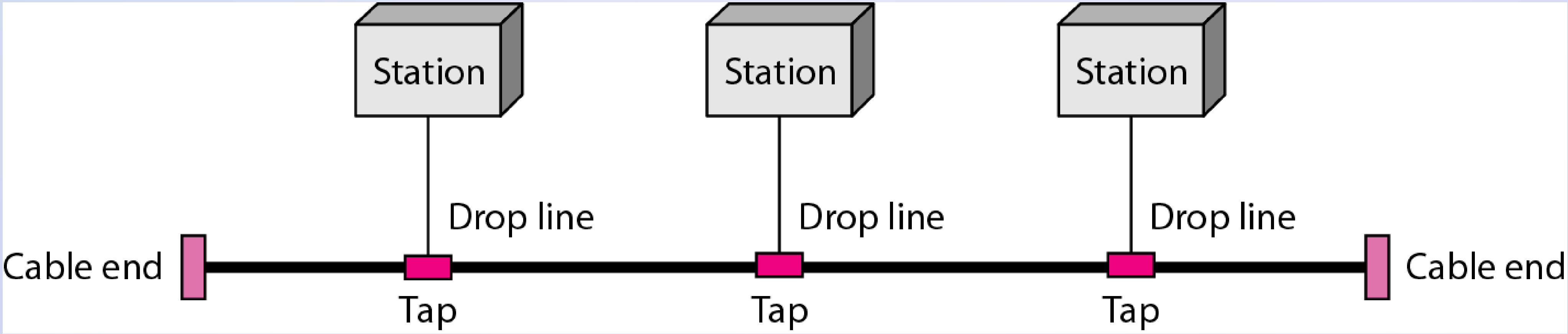
3- Include robustness.

Disadvantage of Star topology

1- the dependency of the whole topology on one single point.

2- more cabling is required in a star than in some other topologies (such as ring or bus).

A BUS TOPOLOGY



ADVANTAGE OF BUS TOPOLOGY

1- Ease of installation.

2- Less cabling than mesh or star topologies.

3- Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.

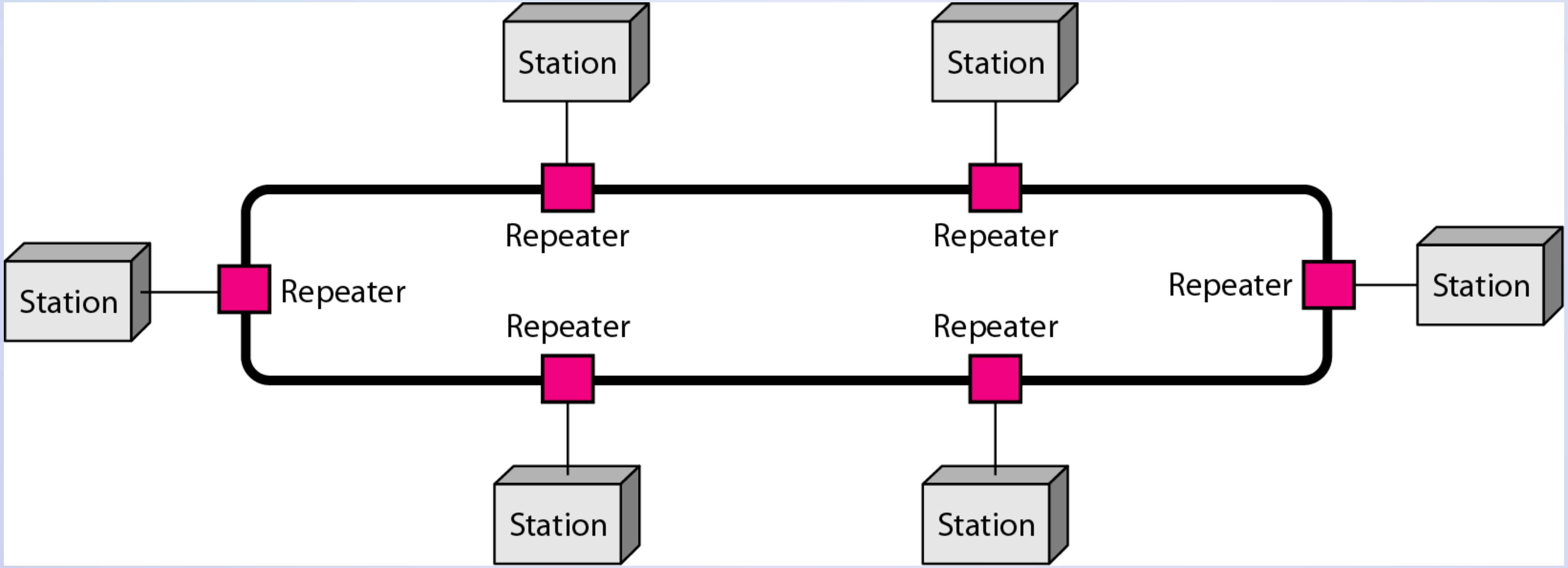
DISADVANTAGE OF BUS TOPOLOGY

1- Difficult reconnection and fault isolation.

2- Signal reflection at the taps can cause degradation in quality.

3- Fault or break in the bus cable stops all transmission.

A RING TOPOLOGY



RING TOPOLOGY

Advantage of Ring topology

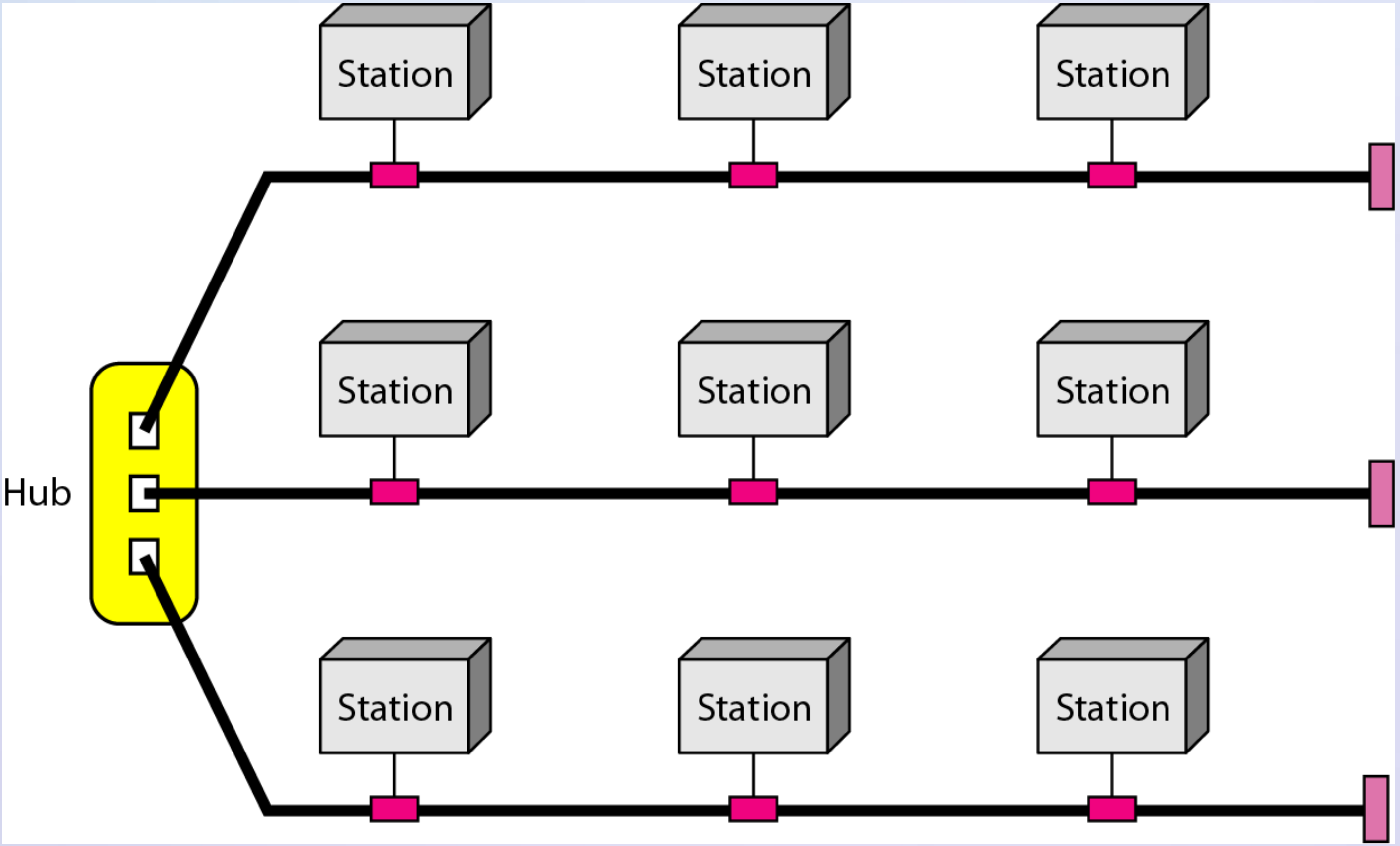
1- Easy to install and reconfigure.

2- Fault isolation is simplified.

Disadvantage of Ring topology

- Unidirectional traffic.

A HYBRID TOPOLOGY



ANY question?