Data Communication & Networking

Trainer : Sujata Mohite
Email: sujata.mohite@sunbeaminfo.com

Contents

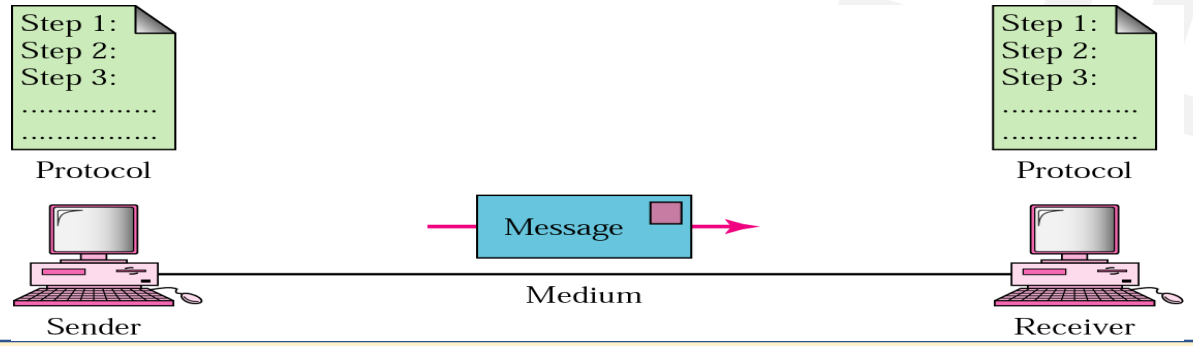
- Network Terminologies
- Need of Network
- Network Types
- Media (Transmission Medium)
- Switching
- Multiplexing
- Network Classification (LAN, MAN, WAN)
- ARP
- Network Classification by Component Role
- Network Physical Structure
  - Types of Connection
  - Physical Topology
- Network Devices
- Addressing
- OSI Layers

Network Terminologies

•connecting multiple devices (computers) together to share the information group of devices/machines/IP addresses/hosts.

- **Data**
- **Communication**
- **Network**
- **Computer Network**

Components of Data communication



Node

- any device connected to the network(a computer, a printer etc)

Network Interface Card (NIC)

- is the circuit board that is used to connect computers to the network.
- In most cases, this is an *Ethernet* card plugged in a computer's motherboard

The effectiveness of a data communications system depends on four fundamental characteristics: Delivery, Accuracy , Timeliness , Jitter

Network Terminologies

- Node - Any device connected to a network (computer, printer, router, etc.)
- Host - A device that sends or receives data over a network (typically has an IP)
- NIC (Network Interface Card) - Hardware that connects a device to a network
- Protocol - A set of rules for communication (e.g., TCP/IP, HTTP, FTP)
- IP Address - Unique identifier assigned to a device on a network
- MAC Address - Hardware-based physical address assigned to NIC
- Bandwidth - Maximum data transfer capacity of a network
- Latency - Delay in data transmission (measured in milliseconds)
- Throughput - Actual amount of data transmitted over a network
- Topology - The physical or logical arrangement of network devices (e.g., star, bus)

Fundamental Characteristics of a Data Communication System

- Data communications means the exchange of data between two devices via some form of transmission medium such as a wire or cable.

- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

- The effectiveness of a data communications system depends on four fundamental characteristics:

1) Delivery
2) Accuracy
3) Timeliness
4) Jitter

Fundamental Characteristics of a Data Communication System

1. Delivery:
The primary task of a data communication system is to deliver or transfer data from sender to receiver. The system must deliver data to the exact destination. No other receiver should receive the data. This characteristics includes the security of the system, that is, the protection of data.

2. Accuracy:
The data communication system must deliver data to the receiver without being altered or damaged. The receiver should receive the exact same data which was sent by the sender. The protocol should also reverse and restore the data back to its original form before representing it to the receiver. The accuracy must be maintained.

3. Timeliness:
The system must maintain timeliness. It must deliver data in a timely manner. Delayed delivery can make the data useless to the receiver. Data must be delivered as they are produced like real-time transmission, in the order they are produced and without any significant delay.

4. Jitter:
Jitter refers to the variation of packet arrival time. Data is sent as packets, audio or video packets so chunk of the whole data is sent in each turn. These packets get re-joined back in the target device to represent the complete data as it is. If some of the packets arrive with some delay, an uneven quality in the video or audio is the result.

Need of Network/ Applications of Network

- Information Sharing
- Enhance communication
- Share resources
- Facilitate centralized management
- Remote computing
- E-commerce, Education, Entertainment

Network Criteria

Performance

- depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.
- Measured in terms of Delay and Throughput(how much data is transferred successfully from the sender node to the receiver node in a particular time frame. It is measured in bits per second or data per second.)

Reliability

- is measured by the frequency of failure, the time it takes a link to recover from a failure
- Measured in terms of availability/robustness

Security

- Data protection against corruption/loss of data due to:
  - Errors
  - Malicious users

Media (Transmission Medium)

Types of Transmission Media

Wired

Medium

- Wire / Cable

Cable Types

- co-axial
  - transfers the data in the form of electrical signals
- CAT Cable / Twisted Pair Cable (STP/UTP)
  - transfers the data in the form of electrical signals
- Fiber Optics
  - transfers the data in the form of light
  - Minimum 10gbps

Types

- LAN , MAN , WAN

- cat1 : - [it was used only for telephony network]
- cat2 : 1 mbps
- cat3 : 10 mbps
- cat4 : 16 mbps
- cat5 : 100 mbps
- cat5e: 125 mbps
- cat6 : 1000 mbps ~ 1 gbps
- cat7 : 10000 mbps ~ 10 gbps
- cat8 : 25000 mbps ~ 25 gbps

Wireless

Medium

- Air (EM Waves)

Cable Types

- PAN
- WLAN
- WAN (GSM)

Transmission Medium

- For any networking to be effective, raw stream of data is to be transmitted from one device to other over some medium.
- Various transmission media can be used for transfer of data.

Types of Transmission Medium

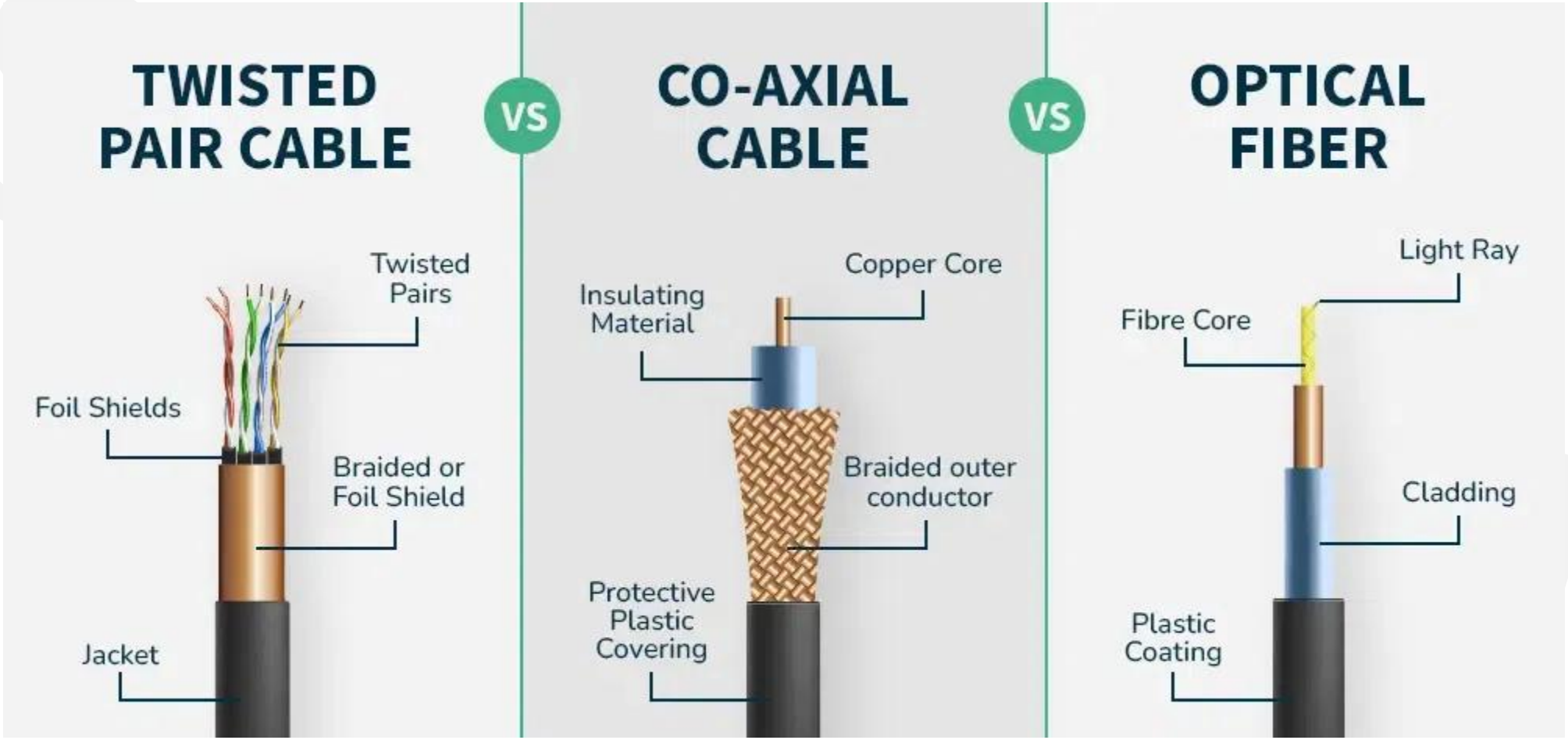
Guided

- Transmitted data travels through cabling system that has a fixed path.
- For example, copper wires, fibre optic wires, etc.

Unguided

- Transmitted data travels through free space in form of electromagnetic signal.
- For example, radio waves, lasers, infrared, electromagnetic waves, etc

Wired or Guided Medium

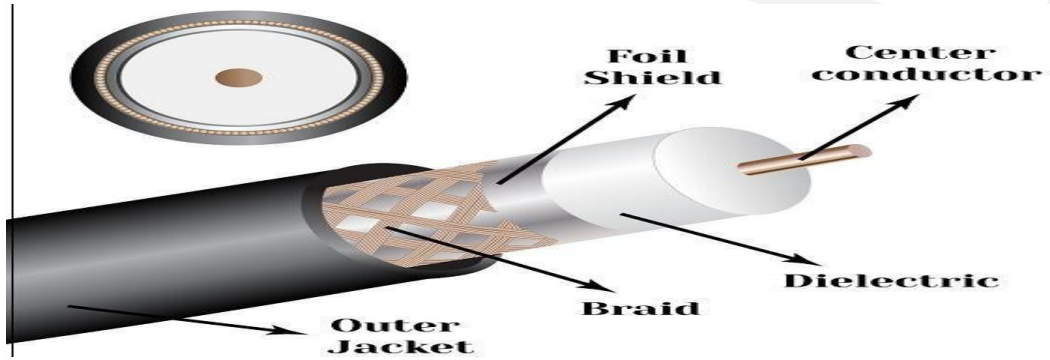


Twisted Pair(maximum length of 100 meters)

- Most common wires used for transmitting signals
- To reduce this electromagnetic interference, pair of copper wires are twisted together.
- Shielding twisted pair cable
  - To counter the tendency of twisted pair cables to pick up noise signals, wires are shielded .
  - Such twisted pairs are called **shielded twisted pair (STP) cables**.
- The wires that are not shielded but simply bundled together in a protective sheath are called **unshielded twisted pair (UTP) cables**.

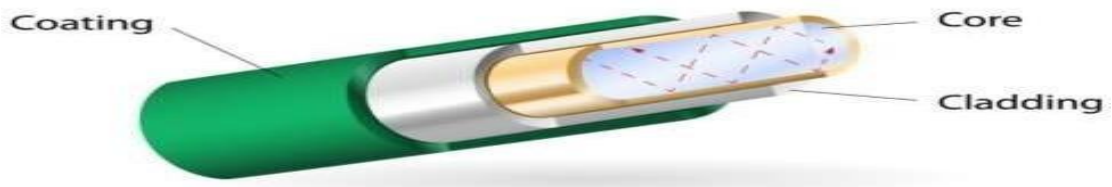
Coaxial Cable

- Coaxial cables are widely used for **cable TV** connections and **LANs**.
- **Coaxial cables** are copper cables with better **shielding** than twisted pair cables.
- Transmitted signals may travel **longer distances** at higher speeds.
  - e.g. 1 to 2 Gbps for 1 Km cable
- Can be used for both analog and digital signals
- Inexpensive as compared to fiber optic cables
- Easy to install and maintain



Optical Fiber

- Thin glass or plastic threads used to transmit data **using light waves** are called **optical fiber**.
- Signals carrying data can travel long distances without weakening
- Immune to electromagnetic interference , Suitable for industrial and noisy areas
- Three Layers:
  - **Core** made of high quality **silica glass** or **plastic**
  - **Cladding** made of high quality **silica glass** or **plastic**, with a lower refractive index than the core
  - Protective outer covering called **buffer**



Transmission Modes

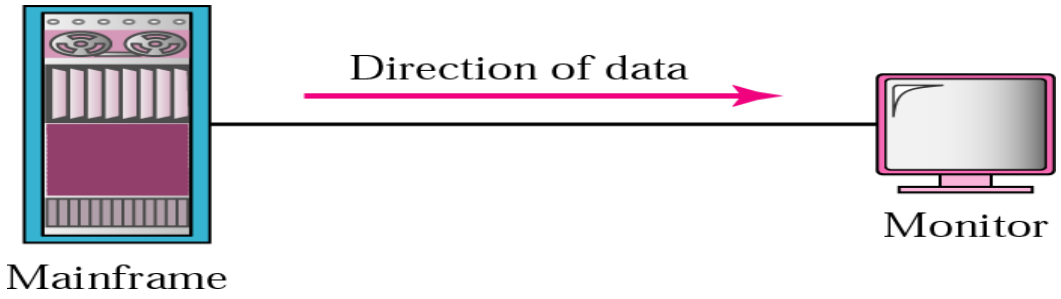
Transmission Modes

Q. What is Transmission Modes?

- Transmission mode means transferring data between two devices. It is also known as a communication mode

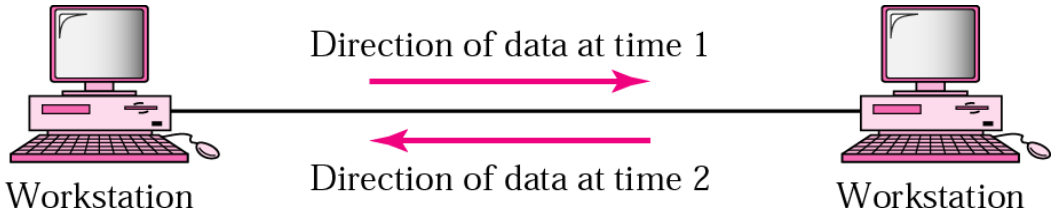
The data that needs to be transferred between the devices.
It can be any device that can send the raw data.
It is the device that receives the data that the sender sends.
The medium between the sender and receiver can be wired, wireless, or both types.
The Protocol can vary according to the modes of transmission.

Transmission Modes / Data Flow Direction



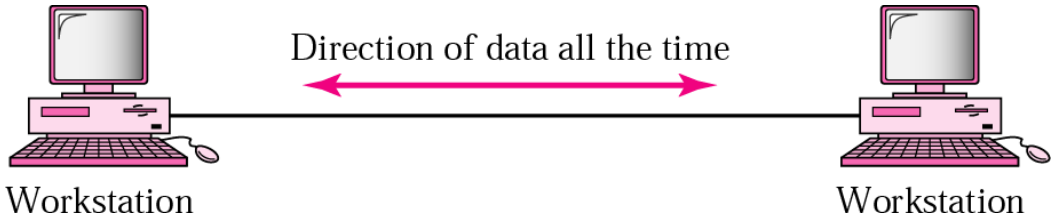
Simplex Mode

- Example: Keyboard and traditional monitors.



Half-Duplex Mode

- each station can both transmit and receive, but not at the same time.
- Example: Walkie- talkie



Full-Duplex Mode

- Example: Telephone Network there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

1) Simplex Mode

- In Simplex mode, the communication is unidirectional.
- Only one of the two devices on a link can transmit, the other can only receive.
- **The simplex mode can use the entire capacity of the channel to send data in one direction.**
- **Eg**: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.
- Simplex mode is the easiest and most reliable mode of communication.
- It is the most cost-effective mode, as it only requires one communication channel.
- **There is no need for coordination between the transmitting and receiving devices, which simplifies the communication process.**
- Simplex mode is particularly useful **in situations where feedback or response is not required, such as broadcasting or surveillance.**

2) Half Duplex Mode

- Here each station can both transmit and receive, but not at the same time.
- When one device is sending, the other can only receive, and vice versa.
- The half-duplex mode is used in cases where there is no need for communication in both directions at the same time.
- The entire capacity of the channel can be utilized for each direction.
- **It is a more efficient mode of communication than simplex mode, as the channel can be used for both transmission and reception**.
- **Half-duplex mode is less expensive than full-duplex mode**, as it only requires one communication channel.
- **Eg**: Walkie-talkie in which message is sent one at a time and messages are sent in both directions.

3) Full Duplex Mode

- In full duplex mode, both stations can transmit and receive simultaneously.

- Full-duplex mode is used when communication in both directions is required all the time.

- Full-duplex mode allows for simultaneous bidirectional communication, **which is ideal for real-time applications such as video conferencing or online gaming.**

- It is the most efficient mode of communication, as both devices can transmit and receive data simultaneously.

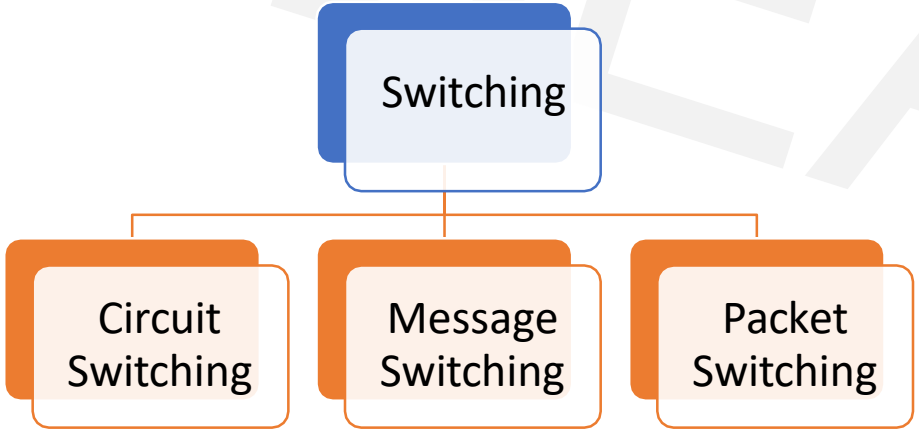
- Full-duplex mode provides a **high level of reliability and accuracy, as there is no need for error correction mechanisms.**

- **Eg**: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

Switching

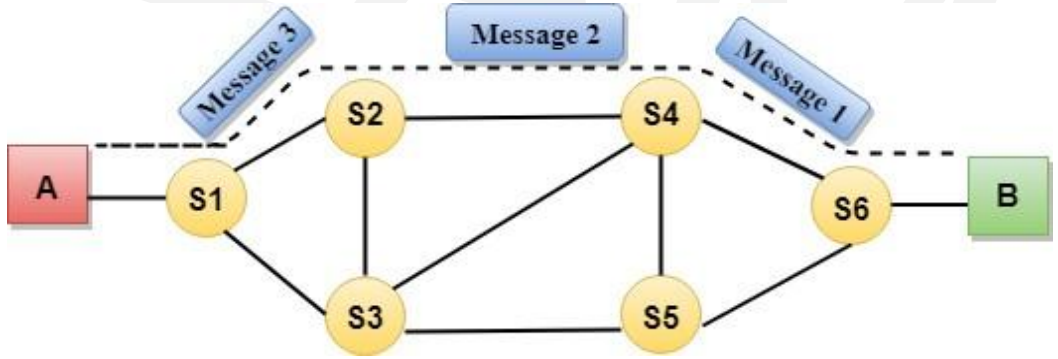
Switching

- In large networks, there can be multiple paths from sender to receiver.
- The switching technique will decide the best route for data transmission.
- Switching technique is used to connect the systems for making one-to-one communication.
- The mechanism for exchange of information between different computer networks and network segments is called switching in Networking.



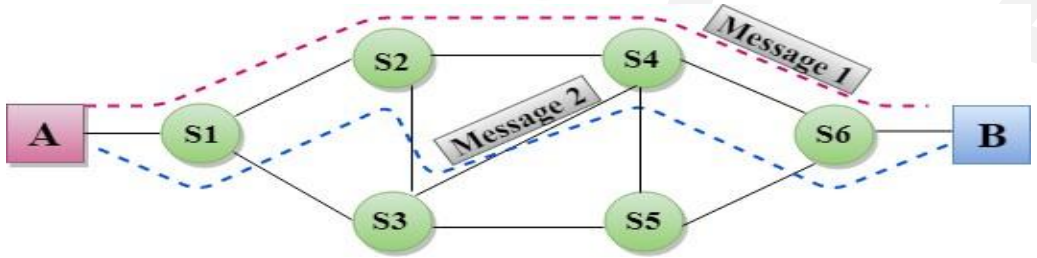
Circuit Switching

- **Establishes a dedicated path between sender and receiver.**
- **once the connection is established then the dedicated path will remain to exist until the connection is terminated.**
- Operates in a similar way as the **telephone** works.
- when any user wants to send the data a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- **Three Phases:**
  - **Circuit Establishment**
  - **Data Transfer**
  - **Circuit Disconnect**



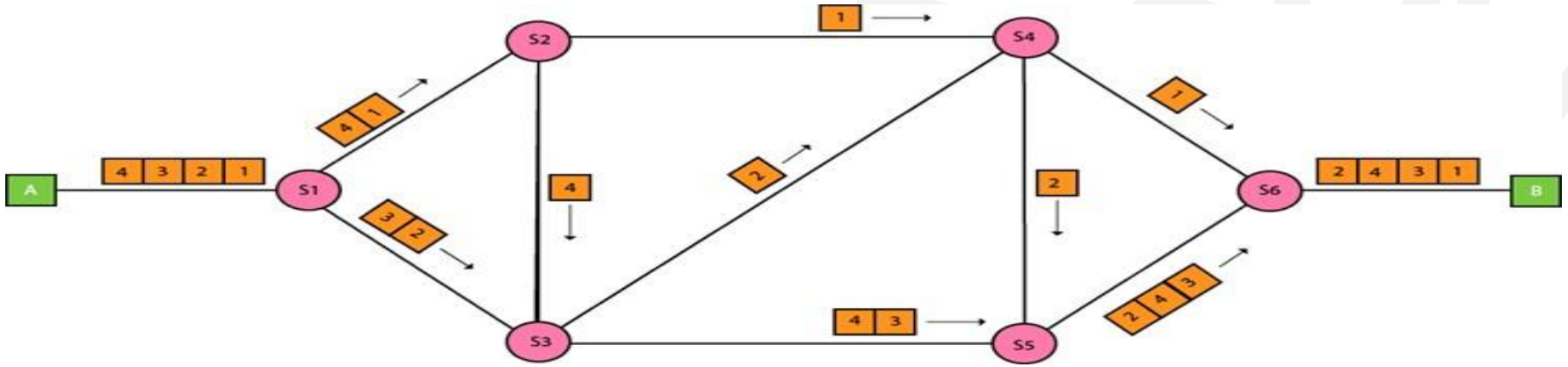
Message Switching

- There is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message.
- provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- they can provide the most efficient routes.
- Uses a method of **store and forward network**
- High delay due to storage and processing



Packet Switching

- Message is divided in packets , packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, **taking the shortest path as possible**.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent



Packet Switching

Advantages:

- Efficient use of network bandwidth
- More reliable (if one path fails, packets choose another)
- Supports many users at once
- Enables modern internet communication

Disadvantages

- Packets may arrive out of order
- Extra processing because each packet needs routing decisions
- Possible delays due to network congestion

Packet Switching

There are two types of Packet Switching:

1) Datagram Packet switching:

- It is a packet switching technology in which **packet is known as a datagram, is considered as an independent entity.**
- Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- **Here the path is not fixed.**
- Intermediate nodes take the routing decisions to forward the packets.
- **It is also known as connectionless switching**

2) Virtual Circuit Switching

- Virtual Circuit Switching is also known as **connection-oriented switching.**
- Here a **preplanned route is established before the messages are sent.**
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, **the path is fixed for the duration of a logical connection.**

Examples of packet switching

- **The Internet:** The global internet is the quintessential example, as it breaks all data (emails, web pages, videos) into packets that are routed independently through various network devices.

- **Voice over IP(VoIP) and video conferencing:** Voice and video are digitized and transmitted as packets, allowing for efficient communication over the internet.

- **Online gaming:** Actions in online games are sent as small data packets between the game client and server, enabling real-time, interactive gameplay.

- **Cloud computing:** Services and data transfer within cloud infrastructures rely heavily on packet switching to move data between servers and clients.

- **Remote monitoring and management(RMM):** Tools used for troubleshooting and updating remote devices use packet switching to maintain their connection and transmit commands and data.

Which switching technique is most efficient for real-time voice and video transmission?

A. Packet switching B. Circuit switching C. Message switching D. Frame Switching

Ans: A

In packet switching, how is data transmitted across the network?

A. In a continuous stream B. Through a dedicated path

C. In discrete units called packets D. By broadcasting

Ans: C

What is the one key advantage of message switching over circuit switching?

A. Faster setup time B. No dedicated path required C. Real-time transmission D. Lower cost

Ans: B

Which of the following best describes the concept of virtual circuit in packet switching?

A. A temporary path established for each session B. A permanent dedicated path

C. Broadcasting of packets to all nodes D. Use of encryption for data security

Ans: A

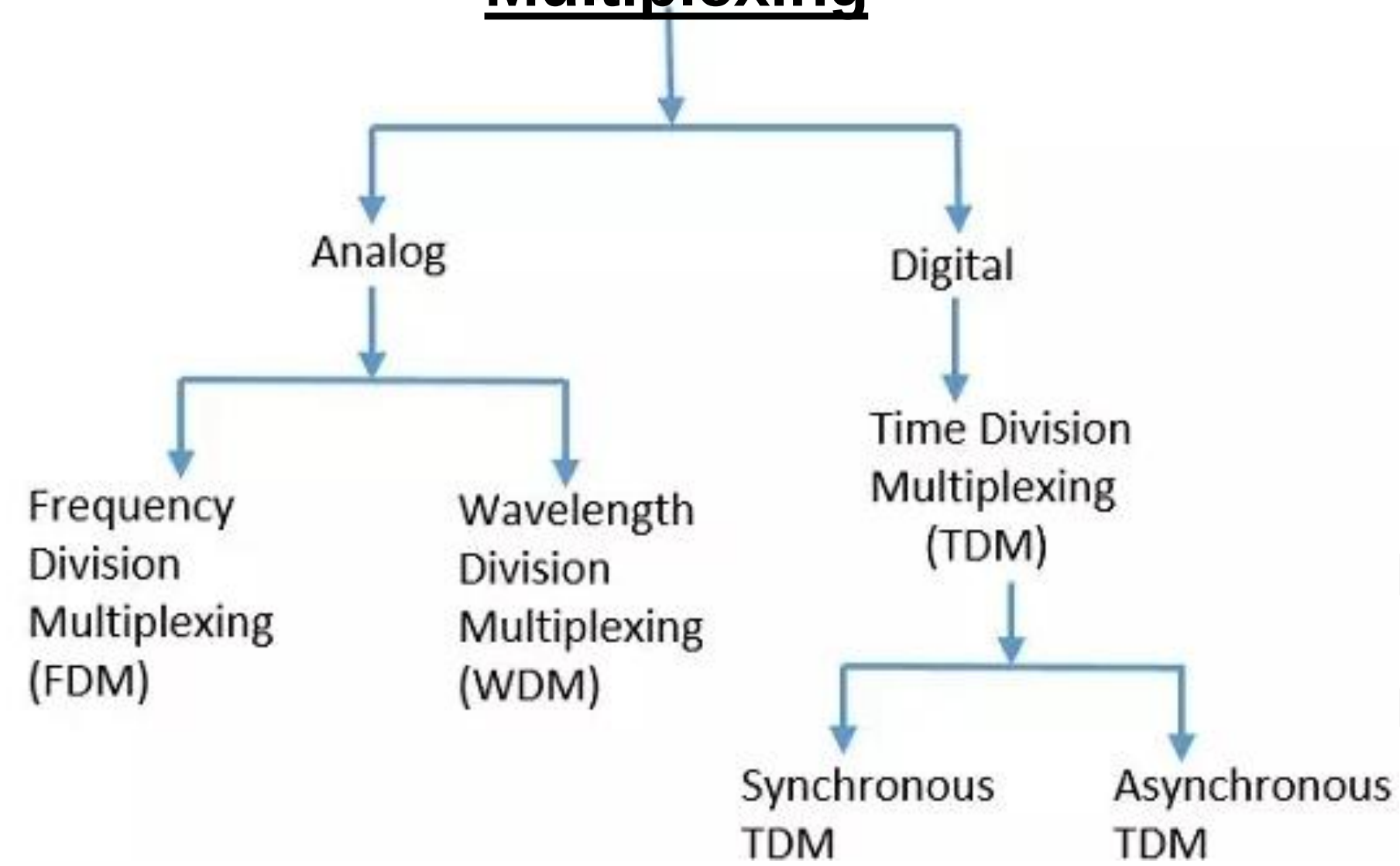
Multiplexing

Multiplexing

1. It's a method that **combines multiple signals or data streams into one signal over a shared medium.**
2. This process allows for efficient use of resources and can significantly increase the amount of data that can be sent over a network.
3. It is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.
4. **If analog signals are multiplexed, it is Analog Multiplexing and if digital signals are multiplexed, that process is Digital Multiplexing.**
5. The device that does **multiplexing** can be simply called as a **MUX** while the one that reverses the process which is **demultiplexing**, is called as **DEMUX**.
6. Reduce cost and complexity.
7. **Improve data transmission rates**

Multiplexing and Demultiplexing

Multiplexing



Multiplexing

Analog Multiplexing

The analog multiplexing techniques involve signals which are analog in nature.
The analog signals are multiplexed according to their frequency (FDM) or wavelength (WDM).

Digital Multiplexing

The term digital represents the discrete bits of information.
Hence the available data is in the form of frames or packets, which are discrete.

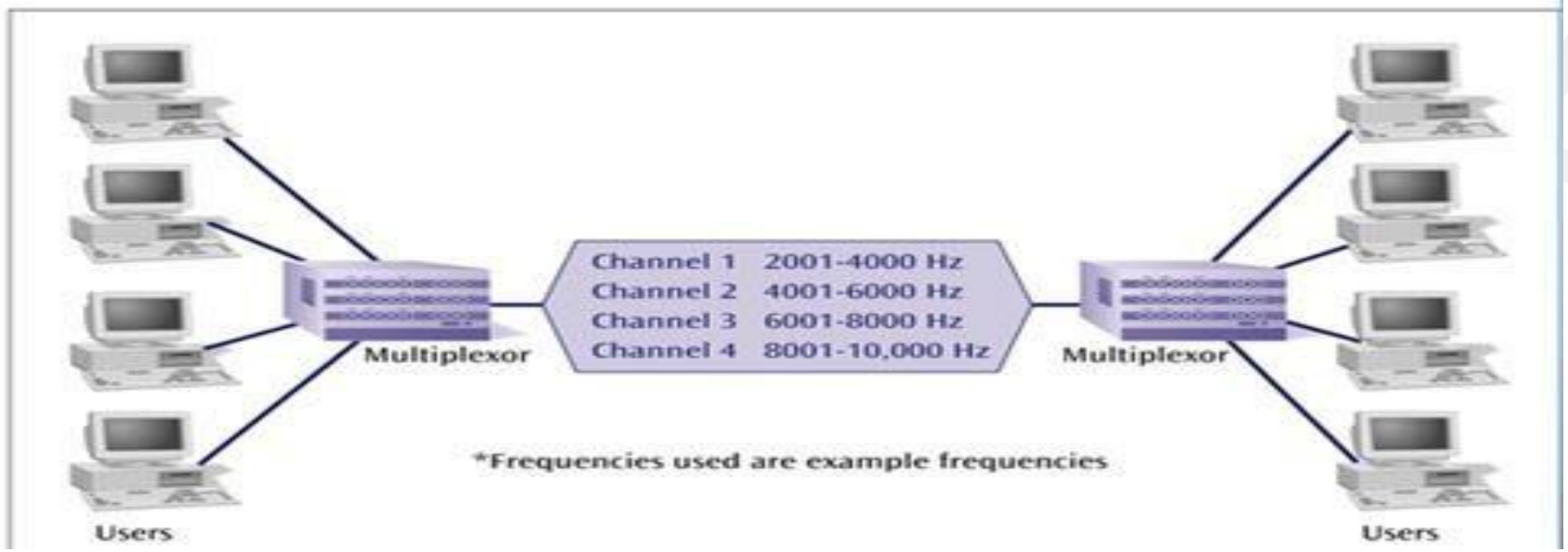
Multiplexing

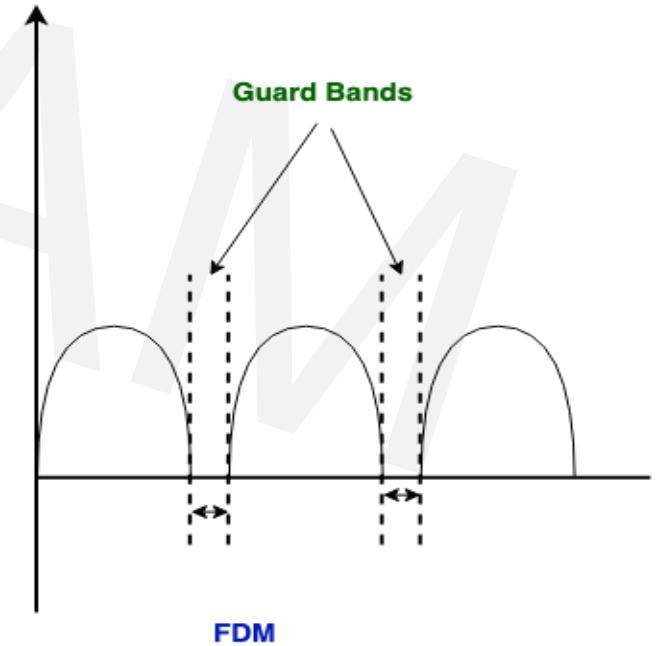
- A communication channel such as an optical fiber or coaxial cable can carry only one signal at any moment in time. **Wastage of Bandwidth**
- Multiplexing is the process of combining multiple signals into one, in such a manner that each individual signal can be retrieved at the destination.
- **Multiplexing** is used in the cases **where the signals of lower bandwidth and the transmitting media is having higher bandwidth**.
- **Methods of Multiplexing:**
  - **FDM (Frequency Division Multiplexing)**
  - **TDM (Time Division Multiplexing)**
  - **WDM(Wavelength Division Multiplexing)**

Frequency Division Multiplexing (FDM)

- Frequency division multiplexing is defined as a type of multiplexing where the bandwidth of a single physical medium is divided into a number of smaller, independent frequency channels.
- There is a lot of inter-channel cross-talk because in this type of multiplexing the bandwidth is divided into frequency channels.
- In order to prevent the inter-channel cross talk, unused strips of bandwidth must be placed between each channel. These unused strips between each channel are known as **guard bands**.

Frequency Division Multiplexing (FDM)





Frequency Division Multiplexing (FDM)

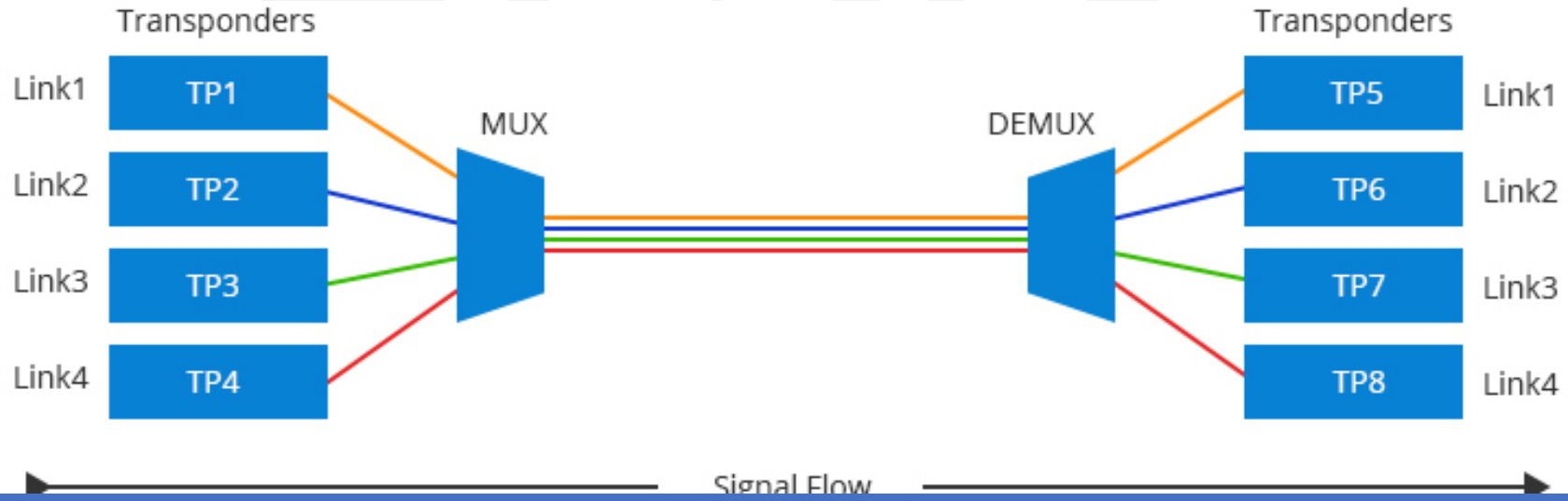
- In analog multiplexing, the most used technique is Frequency Division Multiplexing (FDM).
- This technique uses various frequencies to combine streams of data, for sending them on a communication medium, as a single signal.

- Different signals are sent on **different frequencies** at the same time
- Works with **analog signals**
- **Examples**

1. Radio broadcasting
2. Cable TV
3. Traditional telephone systems

Wavelength Division Multiplexing (WDM)

- It is a multiplexing technology used to increase the capacity of optical fiber by transmitting multiple optical signals simultaneously over a single optical fiber, each with a different wavelength.
- Each signal is carried on a different **wavelength of light**, and the resulting signals are combined onto a single optical fiber for transmission.
- At the receiving end, the signals are separated by their wavelengths, demultiplexed and routed to their respective destinations.
- It is used in telecommunications, cable TV, ISP and data centers for high-speed, long-distance data transmission.



Wavelength Division Multiplexing (WDM)

- Wavelength Division Multiplexing is an **analog technique**, in which many data streams of different wavelengths are transmitted in the light spectrum.
- If the wavelength increases, the frequency of the signal decreases.
- Used in **fiber optic** communication
- Multiple data channels sent using different **light wavelengths**
- Very high capacity

- **Examples**

1. Long-distance fiber networks
2. Internet backbone

Time Division Multiplexing (TDM)

- Time-division multiplexing is multiplexing wherein FDM, instead of sharing a portion of the bandwidth in the form of channels, in TDM, time is shared.
- Each connection occupies a portion of time in the link.
- Here all signals operate with the same frequency (bandwidth) at different times.
- Eg: television broadcast.
- In a television serial, generally, a 10 minutes' serial is followed by a 5 minutes' advertisement. The time in which the serial is being broadcasted, the total frequency is dedicated to the serial.
- Each signal gets a **time slot**
- Signals share the same channel **one after another**
- Works with **digital signals**

- There are two types of Time Division Multiplexing :

1. **Synchronous Time Division Multiplexing**
2. **Statistical (or Asynchronous) Time Division Multiplexing**

Time Division Multiplexing (TDM)

- There are two types of Time Division Multiplexing :

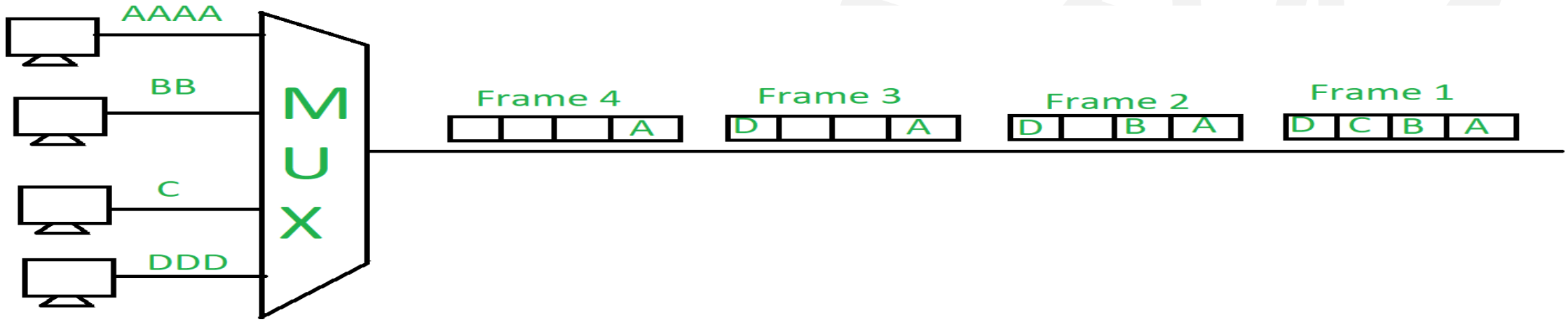
1. **Synchronous Time Division Multiplexing**
2. **Statistical (or Asynchronous) Time Division Multiplexing**

- **Synchronous TDM:** Fixed time slots, even if not used.

- **Asynchronous (Statistical) TDM**: Time slots assigned dynamically based on demand.

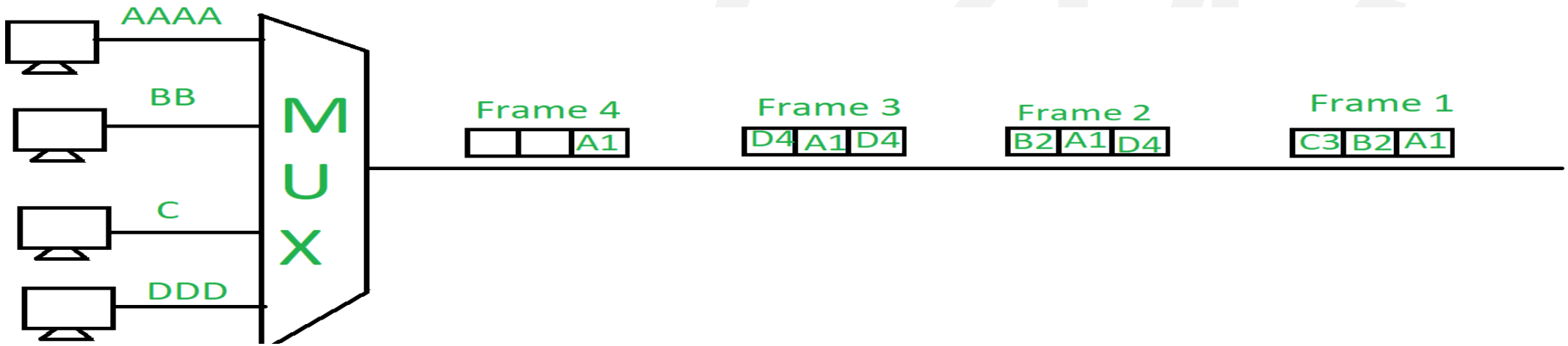
Synchronous Time Division Multiplexing

- In synchronous TDM, every device which is present in this has given the same time slot to transmit data.
- **It does not consider whether the device contains data or not.**
- The devices place their data on the link when their time slots arrive, if somehow any device does not contain data its time-slot remains empty.
- Time slots are grouped into frames.
- One frame consists of one cycle of time slots.
- Synchronous TDM is not efficient because if the input frame has no data to send, a slot remains empty in the output frame.



Asynchronous Time Division Multiplexing

- The asynchronous time division multiplexing, which is also called statistical TDM.
- It allocates the time slots dynamically to the data streams based on requirements.
- Here the time slot is assigned only when the data stream has some information to be sent, making it more flexible.
- the output frame collects data from the input frame till it is full not leaving an empty slot like in Synchronous TDM.
- **Statistical TDM is a more efficient type of time-division multiplexing as the channel capacity is fully utilized and improves the bandwidth efficiency.**
- if there are n input lines, then each slot can contain m frames, where m is less than n.



TDM VS FDM

	TDM (Time Division Multiplexing.)	FDM(Frequency Division Multiplexing)
1	TDM works with digital signals as well as analog signals.	While FDM works with only analog signals.
2	TDM has low conflict.	While it has high conflict.
3	TDM is efficient.	While it is inefficient.
4	In TDM, time sharing takes place.	While in this, frequency sharing takes place.
5	Here synchronization pulse is necessary.	Here Guard band is necessary.
6	Framing bits (Sync Pulses) are used in TDM at the start of a frame in order to enable synchronization	FDM uses Guard bands to separate the signals and prevent its overlapping

Basic systems people use to set up wired networks

An **Ethernet** system

- uses either a twisted copper-pair or coaxial-based transport system.
- The most commonly used cable for Ethernet is a **category 5 unshielded twisted pair (UTP)** cable

A **phone line**

- simply uses existing phone wiring found in most homes

Broadband systems

- provide cable Internet and use the same type of coaxial cable that gives us cable television

Wired Network Designing

Token Ring (Not used)

- Its copy write by IBM.
- It is a data link technology for local area networks (LANs) in which devices are connected in a star or ring topology.
- It was designed by only IBM PCs with 4mbps they increased upto 16mbps.

Ethernet (Used World wide /Now a days)

- It belongs to IEEE
- Its autonomous
  - 10mbps (Ethernet),
  - 100mbps (fast Ethernet)
  - 1Gbps (Gigabit Ethernet)
  - 10gbps (10 gig Ethernet)
  - 100gbps (100 gig Ethernet)
  - LRE (Long Range Ethernet)

Token Ring

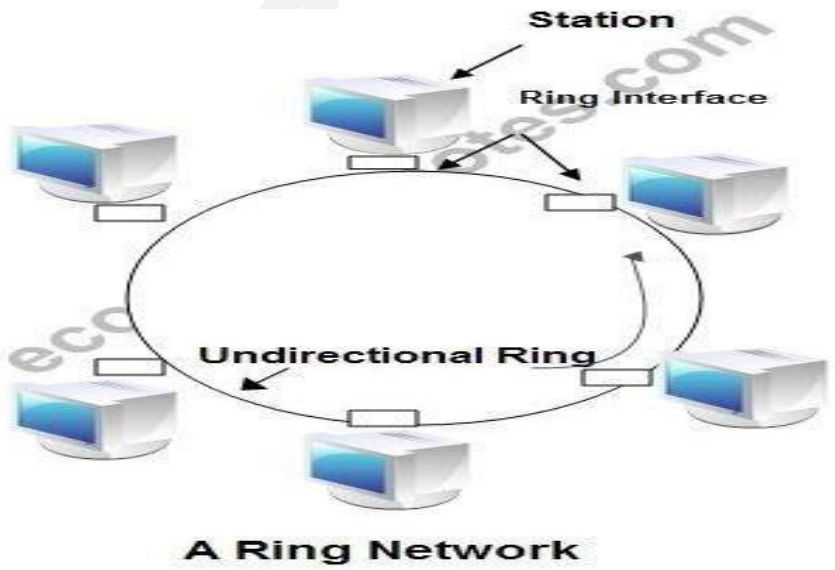
- The token ring LAN process is delineated by the following sequence of events:
  - A token continually circulates inside the toke ring LAN
  - To transmit a message, a node inserts a message and destination address inside an empty token.
  - The token is examined by each successive node.
    The destination node copies the message data and returns the token to the source with the source address and a data receipt message.
  - The source receives the returned token, verifies copied and received data and empties the token.
  - The empty token now changes to circulation mode, and the process continues.

Listen Mode

- The input bits are simply copied to output with a delay of 1-bit time.

Transmit Mode

- The connection between input and output is broken by the interface so that is can insert its own data



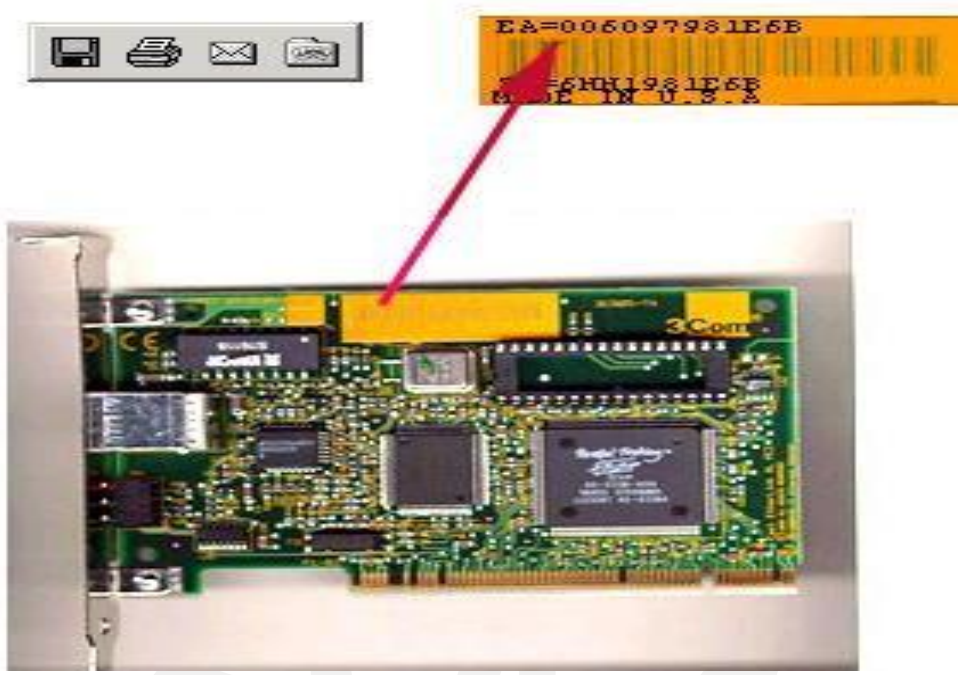
Ethernet Transfer speed 10 Mbps, 100 Mbps, or above

- Ethernet is the dominant cabling and low level data delivery technology used in Local Area Networks (LAN's).
- It was developed by Xerox corp. along with DEC and Intel.
- **Features:**

1. Ethernet Addresses are 6 bytes(48 bits) long.
2. Ethernet supports networks built with twisted pair, thin and thick coaxial and fiber optic cabling.
3. To prevent the loss of data, when two or more devices attempt to send packets at the same time, Ethernet detects collisions.

Ethernet Address/ MAC Address

Example: 47:20:1B:2E:08:EE



- First three bytes from left specify the vendor.
- the last 24 bit should be created uniquely by the company

Cisco	00-00-0C
Dell	20-47-47
Sun	08-00-20
IBM	08-00-5A
Nokia	00-40-43

Ipconfig/all : Ethernet adapter Ethernet(Physical Address)

A network interface card (NIC) / Ethernet Card is a piece of computer hardware designed to allow computers to communicate over a computer network.

Ethernet Frame Format/MAC Frame

Preamble	SFD	Destination MAC	Source MAC	Type	Data and Pad	FCS
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes	4 Bytes

Preamble	• informs the receiving system that a frame is starting and enables synchronization. In IEEE 802.3, eighth byte is start of frame (10101011)
SFD (Start Frame Delimiter)	• signifies that the Destination MAC Address field begins with the next byte.
Destination MAC	• identifies the receiving system.
Source MAC	• identifies the sending system.
Type	• defines the type of protocol inside the frame, for example IPv4 or IPv6.
Data and Pad	• contains the payload data. • Padding data is added to meet the minimum length requirement for this field (46 bytes).
FCS (Frame Check Sequence)	• contains a 32-bit Cyclic Redundancy Check (CRC) which allows detection of corrupted data.

Ethernet Frame Format/MAC Frame

- An **Ethernet Frame** (also called a **MAC Frame**) is the basic data unit used in **Ethernet LANs**. It contains addressing information, control information, and the actual data being carried over the network.

  Ethernet frames operate at a combination of **Layer 2 (Data Link Layer)** and **Layer 1 (Physical Layer)** of the OSI model.

  Eg: Ethernet Frame Format (IEEE 802.3 MAC Frame)

Network Classification

Network Classification

Classification by network geography

- According to the geographical boundaries spanned by the network itself
- This type of network classification is based on the **physical distance or area** covered by the network. It ranges from tiny personal networks to global-scale systems
- LAN, WAN, MAN ,PAN, SAN(Major two are LAN and WAN)

Classification by component roles/Network Architecture

- according to the roles that the networked computers play in the network's operation
- This classification focuses on how different devices (nodes) in a network interact and share responsibilities, especially in terms of resource management, control, and communication.
- Peer-to-peer, server-based, and client-based .

Classification by Network geography

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Classification by Network geography

1. PAN – Personal Area Network
Range: Within a few meters (typically ~10 meters)
Purpose: Connect personal devices for individual use
Technology: Bluetooth, Infrared, USB
Examples:
Connecting a smartphone to wireless earbuds
Smartwatch syncing with your phone

2. LAN – Local Area Network
Range: Within a building or campus (~100 meters)
Purpose: High-speed connection between computers and devices in a localized space
Technology: Ethernet, Wi-Fi
Examples:
Home or office Wi-Fi
School or university computer lab network

Classification by Network geography

3. CAN – Campus Area Network
Range: Multiple LANs connected within a campus or large site
Purpose: Link departments or buildings in a single organization
Technology: Ethernet, Fiber optics
Examples:
University campus with separate LANs for each faculty
Business park with interconnected office buildings

4. MAN – Metropolitan Area Network
Range: Covers a city or metro area (several kilometers)
Purpose: Connect LANs across a city for government, business, or ISP services
Technology: Fiber optics, leased lines
Examples:
City-wide cable TV or broadband networks
Municipal Wi-Fi projects

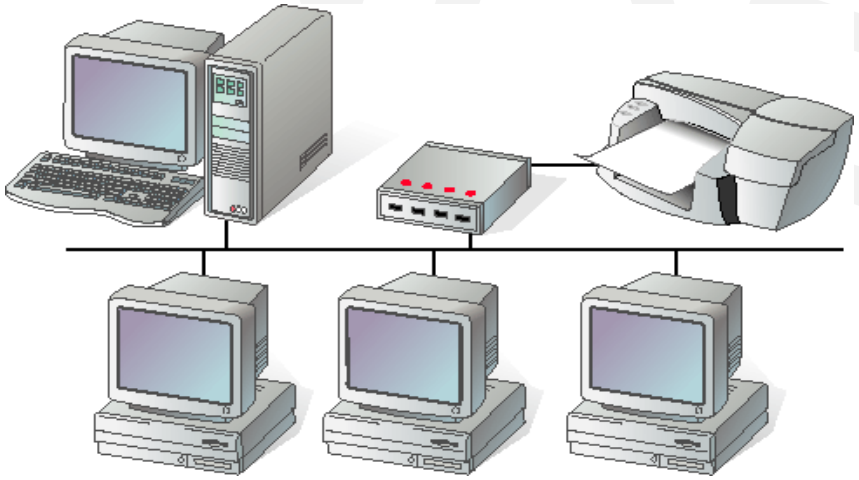
Classification by Network geography

5. WAN – Wide Area Network
Range: Covers a country, continent, or the entire globe
Purpose: Connects LANs and MANs over long distances
Technology: Satellites, leased telecom lines, undersea cables
Examples:
The Internet (largest WAN)
Bank networks spanning branches in multiple cities or countries

6. SAN – Storage Area Network
Range: Within a data center or enterprise environment (limited to building/campus scale)
Purpose: Provides high-speed, block-level access to centralized storage for servers
Technology: Fibre Channel
Examples:
Enterprise database servers accessing shared storage arrays
Virtualization platforms (e.g., VMware) using centralized SAN storage
Backup systems using SAN-connected tape libraries or disk arrays

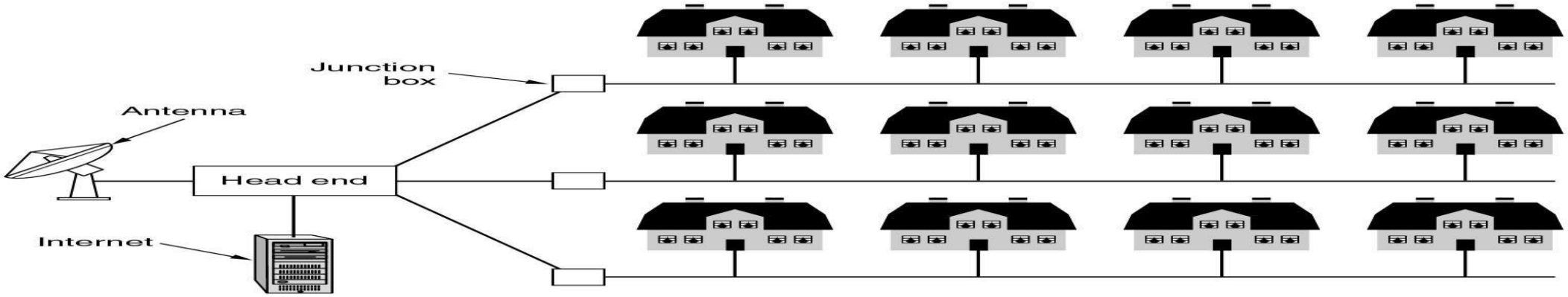
LAN (Local Area Network) : Wired Network

- Network in small geographical Area (Room, Building or a Campus)
- **Short distances (100 meters)**
- **Designed to provide local interconnectivity**
- LAN's can either be made wired or wireless. Twisted pair, coax or fiber optic cable can be used in wired LAN's
- a network that is used for communicating among computer devices, usually within an office building or home.



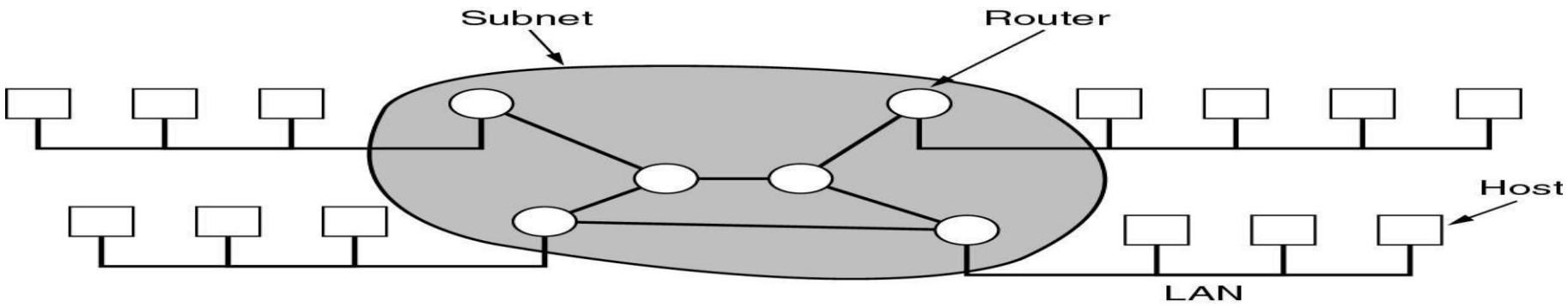
MAN

- A MAN spans the distance of a typical metropolitan city.
- The cost of installation and operation is higher.
- MANs use high-speed connections such as fiber optics to achieve higher speeds.
- Provide connectivity over areas such as a city, a campus
- More than 100m , Designed to handle data communication for multiple organizations in a city and nearby cities as well
- e.g. cable television network



WAN

- Network spread geographically (Country or across Globe)
- WANs consist of two distinct components:
  - transmission lines (copper, fiber, microwave) and switches (electronics, optics)
  - Store-and-forward or packet-switched subnet
- WANs span a larger area than a single city.
- These use long distance telecommunication networks for connection, thereby increasing the cost.
- The Internet is a good example of a WAN.
- More than 1000m long distance, Provide connectivity over large areas



Other Types of Network

CAN (Campus Area Network)
Eg. Sunbeam

PAN(Personal Area Network)
Laptop connected to Bluetooth, speaker, camera , mic etc made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building.
Private Area Network
E.g. One m/c in India (One IP) is connected to other machine in US (Other IP) are connected via Internet / VPN(Virtual Private Network)

SAN(Storage Area Network)
designed to provide high-speed connection in server-to-server applications (cluster environments)
Bank Branches and their transactions are done at centralized Bank server
That connects shared pools of storage devices to several servers, they don’t rely on a LAN or WAN.
One instance of server is created and kept at each location
Google Drive data (google.co.in/ google.com/google.jp etc)

GAN(Global Area Network)
network composed of different interconnected networks that cover an unlimited geographical area.
used to support mobile number of arbitrary number of wireless LAN (LAN), satellite coverage areas, etc

Other Types of Network

- **VPN stands for Virtual Private Network.**
- It allows you to connect your computer to a private network, creating an encrypted connection that masks your IP address to securely share data and surf the web, protecting your identity online.
- A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network.
- The encrypted connection helps ensure that sensitive data is safely transmitted.
- It prevents unauthorized people and allows the user to conduct work remotely.
- VPN technology is widely used in corporate environments.

- **EPN (Enterprise Private Network)**
- Enterprise networking involves connecting various devices and components within an organization, such as data centers, branch offices, and cloud services, to facilitate data exchange, business processes, and analysis of network activity.
- Enterprise networking typically begins with a local area network (LAN), which connects devices within a particular location or facility. These LANs may then be connected to each other using a wide area network (WAN), which enables data to be transmitted over longer distances.
- The devices within an enterprise network are connected to a router or a switch, which serves as the central hub for network traffic.

BLUETOOTH

- Bluetooth is a wireless technology that lets devices like phones, tablets, and headphones connect to each other and share information without needing cables.
- Bluetooth follows the principle of transmitting and receiving data using radio waves.
- It is a Wireless Personal Area Network (WPAN) technology and is used for data communications over smaller distances.
- The spreading method that it uses is FHSS (Frequency-hopping Spread spectrum).
- A Bluetooth network is called a piconet (A small ad hoc network of up to 8 devices (1 master, 7 slaves)).
- A group of interconnected piconets is called a scatternet.

Q. A Bluetooth network consists of _____ primary device(s) and up to ____ secondary devices.

A. one; five
B. five; three
C. two; six
D. one; seven

Ans: D

Classification by Component Roles / Network Architecture

This classification focuses on **how different devices (nodes)** in a network **interact and share responsibilities**, especially in terms of resource management, control, and communication.

1. Peer-to-Peer (P2P) Architecture-

- All devices are equal (peers) and can act as both clients and servers.
- Peers share resources directly without a centralized server.
- Decentralized ,
- Less expensive (no dedicated server needed)
- Difficult to manage and secure in large scale
- Eg: File sharing ,LAN-based multiplayer gaming, Block chain and decentralized applications

Classification by Component Roles / Network Architecture

2. Client-Server Architecture -

- A central server provides resources and services.
- Clients (devices/users) request and consume those services.
- Centralized control and management
- Easier to secure and back up
- Scalable (can add more clients easily)
- Eg: Web browsing: your browser (client) connects to a web server, Email services, file servers, database access.

Network Physical Structure

Physical Structure

Type of Connection

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

Physical Topology

- Connection of devices
- Refers to the way in which a network is laid out physically
- The geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

Types of Connection

Point-to-Point Communication

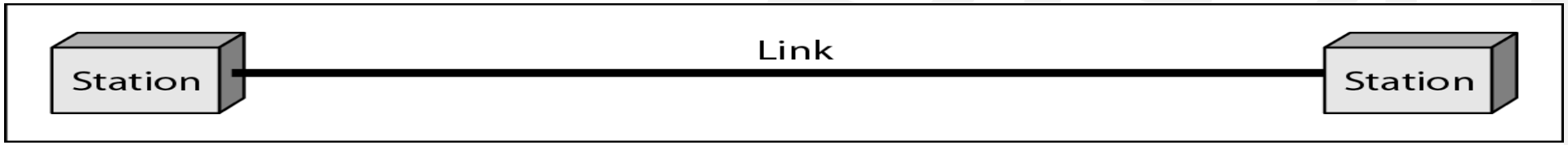
A direct connection between a single sender and a single receiver.

The communication path is dedicated between two devices.

High performance, low interference, and simpler management.

Eg: Computer connected to a modem via a cable, A leased line between two branch offices ,Bluetooth file transfer between two phones

Point-to-point: a dedicated link between two devices



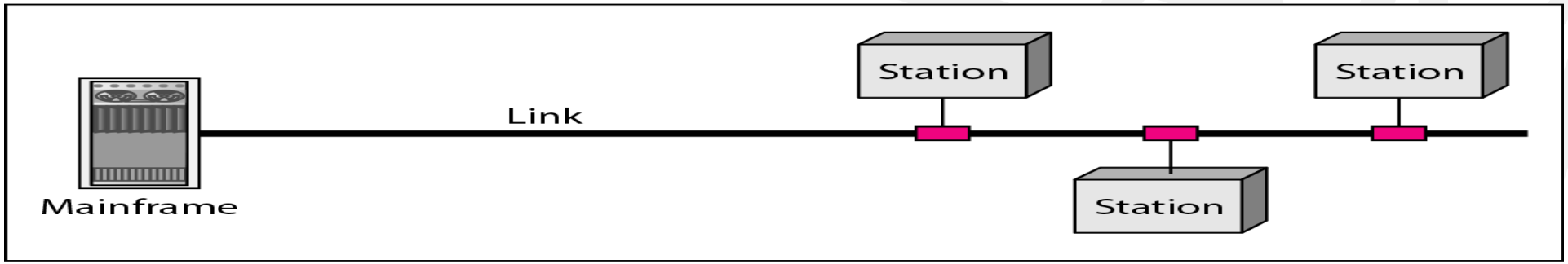
a. Point-to-point

Types of Connection

Multipoint Communication

A single sender communicates with multiple receivers over the same medium.
The communication channel is shared among multiple devices.
Efficient use of resources in broadcast or shared environments.
Eg: LAN using a hub (all devices share the same medium), Cable TV network (single signal received by multiple homes) , Wireless broadcast from an access point to several devices

Multipoint: More than two specific devices share a single link

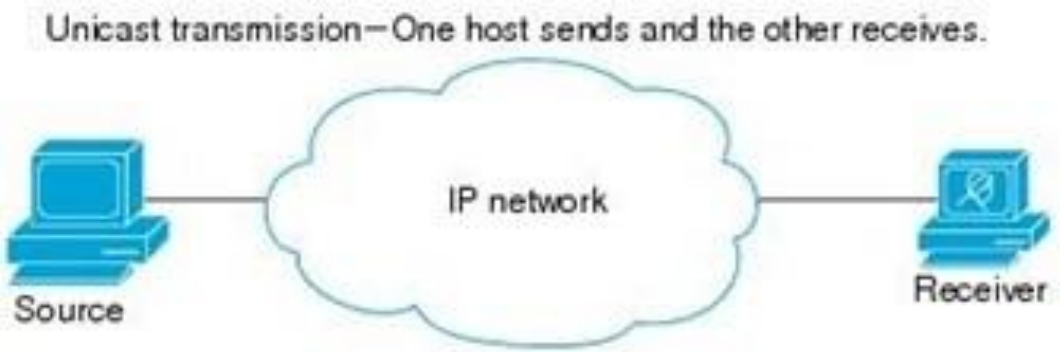


b. Multipoint

Type of transmission

Type of transmission - unicast, multicast, broadcast

1) **Unicast Transmission**

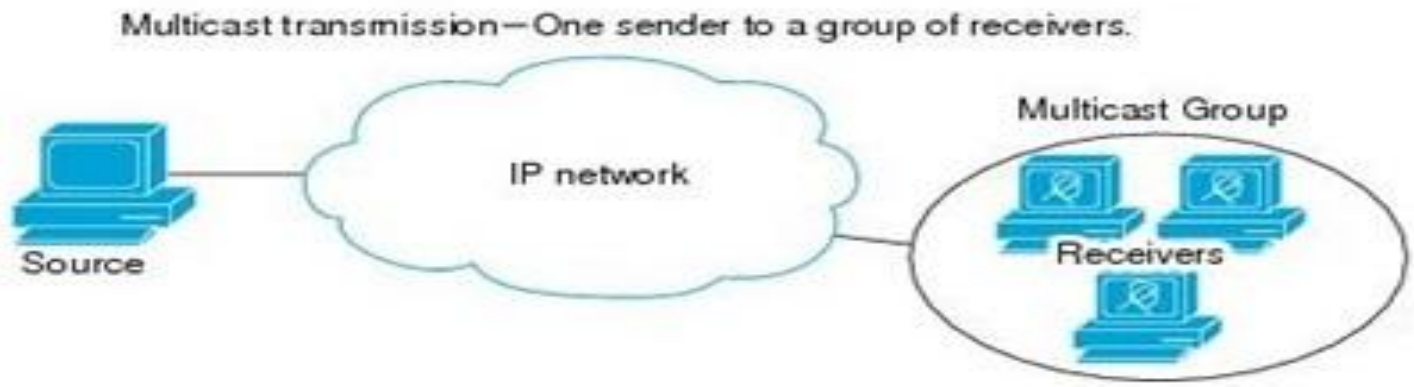


- The term unicast refers to "one to one".
- In unicast mode, transmission happens from host to host i.e. one to one. This will not incur any traffic burden on the LAN.
- The devices such as switch uses unicast mode of transmission.

Eg: Phone call between two people

Type of transmission

2)Multicast Transmission

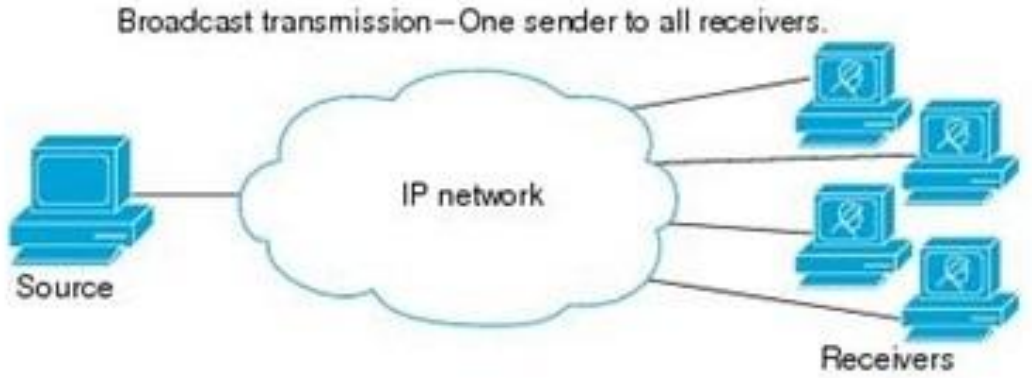


- The term **multicast** refers to "one to selected group of members".
- In multicast mode, transmission happens from one host machine to selected group of host machines.

Eg: giving a group call on WhatsApp or any application.

Type of transmission

3) Broadcast Transmission



The term **broadcast** refers to "one to all".

• In broadcast mode, transmission happens from one host to all the other hosts connected on the LAN.

The devices such as bridge uses this. The protocol such as ARP implement this, in order to know MAC address for the corresponding IP address of the host machine.

Thank You!!