Introduction

• A computer network is a set of devices (often referred to as node) connected by communication links.

• A node can be a computer, printer or any other device capable of sending or receiving data generated by other nodes on the network.

Computer Network

Networking

Networking is a process of communication between two or more remote parties, that involves the connection of computers, media and networking devices.

Network Applications

Advantages of Networking

- Easy communication
- File, data and information sharing
- Resource sharing (hardware)
- Increase storage capacity
- Reduce cost
- Save time

Network Hardware

Network Cables

Network cables are the transmission media to transfer data from one device to another. A commonly used network cable is category 5 cable with RJ – 45 connector, as shown in the image below:

Routers

A router is a connecting device that transfers data packets between different computer networks. Typically, they are used to connect a PC or an organization's LAN to a broadband internet connection. They contain RJ-45 ports so that computers and other devices can connect with them using network cables.

Repeaters, Hubs, and Switches

- Repeaters, hubs and switches connect network devices together so that they can function as a single segment.
- A repeater receives a signal and regenerates it before re-transmitting so that it can travel longer distances.
- Hub is a multiport repeater having several input/output ports, so that input at any port is available at every other port.
- A switch receives data from a port, uses packet switching to resolve the destination device and then forwards the data to the particular destination, rather than broadcasting it as a hub.


REPEATER
HUB
SWITCH

Bridges

- A bridge connects two separate Ethernet network segments. It forwards packets from the source network to the destined network.

Gateways

• A gateway connects entirely different networks that work upon different protocols. It is the entry and the exit point of a network and controls access to other networks.

Network Interface Cards

• NIC is a component of the computer to connect it to a network. Network cards are of two types: Internal network cards and external network cards.

Network Software

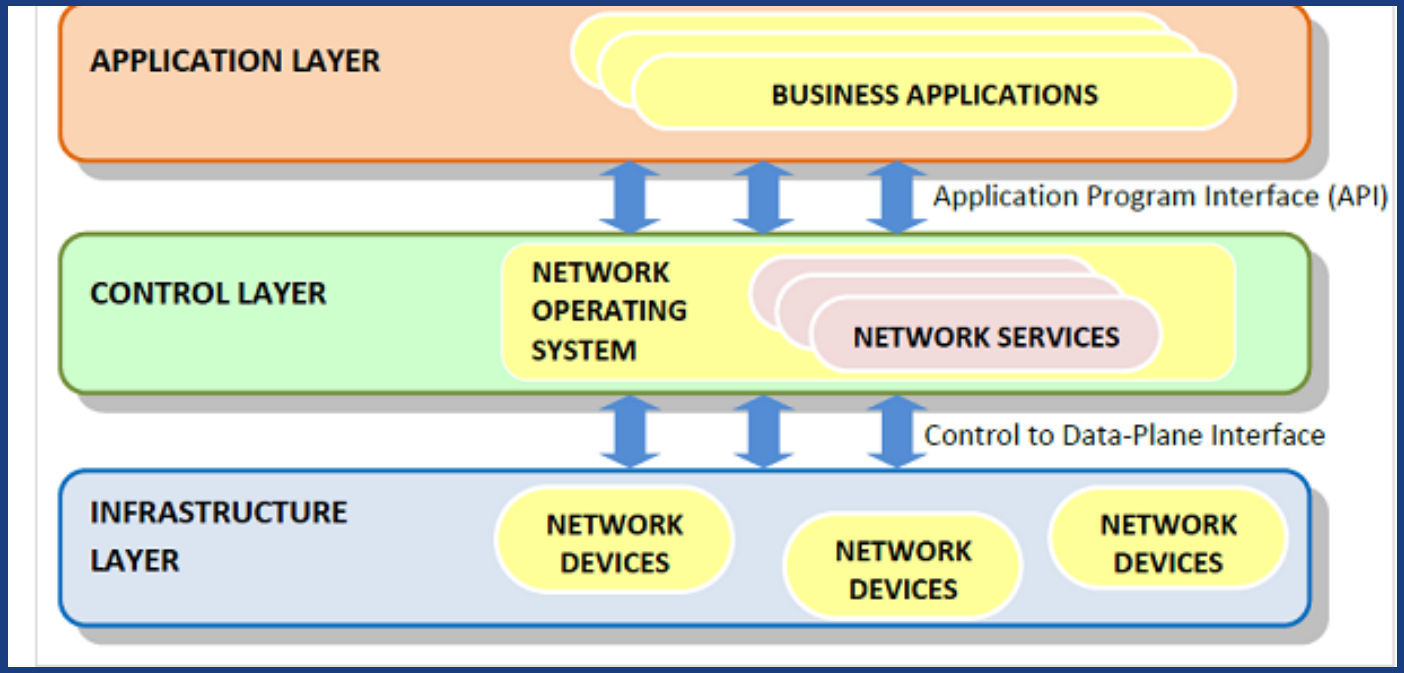
- Network software encompasses a broad range of software used for design, implementation and operation and monitoring of computer networks.
- Traditional networks were hardware based with software embedded
- With the advent of Software – Defined Networking (SDN), software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

Functions of Network Software

- Helps to set up and install computer networks
- Enables users to have access to network resources in a seamless manner
- Allows administrations to add or remove users from the network
- Helps to define locations of data storage and allows users to access that data
- Helps administrators and security system to protect the network from data breaches, unauthorized access and attacks on a network
- Enables network virtualizations

SDN Framework

- The Software Defined Networking framework has three layers as depicted in the following diagram



APPLICATION LAYER – SDN applications reside in the Application Layer. The applications convey their needs for resources and services to the control layer through APIs.

CONTROL LAYER – The Network Control Software, bundled into the Network Operating System, lies in this layer. It provides an abstract view of the underlying network infrastructure. It receives the requirements of the SDN applications and relays them to the network components.

INFRASTRUCTURE LAYER – Also called the Data Plane Layer, this layer contains the actual network components. The network devices reside in this layer that shows their network capabilities through the Control to data-Plane Interface.

Uses of Networks

Business Applications

1. Resource Sharing:

The goal is to make all programs, equipments(like printers etc), and especially data, available to anyone on the network without regard to the physical location of the resource and the user.

2. Server-Client model:

One can imagine a company's information system as consisting of one or more databases and some employees who need to access it remotely. In this model, the data is stored on powerful computers called **Servers**. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simple machines, called **Clients**, on their desks, using which they access remote data.

3. Communication Medium:

A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication.

4. e-Commerce:

A goal that is starting to become more important in businesses is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future.

Tag and Full Name	Example
B2C - Business-to-Consumer	Ordering books on-line
B2B - Business-to-Business	Car manufacturer ordering tires from supplier
C2C - Consumer-to-Consumer	Auctioning second-hand products on line
G2C - Government-to-Consumer	Government distributing tax forms electronically
P2P - Peer-to-Peer	File sharing

Home Applications

Some of the most important uses of the Internet for home users are as follows:

- **Access to remote information**
- **Person-to-person communication**
- **Interactive entertainment**
- **Electronic commerce**

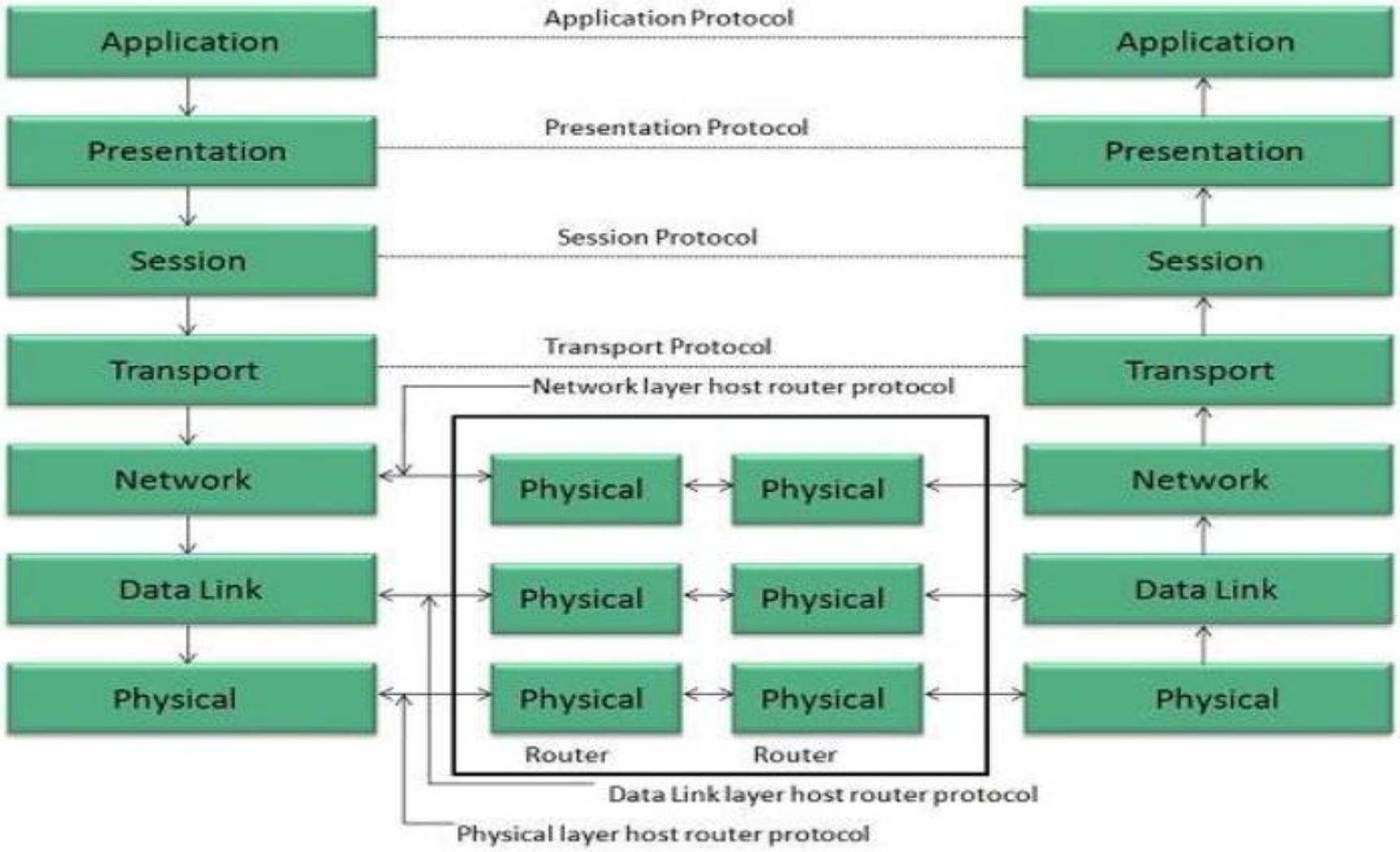
Mobile Users

• Mobile computers, such as notebook computers and Mobile phones, is one of the fastest-growing segment of the entire computer industry. Although wireless networking and mobile computing are often related, they are not identical, as the below figure shows.

Wireless	Mlobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Reference Models

OSI MODEL


Application
Presentation
Session
Transport
Network
Data Link
Physical
Application Protocol
Presentation Protocol
Session Protocol
Transport Protocol
Network layer host router protocol
Physical
Physical
Physical
Physical
Physical
Physical
Router
Router
Data Link layer host router protocol
Physical layer host router protocol
Application
Presentation
Session
Transport
Network
Data Link
Physical

Physical Layer

- Activating, maintaining and deactivating the physical connection.
- Defining voltages and data rates needed for transmission.
- Converting digital bits into electrical signal.
- Deciding whether the connection is simplex, half duplex or full duplex.

Data Link Layer

- Performs synchronization and error control for the information which is to be transmitted over the physical link.
- Enables error detection, and adds error detection bits to the data which are to be transmitted.

Network Layer

- To route the signals through various channels to the other end.
- To act as the network controller by deciding which route data should take.
- To divide the outgoing messages into packets and to assemble incoming packets into messages for higher levels.

Transport Layer

- It decides if the data transmission should take place on parallel paths or single path.
- It performs multiplexing, splitting on the data.
- It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.
- The Transport Layer guarantees transmission of data from one end to other end.

Session Layer

- Manages the messages and synchronizes conversations between two different applications.
- It controls logging on and off, user identification, billing and session management.

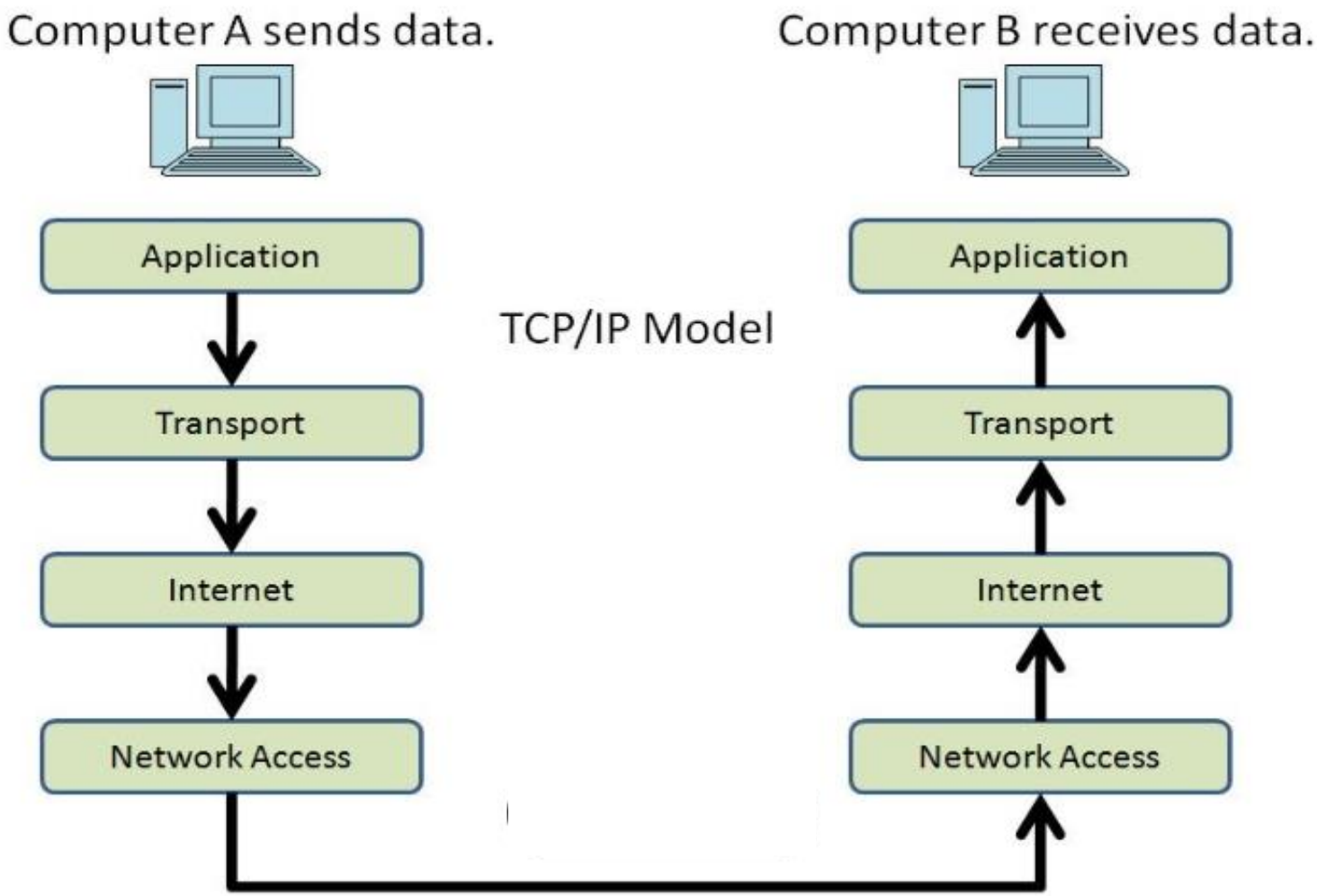
Presentation Layer

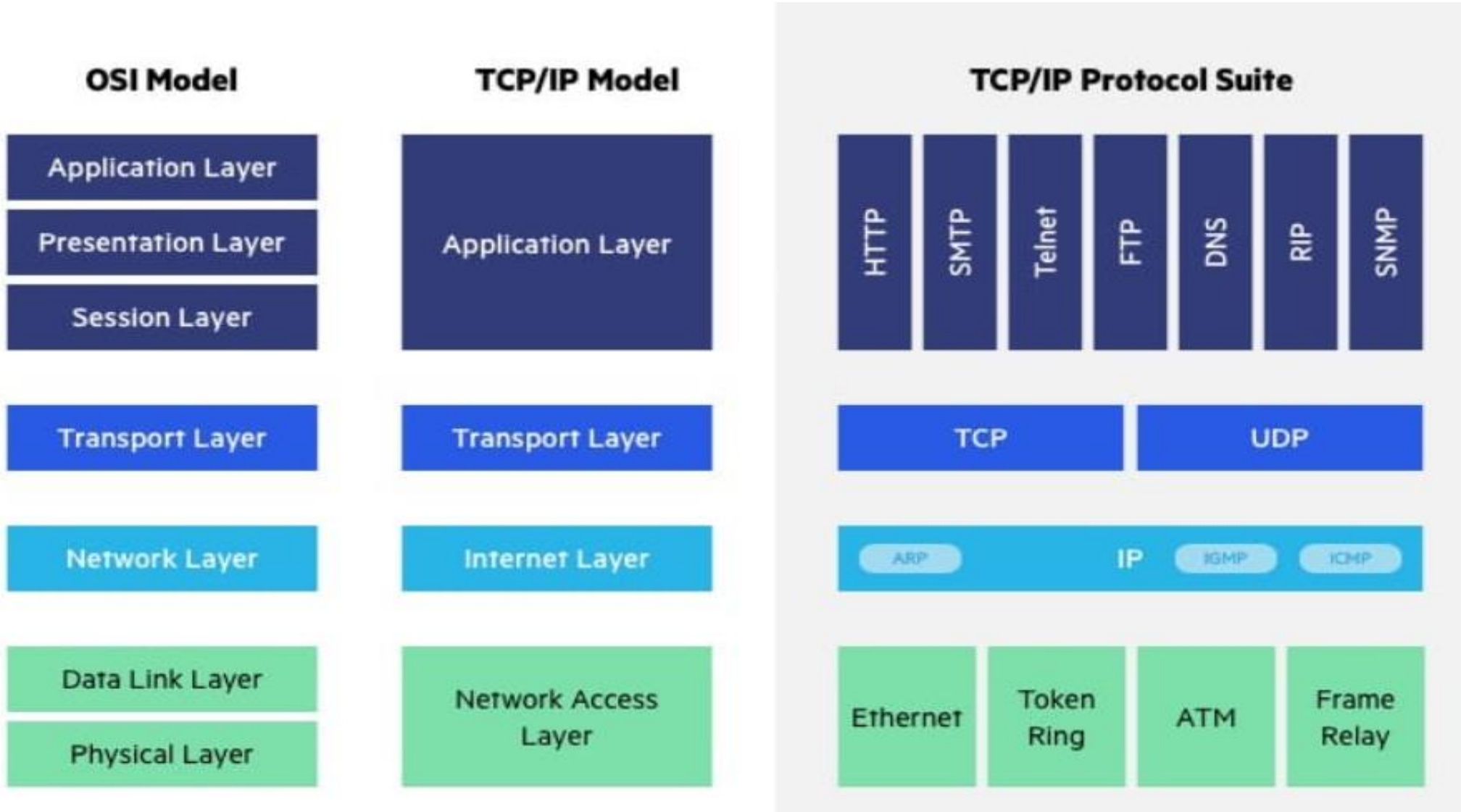
- This layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.

Application Layer

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.
- The functions such as LOGIN or password checking are also performed by the application layer.

TCP/IP MODEL


Computer A sends data.
Computer B receives data.
Application
Transport
Internet
Network Access
TCP/IP Model
Application
Transport
Internet
Network Access


OSI Model
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
TCP/IP Model
Application Layer
Transport Layer
Internet Layer
Network Access Layer
TCP/IP Protocol Suite
HTTP
SMTP
Telnet
FTP
DNS
RIP
SNMP
TCP
UDP
ARP
IP
IGMP
ICMP
Ethernet
Token Ring
ATM
Frame Relay

Network Access Layer

- Layer corresponds to the **combination of Data Link Layer and Physical Layer** of the OSI model.
- It looks out for **hardware addressing** and the **protocols** present in this layer allows for the physical **transmission** of data.

Internet Layer

1. **IP –** stands for **Internet Protocol** and it is responsible for **delivering packets** from the source host to the destination host by looking at the IP addresses in the packet headers.

IP has 2 versions:
IPv4 and **IPv6**. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.

2. **ICMP –** stands for **Internet Control Message Protocol**. It is encapsulated within IP datagrams and is responsible for providing hosts with **information about network problems.**

3. **ARP –** stands for **Address Resolution Protocol**. Its job is to **find the hardware address** of a host from a known IP address.

Transport Layer

1. **Transmission Control Protocol (TCP) –** It is provides **error-free communication** between end systems. It performs **sequencing** and **segmentation** of data. It also has **acknowledgment** feature and **controls the flow of the data** through flow control mechanism.

2. **User Datagram Protocol (UDP) –** It is the **go-to protocol** if your application does not require reliable transport as it is **very cost-effective**. Unlike TCP, which is connection-oriented protocol, UDP is **connectionless**.

Application Layer

- Responsible for **node-to-node communication** and **controls user-interface specifications**. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, SMTP..

1. HTTP and HTTPS – HTTP stands for **Hypertext transfer protocol**. It is used by the World Wide Web to manage **communications between web browsers and servers**. HTTPS stands for HTTP-Secure. It is a combination of **HTTP with SSL**(Secure Socket Layer). It is efficient in cases where the **browser need to fill out forms, sign in, authenticate and carry out bank transactions.**

2. SSH – SSH stands for **Secure Shell**. It is more preferred because of its ability to maintain the **encrypted connection**. It sets up a **secure session over a TCP/IP connection**.

3. NTP – NTP stands for **Network Time Protocol**. It is used to **synchronize the clocks** on our computer to one standard time source. It is very **useful** in situations like **bank transactions**. Assume the following situation without the presence of NTP.

Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

Switching

Switching

- Technique of transferring the information from one computer network to another network is known as **switching**.
- A switch is a small **hardware device** which is used to **join multiple computers** together with one local area network (LAN).
- Network switches operate at layer 2 (**Data link layer**) in the OSI model.
- Switches are used to **forward the packets** based on MAC addresses.
- A Switch is used to **transfer the data** only to the **device** that has been **addressed**.

- It **verifies** the destination address to route the packet appropriately.
- It is operated in **full duplex mode**.
- **Packet collision is minimum** as it directly communicates between source and destination.
- It does not broadcast the message as it works with **limited bandwidth**.

Importance of Switching Concept

- **Bandwidth:**

It is defined as the **maximum transfer rate of a cable**. It is a very critical and expensive resource. Therefore, switching techniques are used for the **effective utilization of the bandwidth** of a network.

- **Collision:**

Collision is the effect that occurs when **more than one device transmits the message over the same physical media**, and they collide with each other. To overcome this problem, **switching technology** is implemented so that **packets do not collide** with each other.

Advantages of Switching:

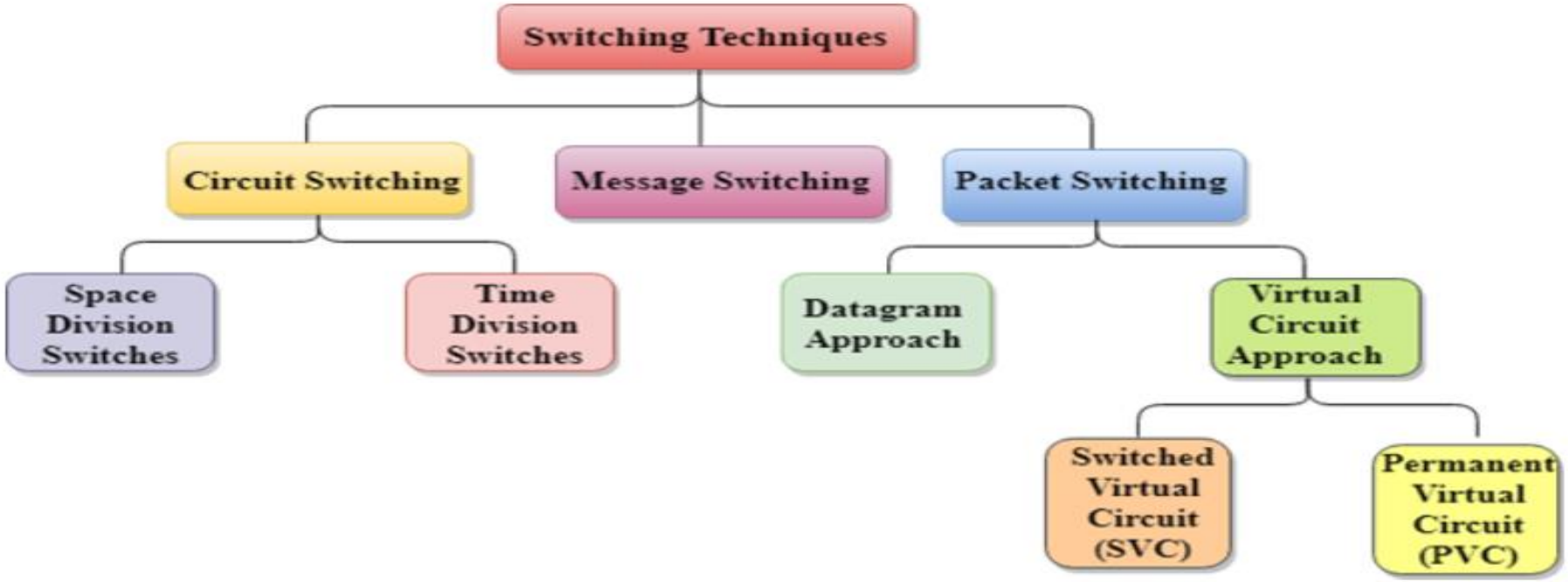
- Switch **increases the bandwidth of the network**.
- It **reduces the workload** on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by **reducing the traffic on the network**.
- There will be **less frame collision** as switch creates the collision domain for each connection.

Disadvantages of Switching:

- A Switch is more **expensive** than network bridges.
- A Switch **cannot determine** the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

Switching Techniques

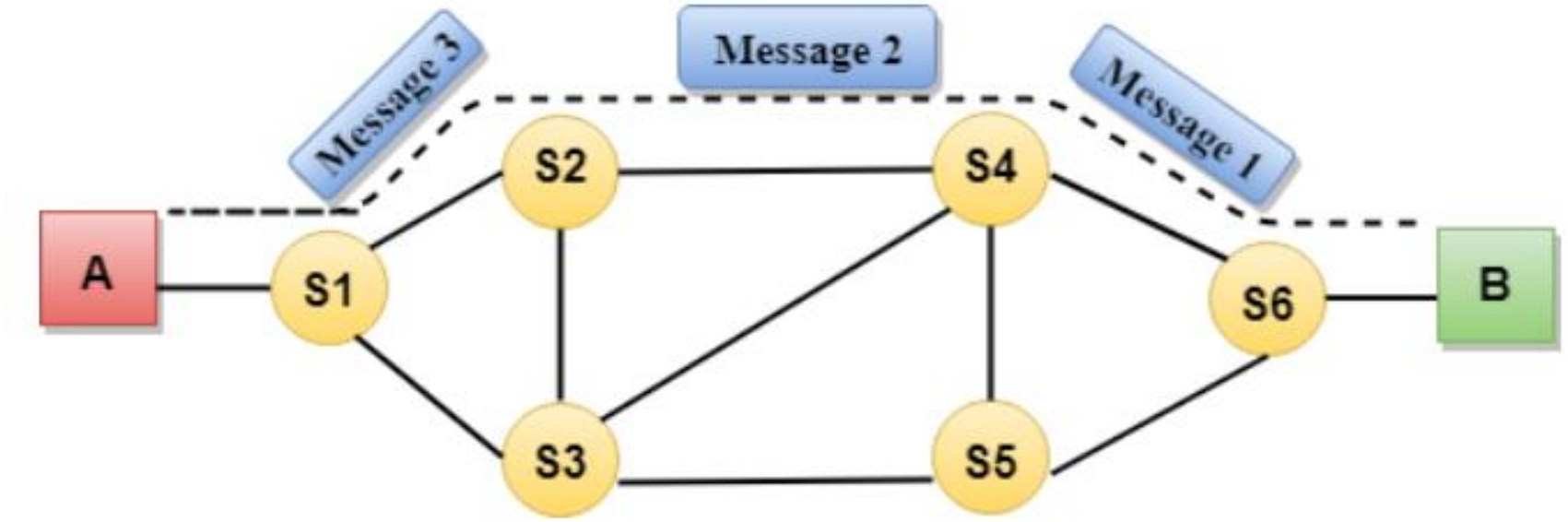
- In large networks, there can be **multiple paths** from sender to receiver. The switching technique will decide the **best route for data transmission.**



Circuit Switching

- Technique that 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**.
- Circuit switching in a network operates in a similar way as the **telephone works**.
- In circuit switching technique, when any user wants to send the data, voice, video, 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**.
- Circuit switching is used in **public telephone network**. It is used for **voice transmission**

- Circuit establishment
- Data transfer
- Circuit Disconnect



Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

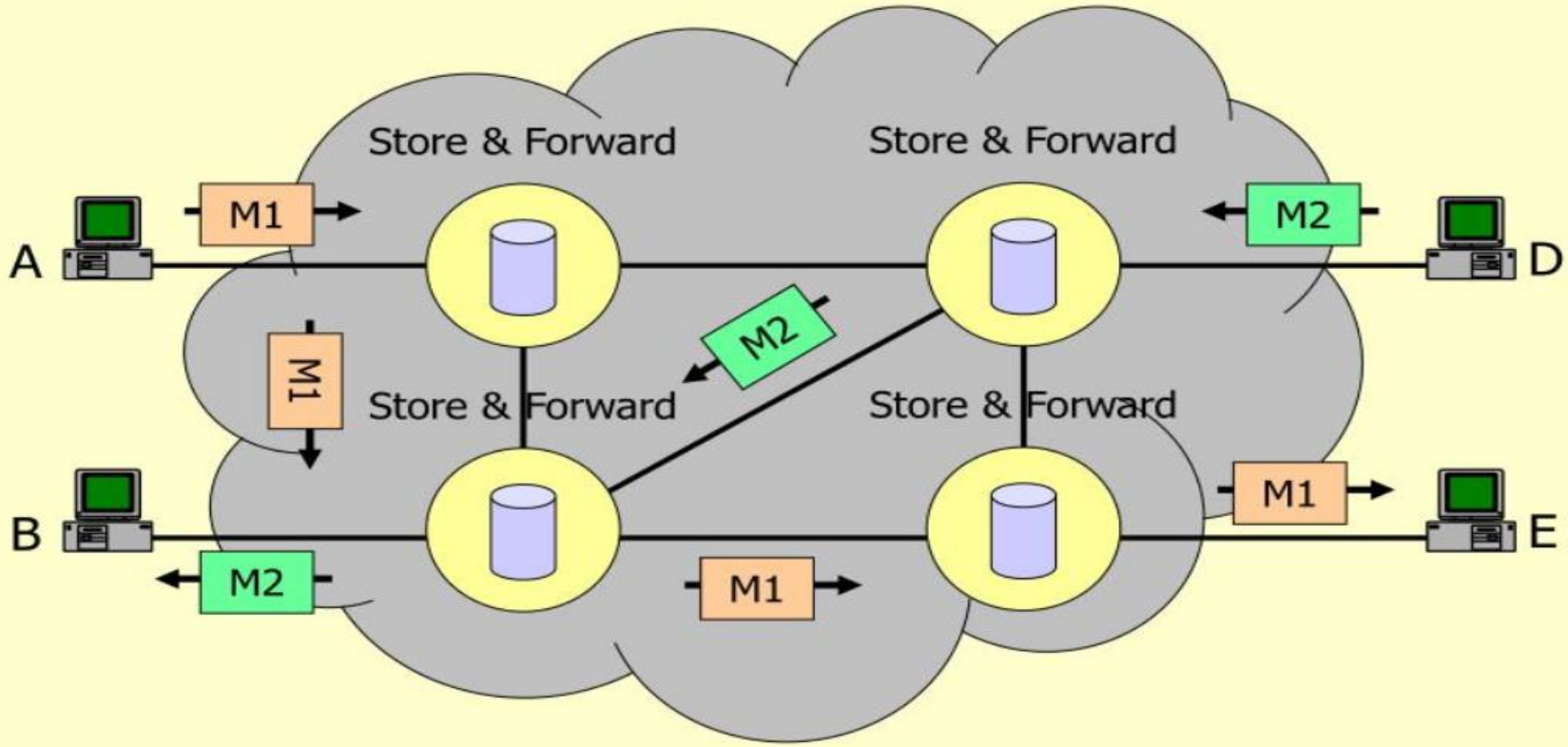
Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the **only delay occurs** in the **speed of data transmission**.
- It takes a **long time** to establish a connection **approx 10 seconds** during which no data can be transmitted.
- It is **more expensive** than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the **path is established and no data is transferred**, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore **no other data can be transferred even if the channel is free.**

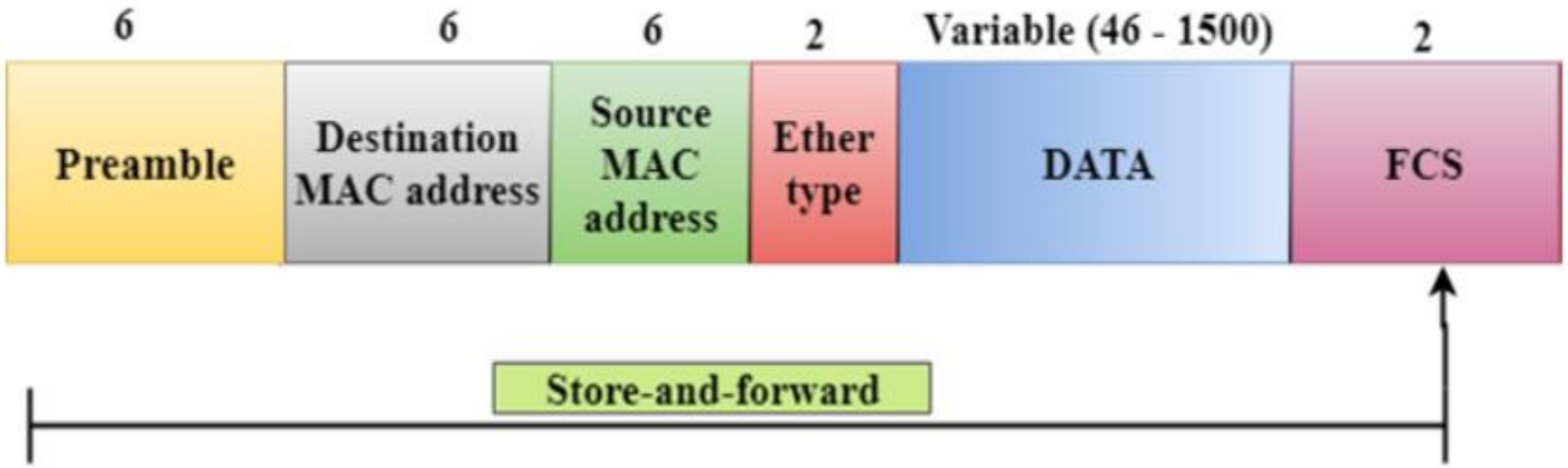
Message Switching

- Message Switching is a switching technique in which a message is **transferred as a complete unit** and routed through intermediate nodes at which it is **stored and forwarded.**
- 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

Message Switching



Store and Forward



- Store-and-forward is a technique in which the intermediate nodes store the received frame and then **check for errors** before forwarding the packets to the next node.
- If any error found, the **message is discarded** otherwise the message is forwarded to the next node.
- **CRC (Cyclic Redundancy Check) technique** is implemented that uses a number of bits to check for the errors on the received frame.
- The store-and-forward technique ensures a **high level of security** as the destination network will not be affected by the corrupted frames.
- Store-and-forward switches are highly reliable as it **does not forward the collided frames.**

Advantages Of Message Switching

- **Data channels are shared** among the communicating devices that improve the efficiency of using available bandwidth.
- **Traffic congestion can be reduced** because the message is temporarily stored in the nodes.
- **Message priority** can be used to manage the network.
- It supports the data of unlimited size.

Disadvantages Of Message Switching

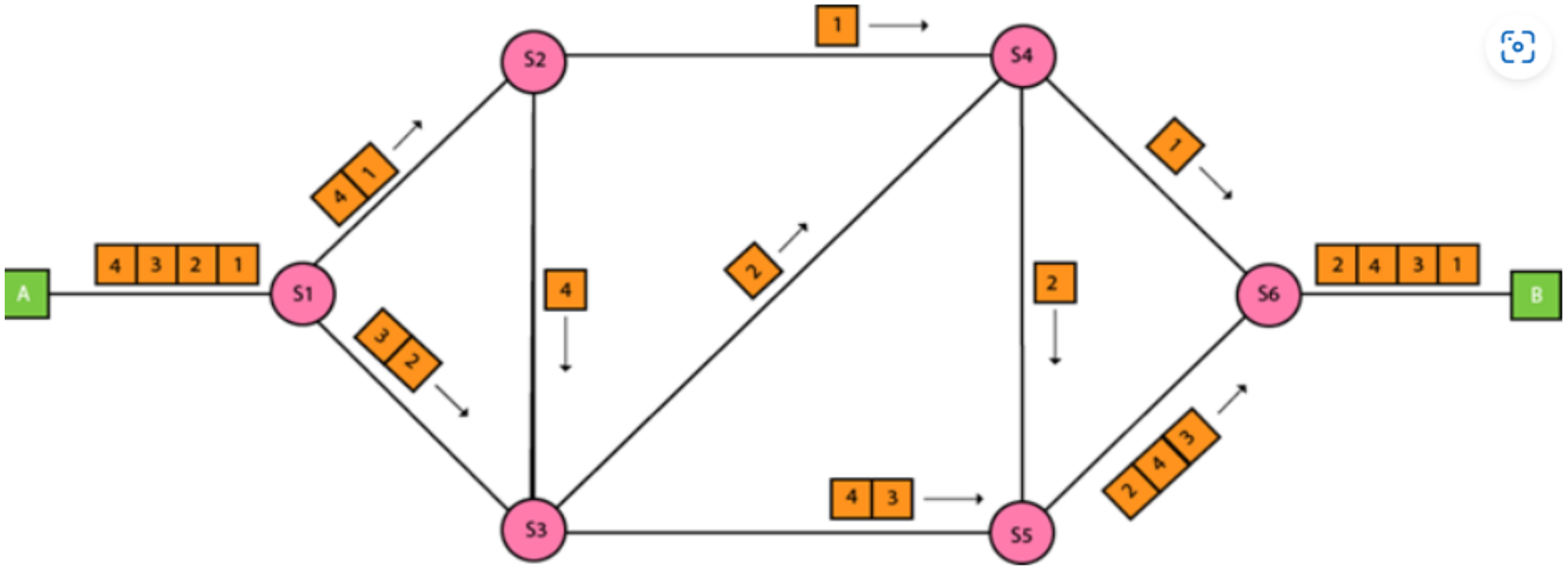
- The message switches must be **equipped with sufficient storage** to enable them to store the messages until the message is forwarded.
- The **Long delay can occur** due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the **message** is sent in one go, but it is **divided into smaller pieces**, and they are sent individually.
- The message splits into smaller pieces known as **packets** and 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



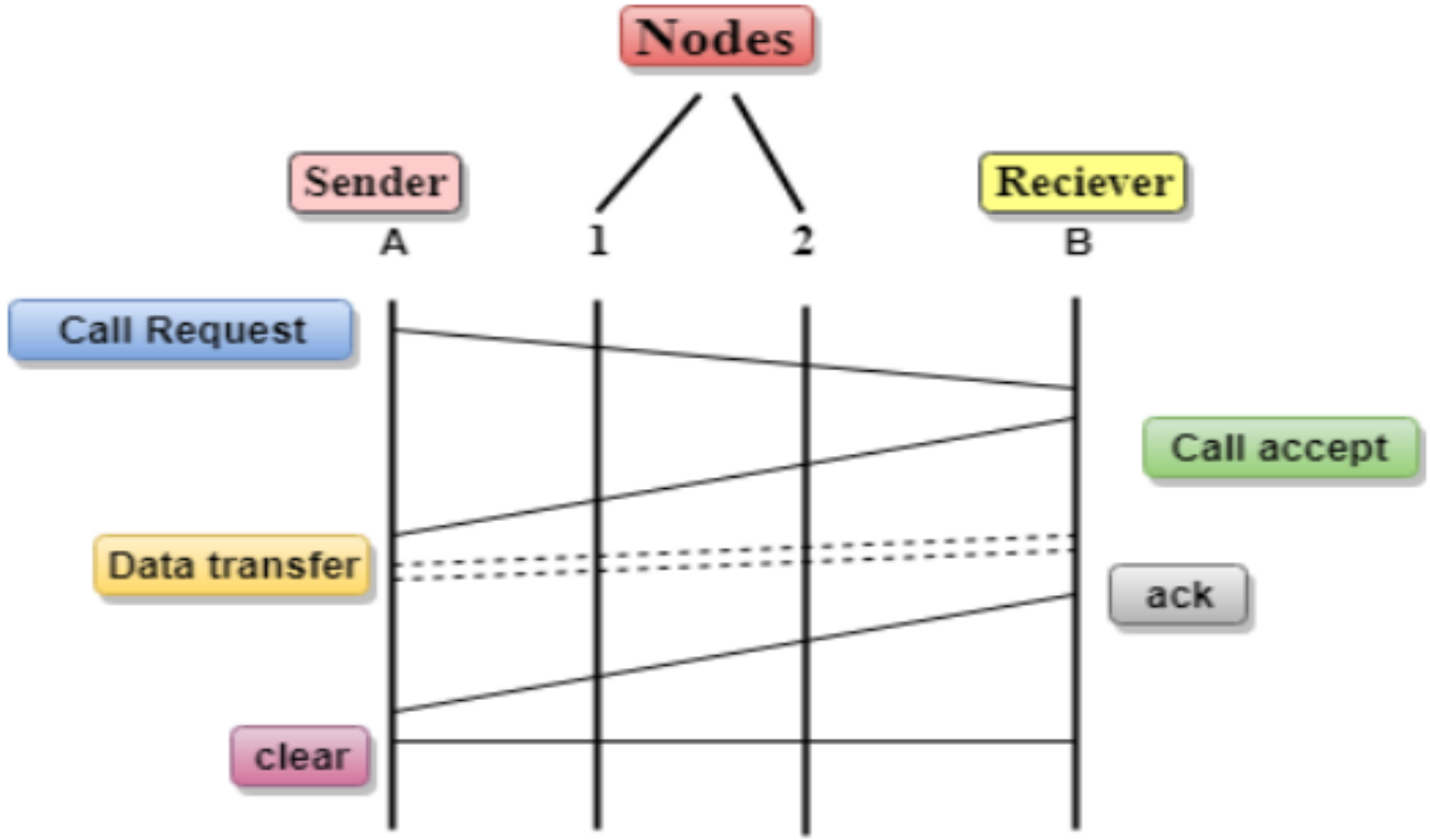
Approaches Of Packet Switching:

Datagram Packet switching:

- 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**.
- In Datagram Packet Switching technique, the **path is not fixed**.
- Intermediate nodes take the **routing decisions** to forward the packets.
- Datagram Packet Switching is also known as **connectionless switching**.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as **connection-oriented switching.**
- In the case of Virtual circuit switching, 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.


Nodes
Sender
A
1
2
Reciever
B
Call Request
Call accept
Data transfer
ack
clear

Advantages Of Packet Switching

- **Cost-effective:**

In packet switching technique, switching devices do **not** require **massive secondary storage to store the packets**.

- **Reliable:**

If any node is busy, then the packets can be **rerouted**. This ensures that the Packet Switching technique provides reliable communication.

- **Efficient:**

It does **not require any established path prior to the transmission**, and many users can **use the same communication channel** simultaneously, hence makes use of available bandwidth very efficiently.

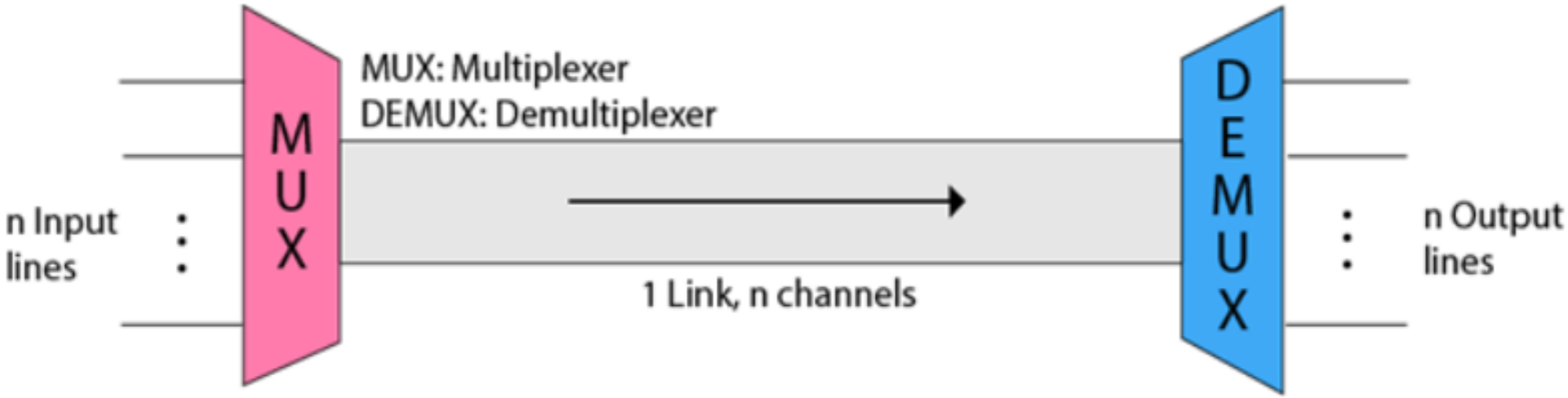
Disadvantages Of Packet Switching:

- Packet Switching technique **cannot be implemented** in those applications that **require low delay and high-quality services**.
- The protocols used in a packet switching technique are very complex and requires **high implementation cost**.
- If the network is overloaded or corrupted, then it requires **retransmission of lost packets**. It can also lead to the loss of critical information if errors are not recovered.

Multiplexing

- Multiplexing is a technique used to combine and send the multiple data streams over a single medium.
- Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line.
- Demultiplexer (DEMUX) separates a signal into its component signals (one input and n outputs).
- For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.

Concept of Multiplexing



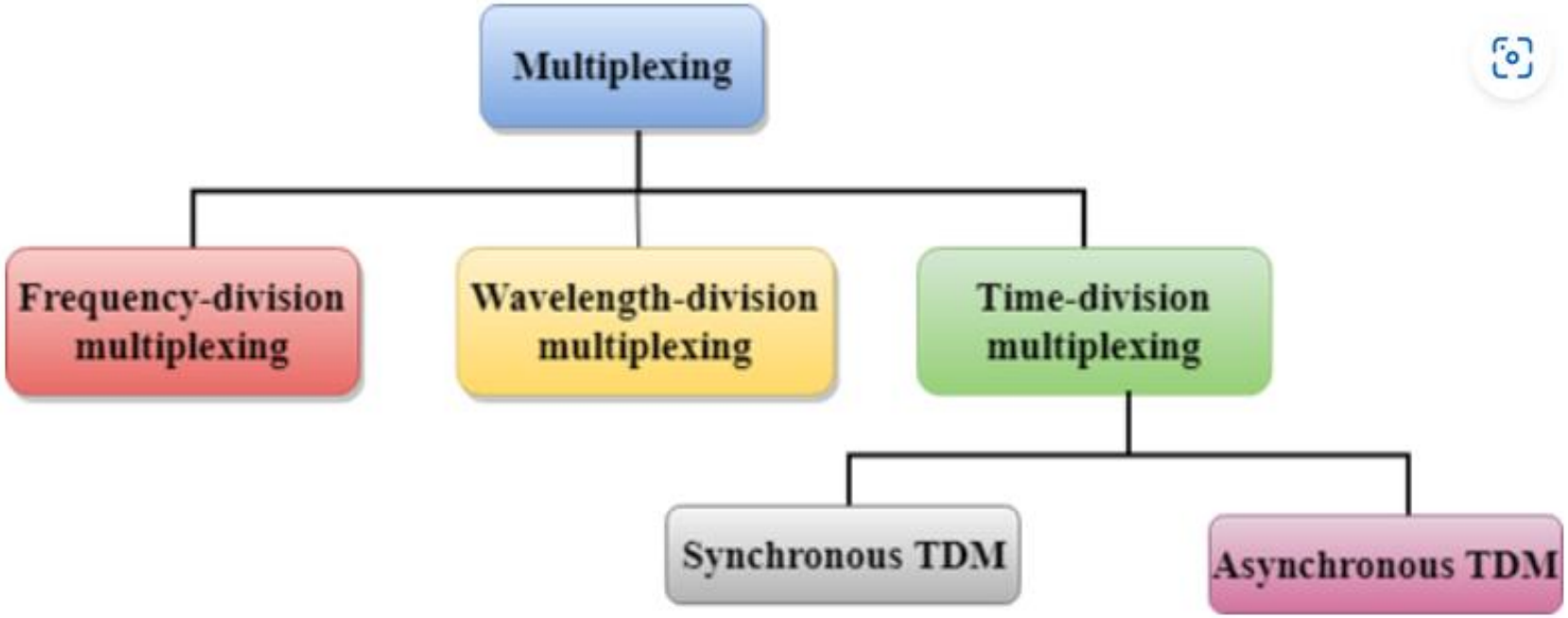
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.

- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

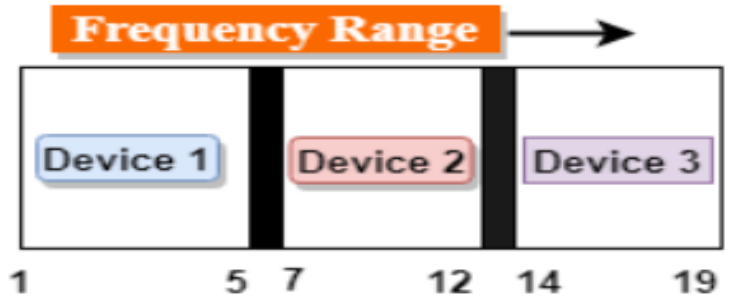
- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

Multiplexing Techniques

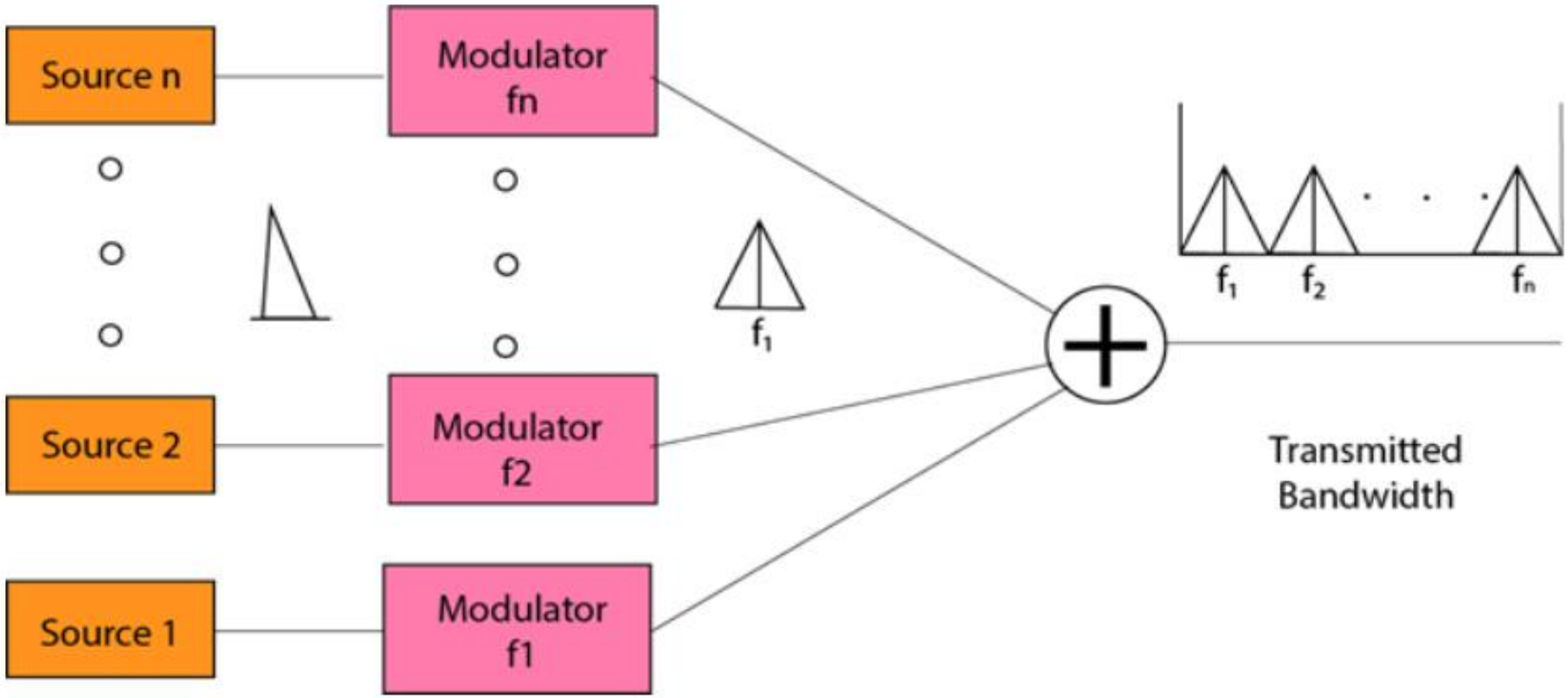


Frequency-division Multiplexing (FDM)

- It is an analog technique.
- **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.
- **FDM** is mainly used in radio broadcasts and TV networks.


Source n
Source 2
Source 1
Modulator fn
Modulator f2
Modulator f1
f1
f1
f2
fn
Transmitted Bandwidth

Advantages Of FDM:

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

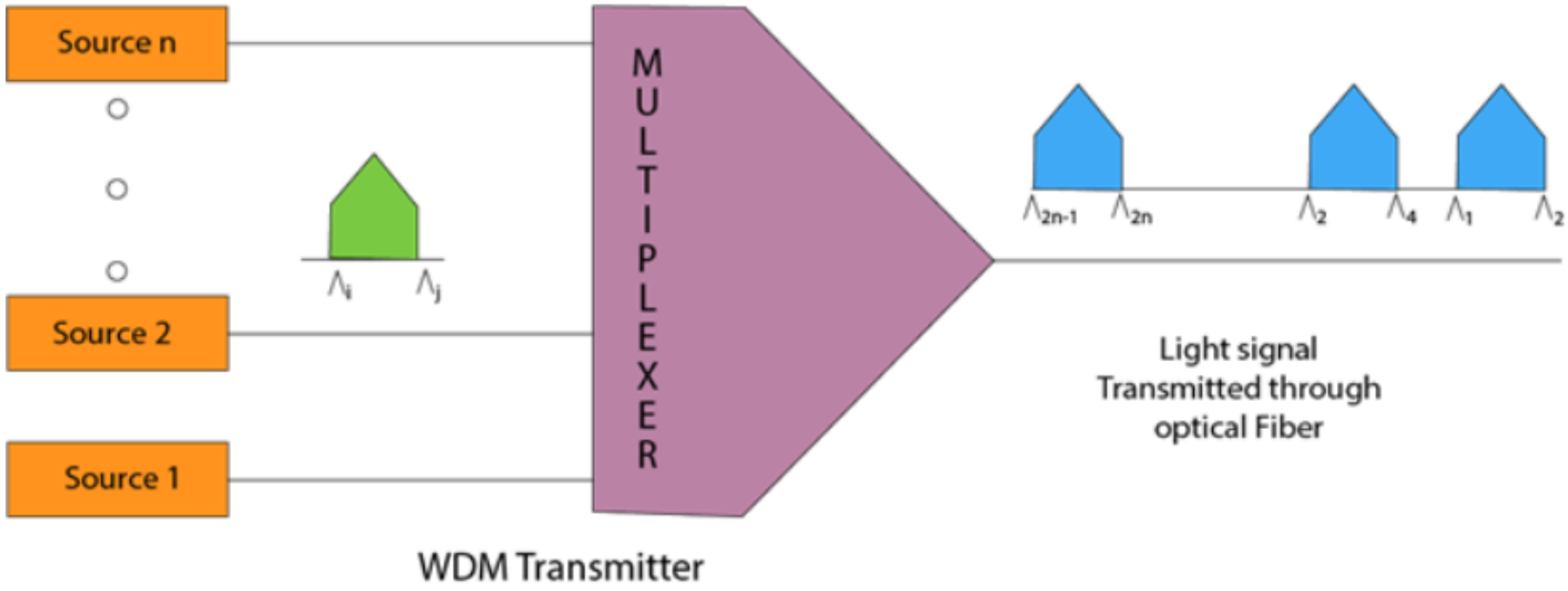
Disadvantages Of FDM:

- FDM technique is used only when low-speed channels are required.
- It suffers the problem of crosstalk.
- A Large number of modulators are required.
- It requires a high bandwidth channel.

Applications Of FDM:

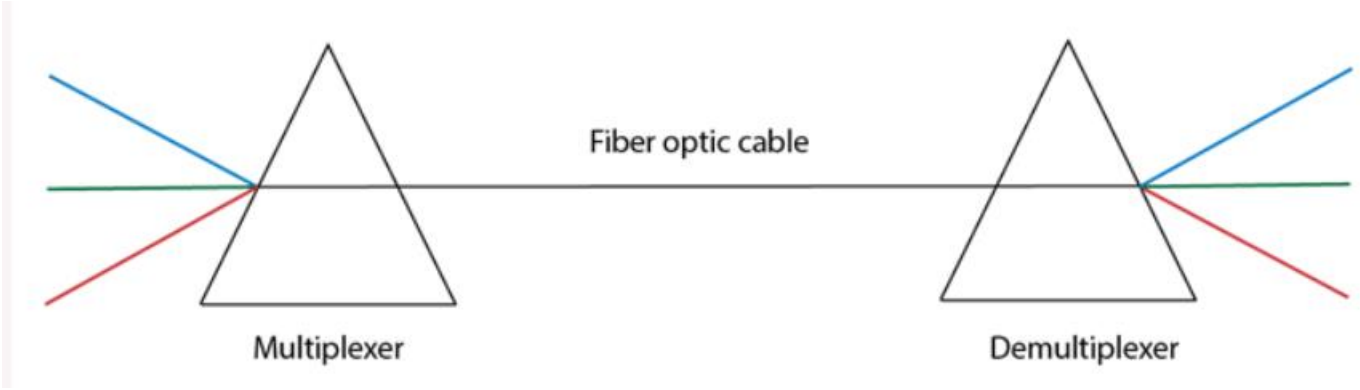
- FDM is commonly used in TV networks.
- It is used in FM and AM broadcasting.
- Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



- Wavelength Division Multiplexing is same as FDM except that the **optical signals** are transmitted through the **fibre optic cable**.
- WDM is used on fibre optics to **increase the capacity** of a single fibre.
- It is used to utilize the **high data rate** capability of fibre optic cable.
- It is an analog multiplexing technique.
- **Optical signals** from different source are **combined to form a wider band of light** with the help of multiplexer.
- At the receiving end, **demultiplexer separates** the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a **prism**.

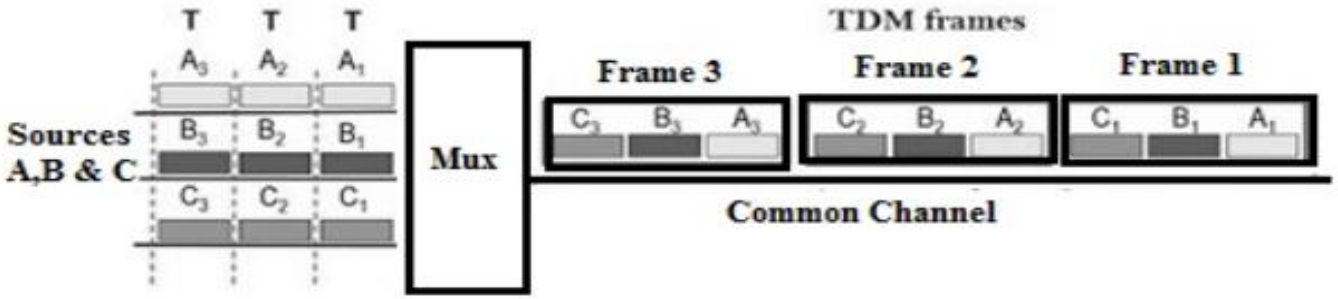
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.



Time Division Multiplexing

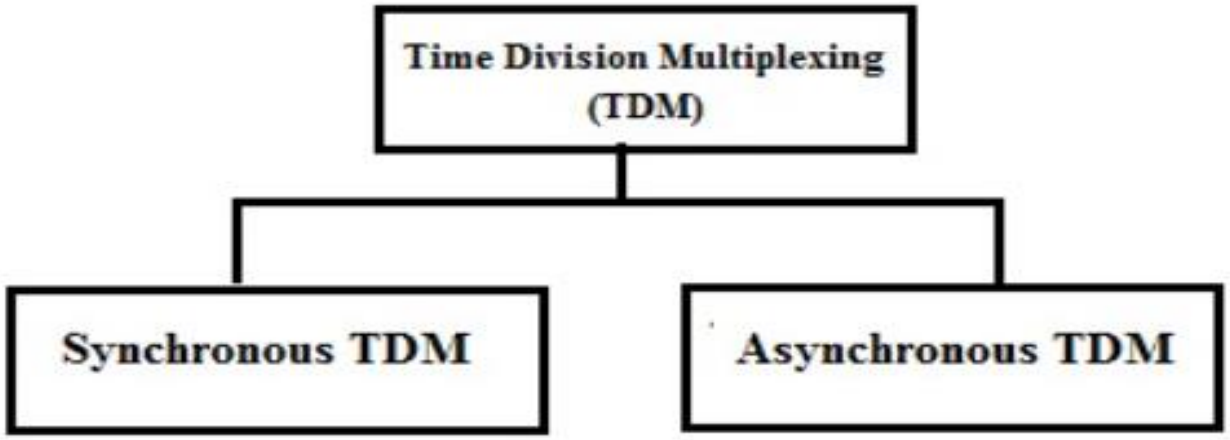
- It is a **digital** technique.
- In **FDM Technique**, all signals operate at the **same time with different frequency**, but in case of **TDM technique**, all signals operate at the **same frequency with different time**.
- In **TDM**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a **Time slot** at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.

- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the **data is transmitted one-by-one**.
- In TDM, the signal is **transmitted** in the form of **frames**. Frames contain a **cycle of time slots** in which **each frame contains one or more slots** dedicated to each user.



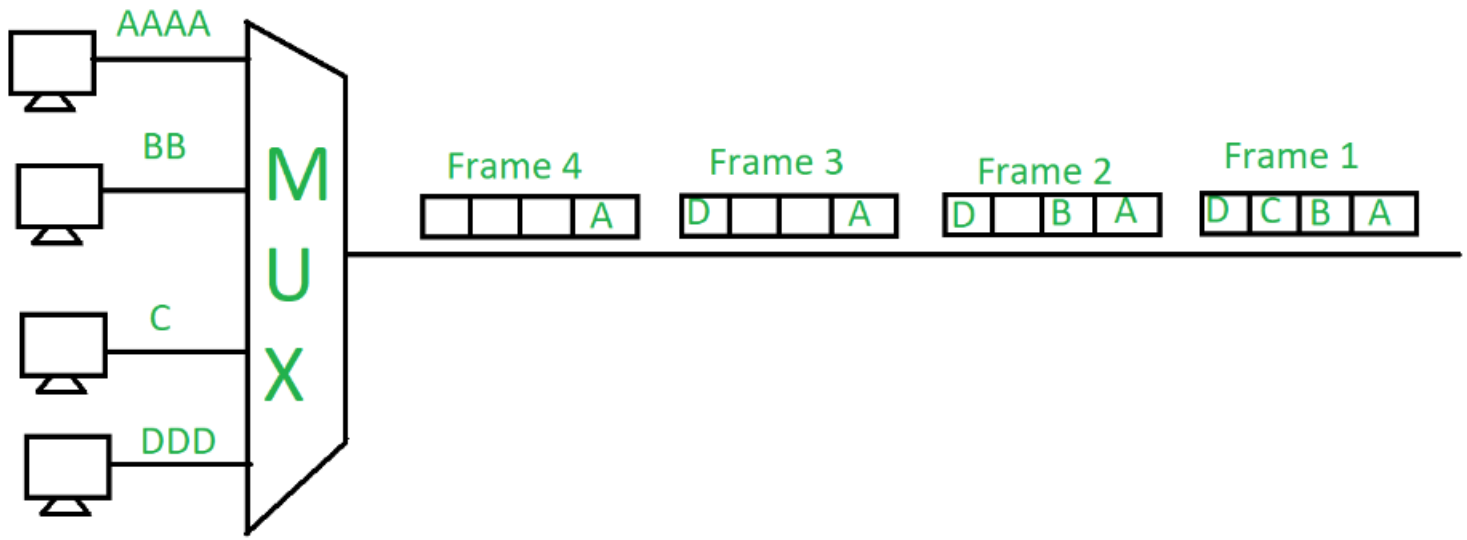
Time Division Multiplexing Working

Types of TDM


Time Division Multiplexing (TDM)
Synchronous TDM
Asynchronous TDM

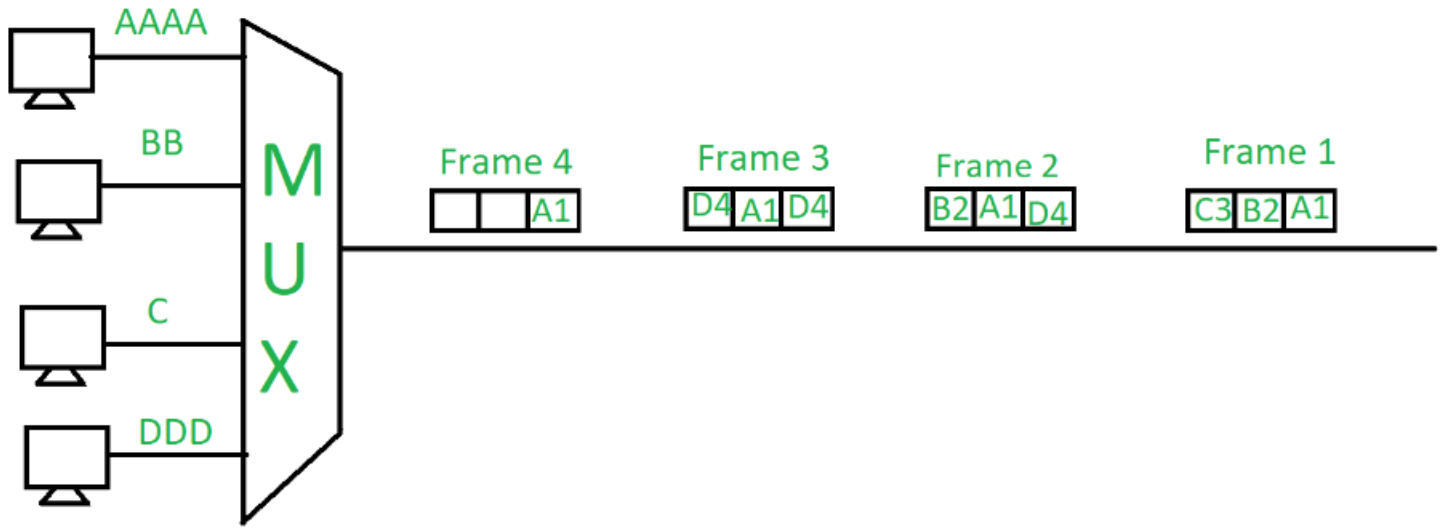
Synchronous TDM

- The time slots are **pre-assigned** and **fixed**.
- This slot is even given if the source is not ready with data at this time. In this case, the slot is transmitted empty.
- It is used for multiplexing digitized voice streams.

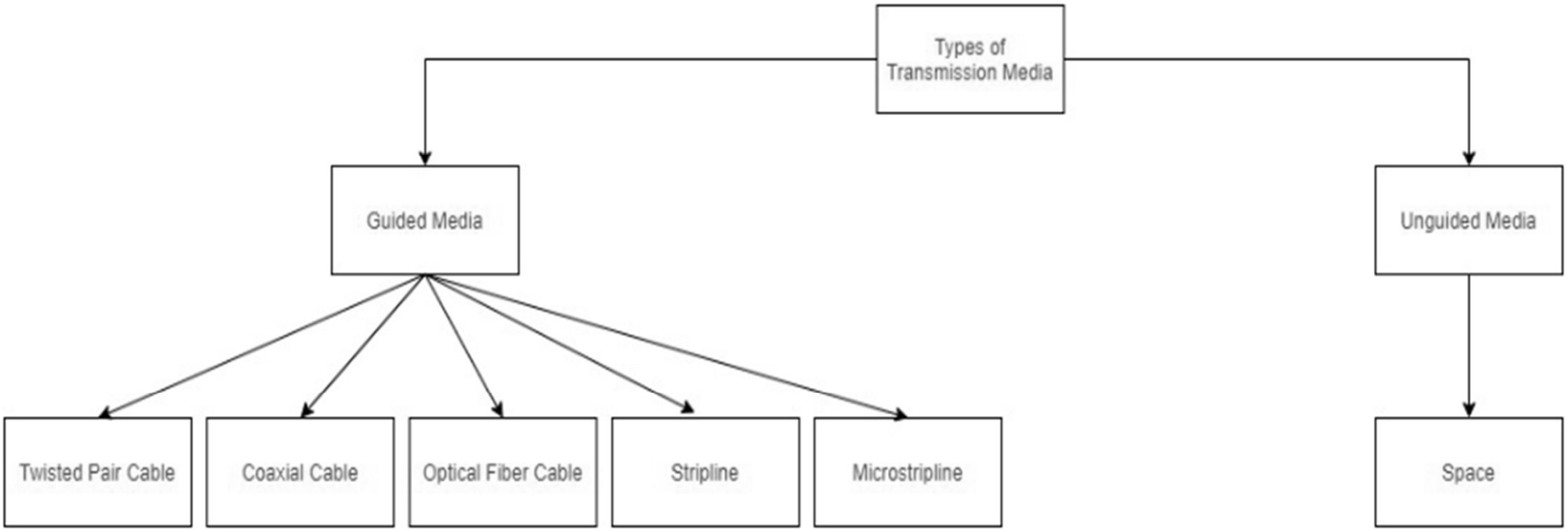


Asynchronous (or statistical) TDM:

- The slots are allocated **dynamically** depending on the speed of the source or their ready state.
- It dynamically allocates the time slots according to different input channels' needs, thus saving the channel capacity.



Transmission Media


Types of Transmission Media
Guided Media
Unguided Media
Twisted Pair Cable
Coaxial Cable
Optical Fiber Cable
Stripline
Microstripline
Space

Guided Media

- It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable

- **Unshielded Twisted Pair**
- **Shielded Twisted Pair**

(ii) Coaxial Cable

(iii) Optical Fibre Cable

Twisted Pair Cable

Unshielded Twisted Pair (UTP):

- UTP consists of two insulated copper wires twisted around one another.
- This type of cable has the ability to block interference and does not depend on a physical shield for this purpose.
- It is used for telephonic applications.

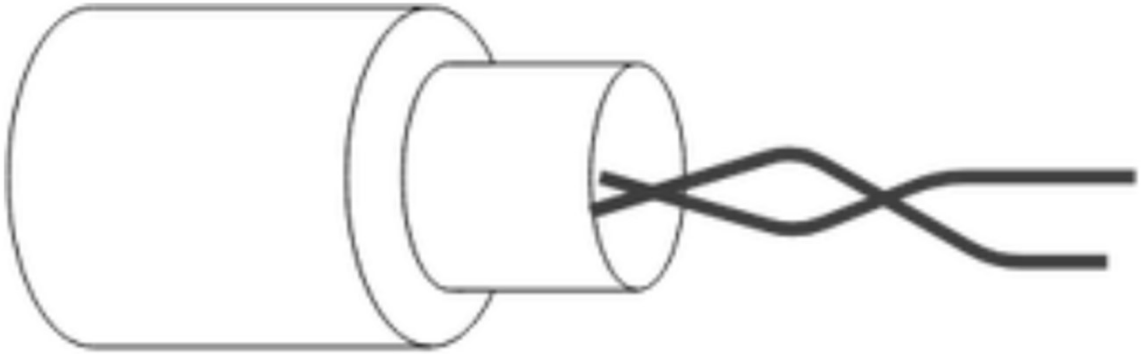
Unshielded Twisted Pair

Advantages:

- Least expensive
- Easy to install
- High-speed capacity
- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

- **Shielded Twisted Pair (STP):**

This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Shielded Twisted Pair

Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster
- Comparatively difficult to install and manufacture
- More expensive
- Bulky

Coaxial Cable

- It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover.

- The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges).

- Cable TVs and analog television networks widely use Coaxial cables.

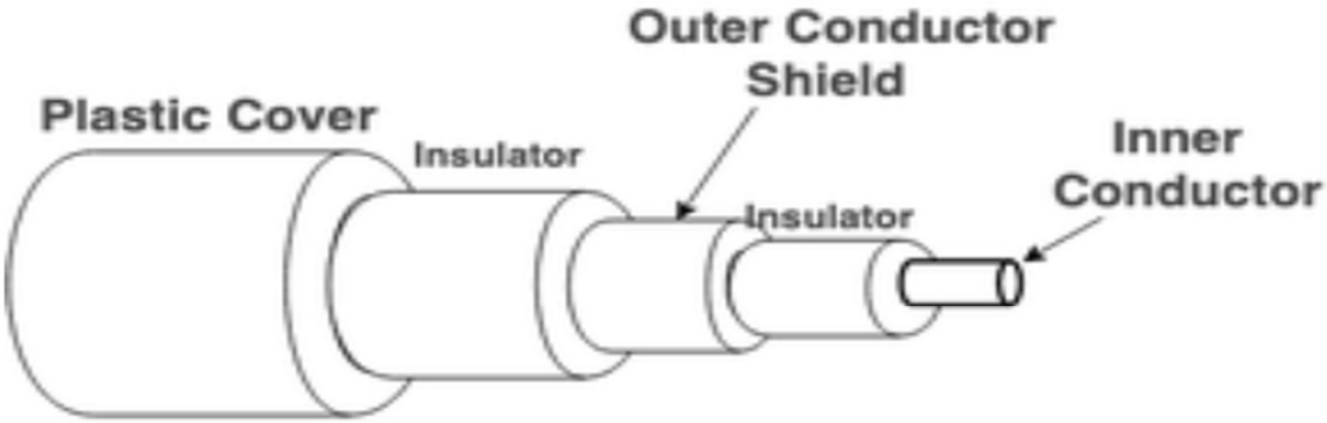


Figure of Coaxial Cable

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

Optical Fiber Cable

- It uses the concept of refraction of light through a core made up of glass or plastic.
- The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.
- The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

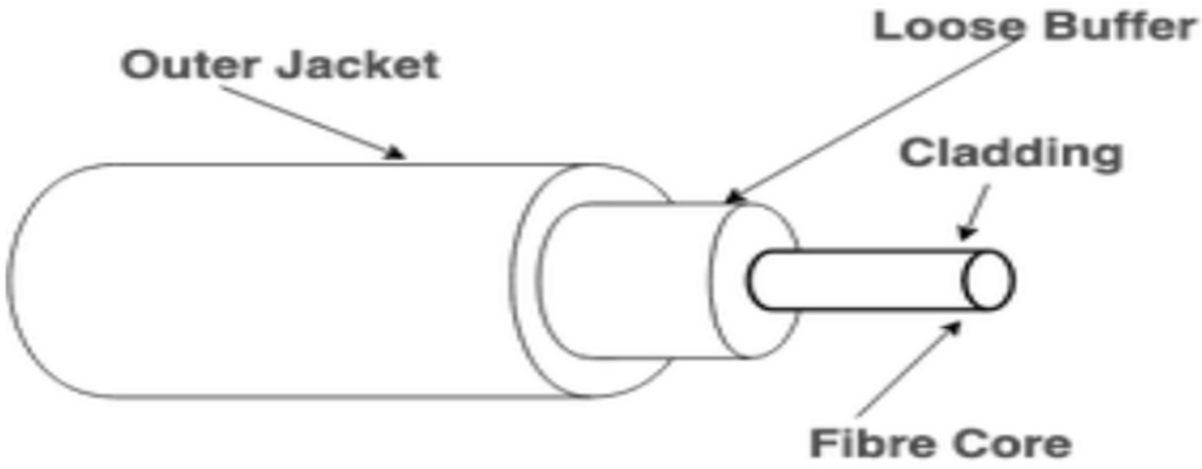


Figure of Optical Fibre Cable

Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

Unguided Media:

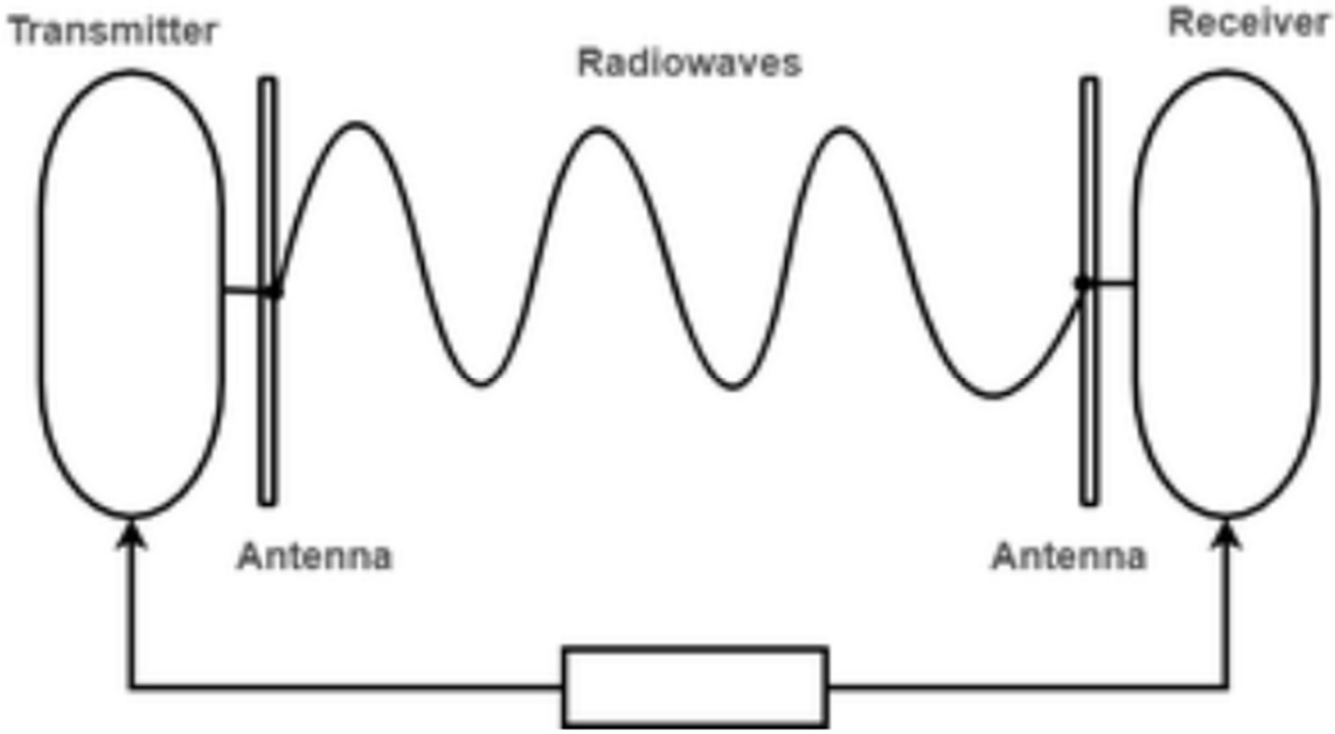
- It is also referred to as **Wireless** or Unbounded transmission media. **No physical medium** is required for the transmission of **electromagnetic signals**.

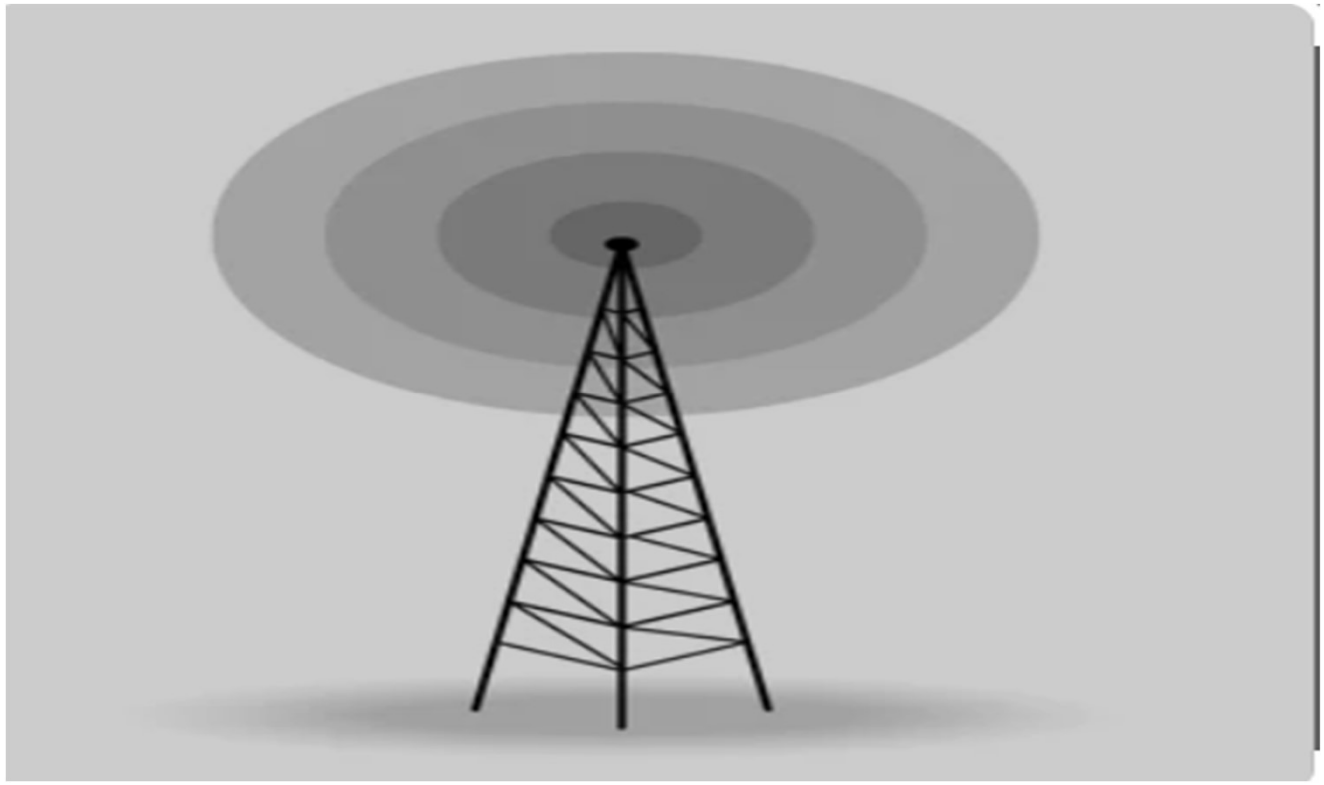
Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

(i) Radio waves –

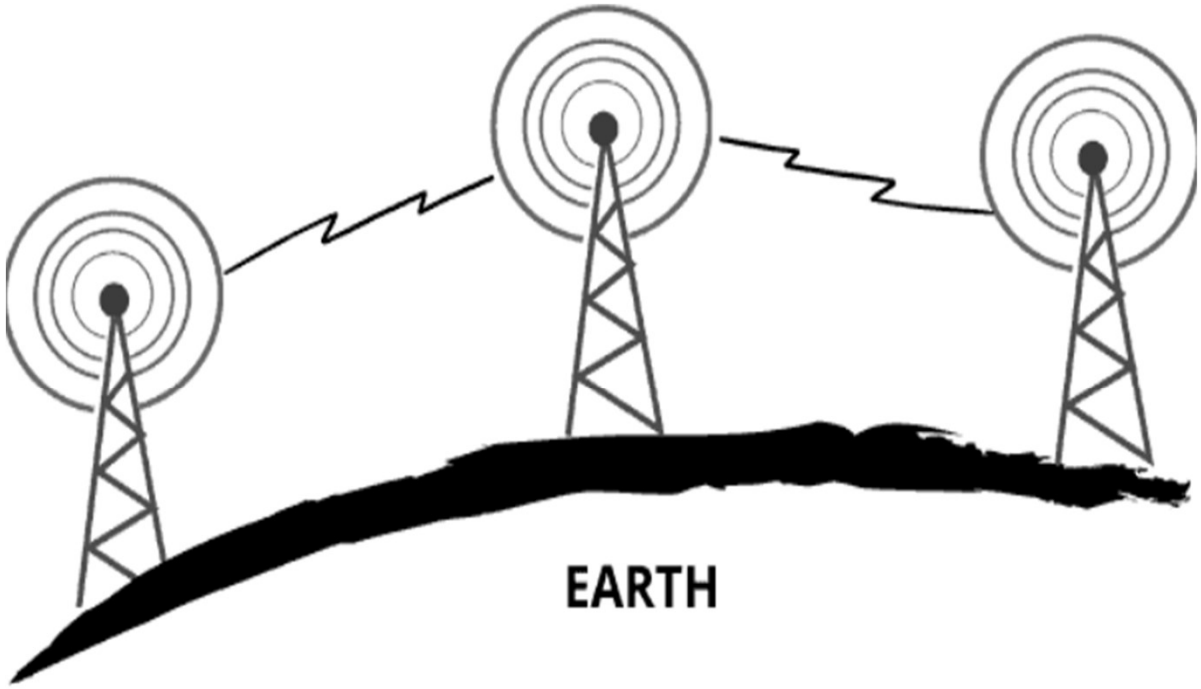
- These are easy to generate and can penetrate through buildings.
- The sending and receiving antennas need not be aligned.
- Frequency Range:3KHz – 1GHz.
- AM and FM radios and cordless phones use Radio waves for transmission.
- Omnidirectional

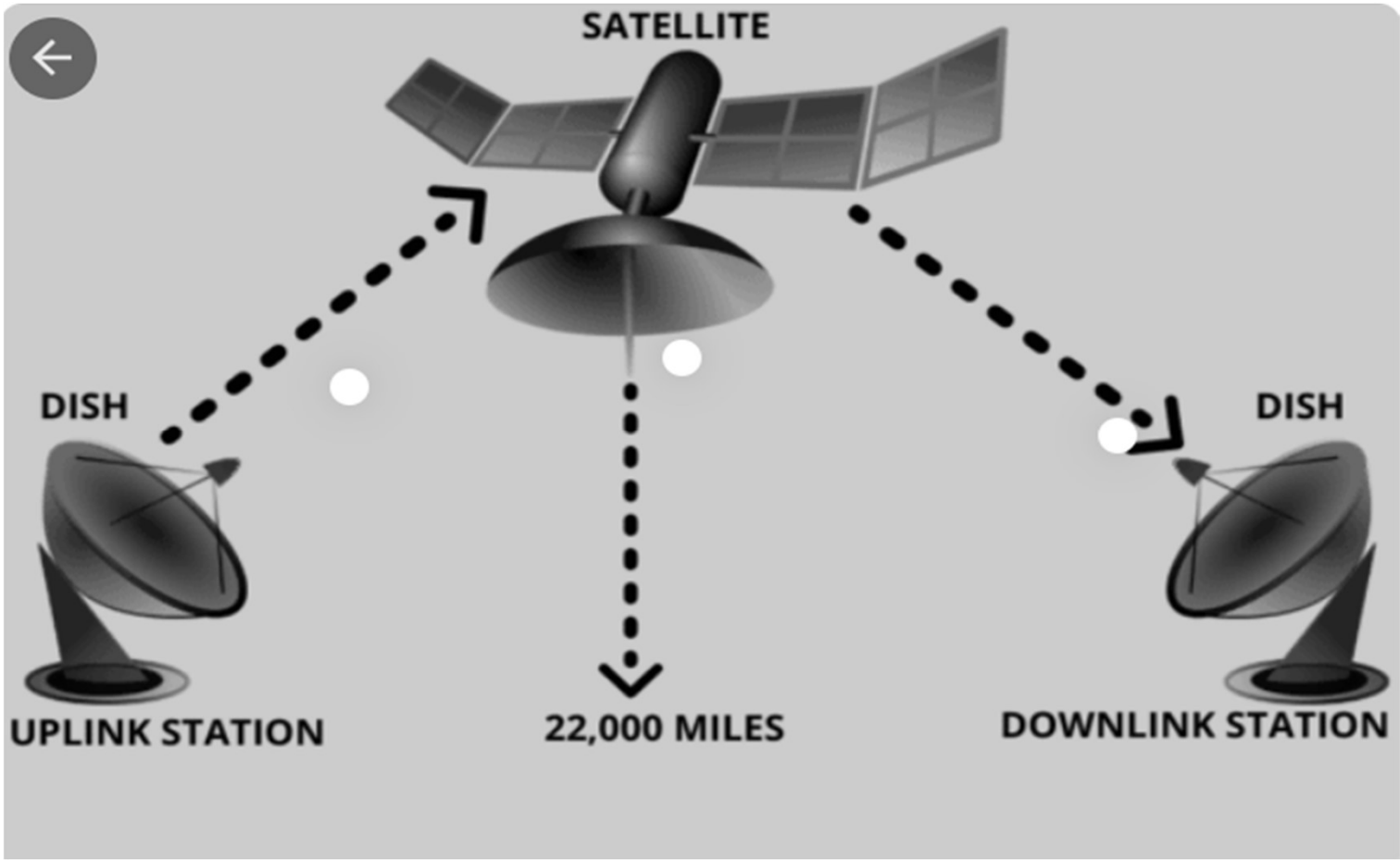

Transmitter
Radiowaves
Receiver
Antenna
Antenna



(ii) Microwaves –

- It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other.
- The distance covered by the signal is directly proportional to the height of the antenna.
- Frequency Range:1GHz – 300GHz.
- These are majorly used for mobile phone communication and television distribution.


EARTH


SATELLITE
DISH
DISH
UPLINK STATION
22,000 MILES
DOWNLINK STATION

(iii) Infrared –

- Infrared waves are used for very short distance communication.
- They cannot penetrate through obstacles.
- This prevents interference between systems.
- Frequency Range:300GHz – 400THz.
- It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Television

Infrared Radiations

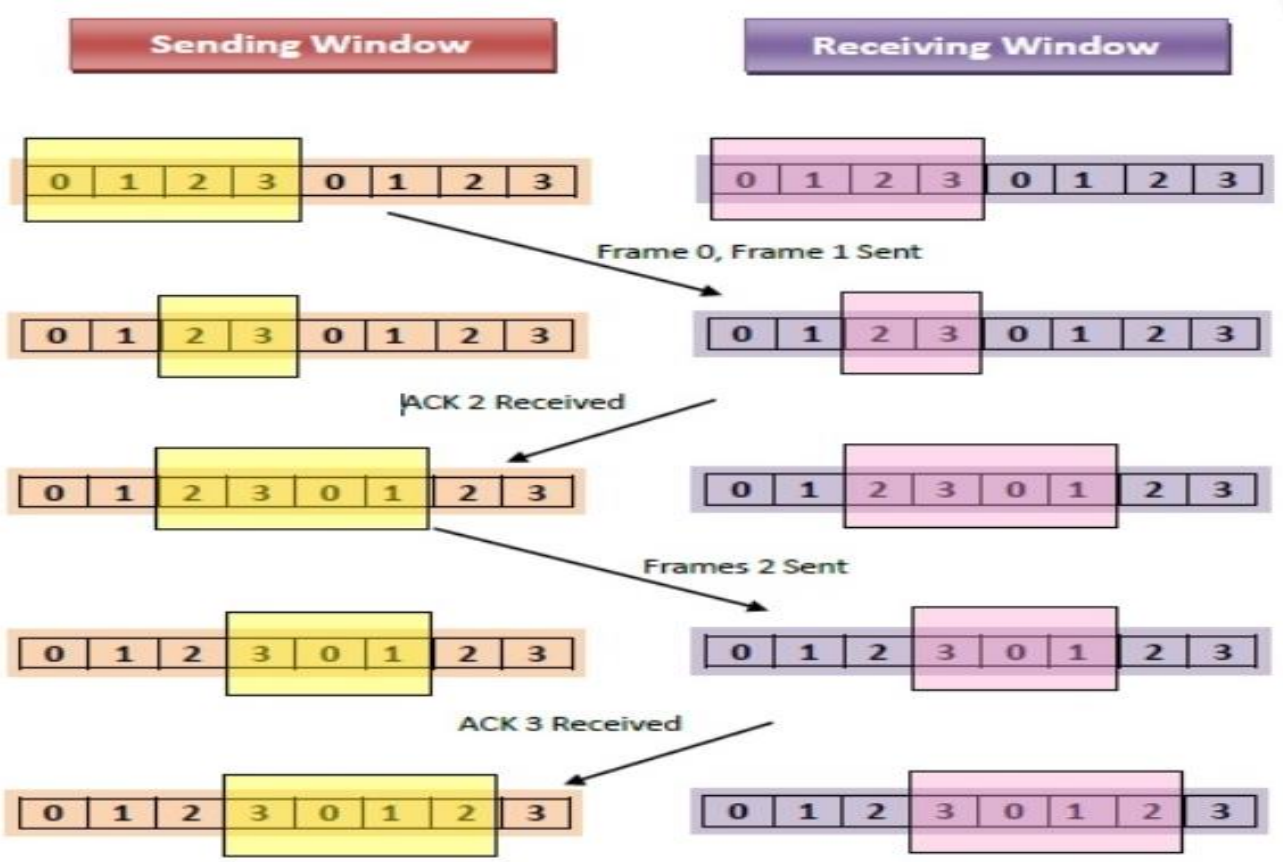
Remote

Sliding Window Protocol

Sliding Window Protocol

- Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames.
- The sliding window is also used in Transmission Control Protocol.
- In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver.
- The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

Working of Sliding Window Protocol



Types of Sliding Window Protocols

- In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.
- The size of the sending window determines the sequence number of the outbound frames.
- If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n–1.

Go – Back – *N* ARQ

- Go – Back – *N* ARQ provides for **sending multiple frames before receiving the acknowledgment for the first frame**.
- The frames are sequentially numbered and a finite number of frames are sent.
- If the acknowledgment of a **frame is not received** within the time period, **all frames starting from that frame are retransmitted**.

Selective Repeat ARQ

- This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame.
- Only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

Data Link Layer

Design Issues in Data Link Layer

- Data-link layer is the second layer after the physical layer.
- The data link layer is responsible for maintaining the data link between two hosts or nodes.
- Some of its sub-layers and their functions are as following below.
- The data link layer is divided into two sub-layers :

1.<u>Logical Link Control Sub-layer (LLC)</u> –

Provides the logic for the data link, Thus it controls the synchronization, flow control, and error checking functions of the data link layer. Functions are –

(i) Error Recovery.

(ii) It performs the flow control operations.

(iii) User addressing.

2. Media Access Control Sub-layer (MAC) –

- It controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. This layer is responsible for sending the data over the network interface card. Functions are –

  (i) To perform the control of access to media.

  (ii) It performs the unique addressing to stations directly connected to LAN.

  (iii) Detection of errors.

Design issues with data link layer are :

1.Services provided to the network layer

- The data link layer act as a **service interface to the network layer**.
- The principle service is **transferring data** from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).

2.Frame synchronization

The source machine sends data in the form of blocks called **frames** to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.

3. Flow control

Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4.Error control

Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

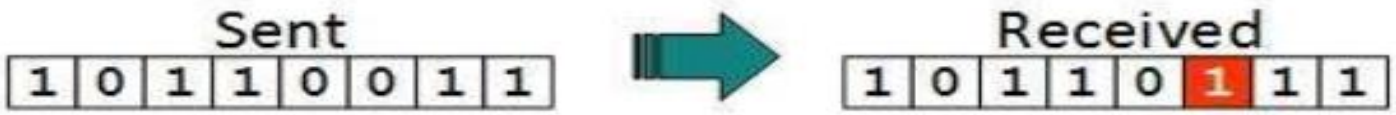
Error Detection and Correction

Error Detection and Correction

- There are many reasons such as **noise, cross-talk** etc., which may help data to get corrupted during transmission.
- Most of the applications would not function expectedly if they receive erroneous data.
- Applications such as voice and video may not be that affected and with some errors they may still function well.
- Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy.

Types of Errors

- **Single bit error**



In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**

Frame is received with more than one bits in corrupted state.

- **Burst error**

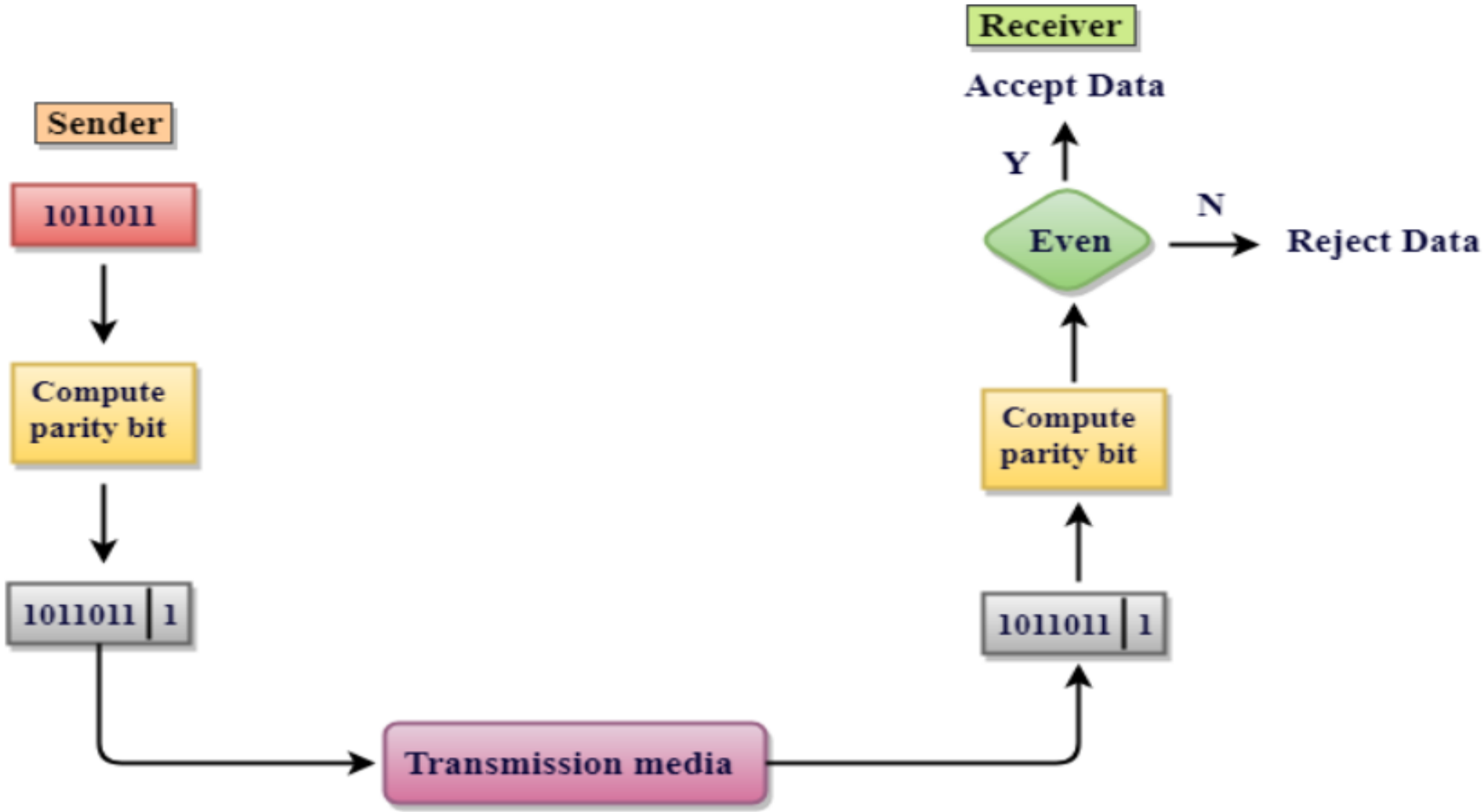
Frame contains more than1 consecutive bits corrupted.

Error Detecting Techniques

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

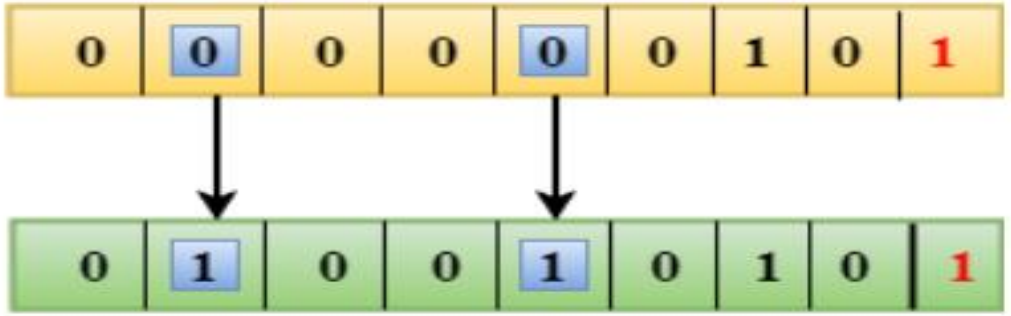
Single Parity Check

- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even.
- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.


Sender
1011011
Compute parity bit
1011011 | 1
Transmission media
Receiver
Accept Data
Y
N
Even
Reject Data
Compute parity bit
1011011 | 1

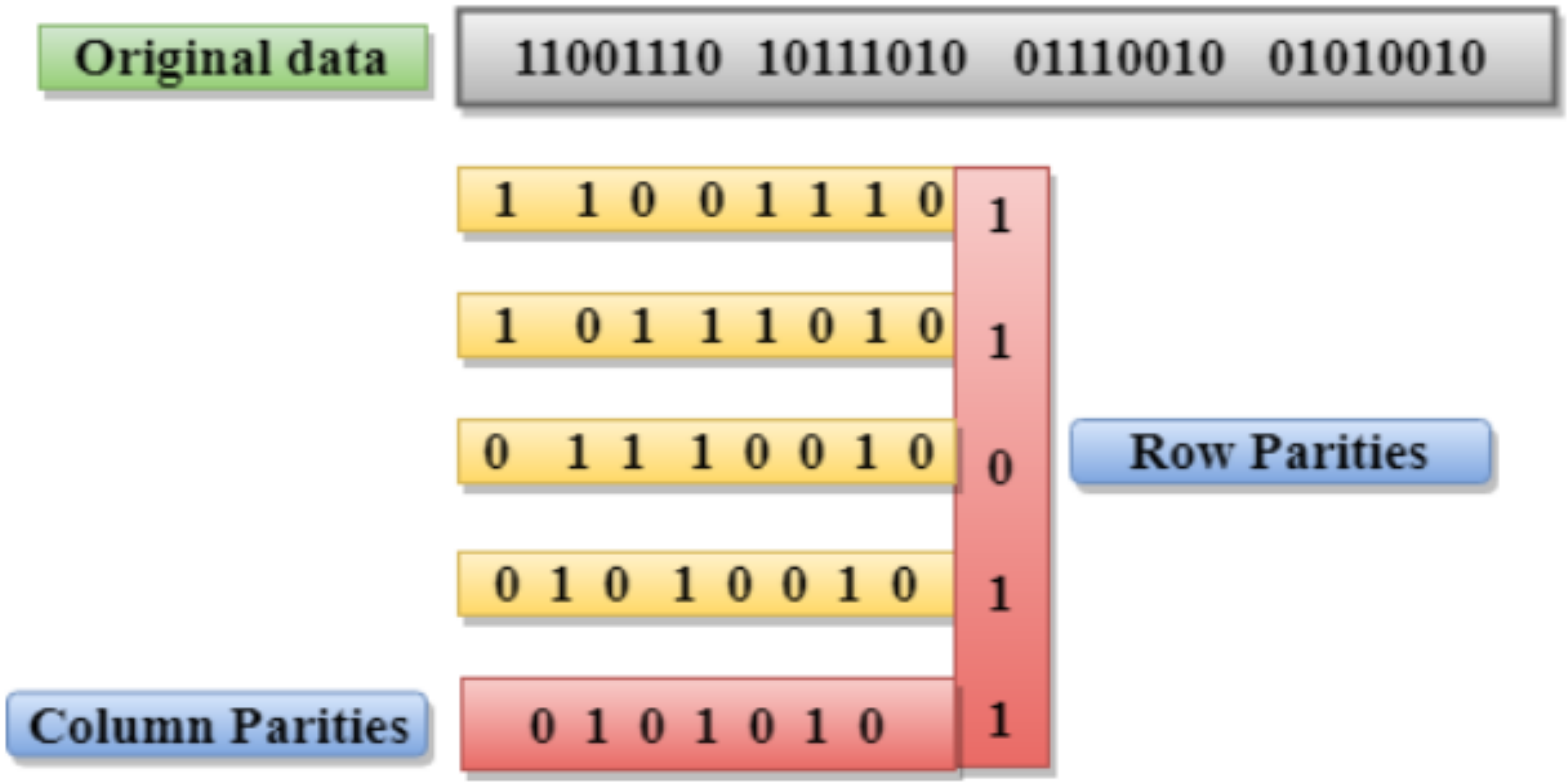
Drawbacks Of Single Parity Checking

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.


Original data
11001110 10111010 01110010 01010010
1 1 0 0 1 1 1 0
1
1 0 1 1 1 0 1 0
1
0 1 1 1 0 0 1 0
0
Row Parities
0 1 0 1 0 0 1 0
1
Column Parities
0 1 0 1 0 1 0
1

Checksum

- A Checksum is an error detection technique based on the concept of redundancy.

Checksum Generator

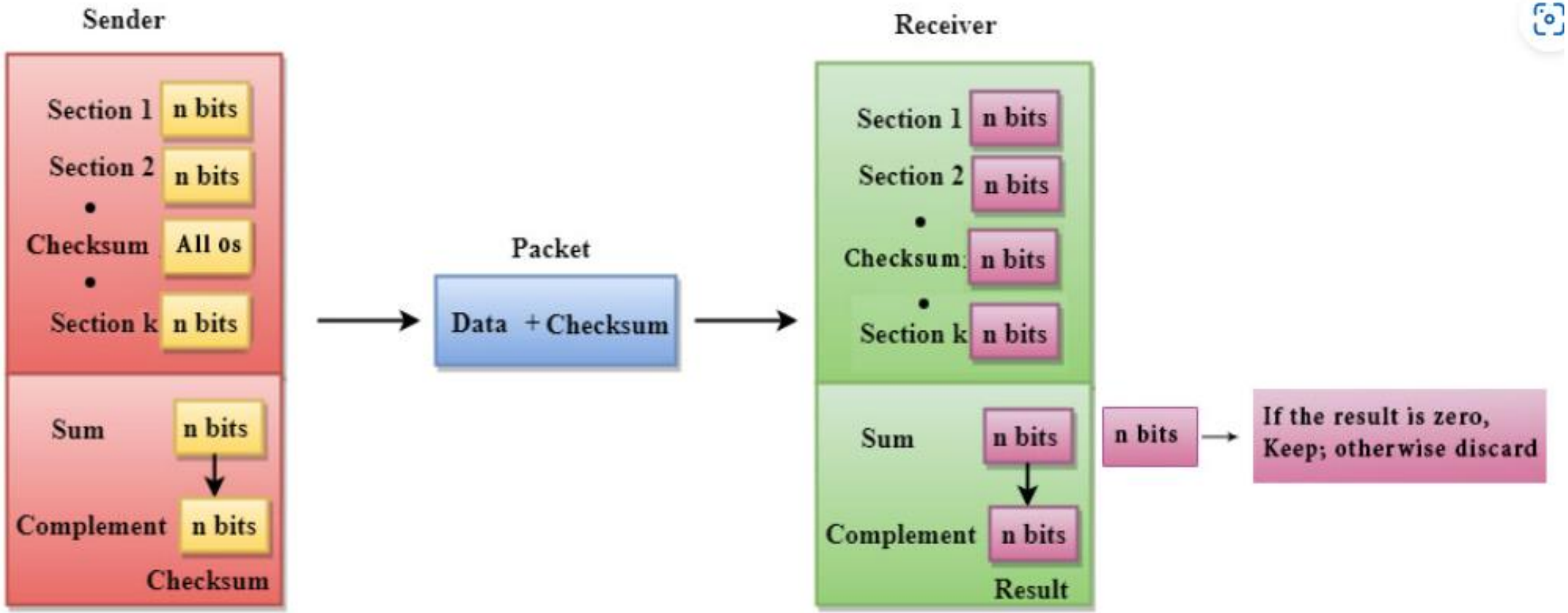
The Sender follows the given steps:

1. The block unit is divided into k sections, and each of n bits.
2. All the k sections are added together by using one's complement to get the sum.
3. The sum is complemented and it becomes the checksum field.
4. The original data and checksum field are sent across the network.

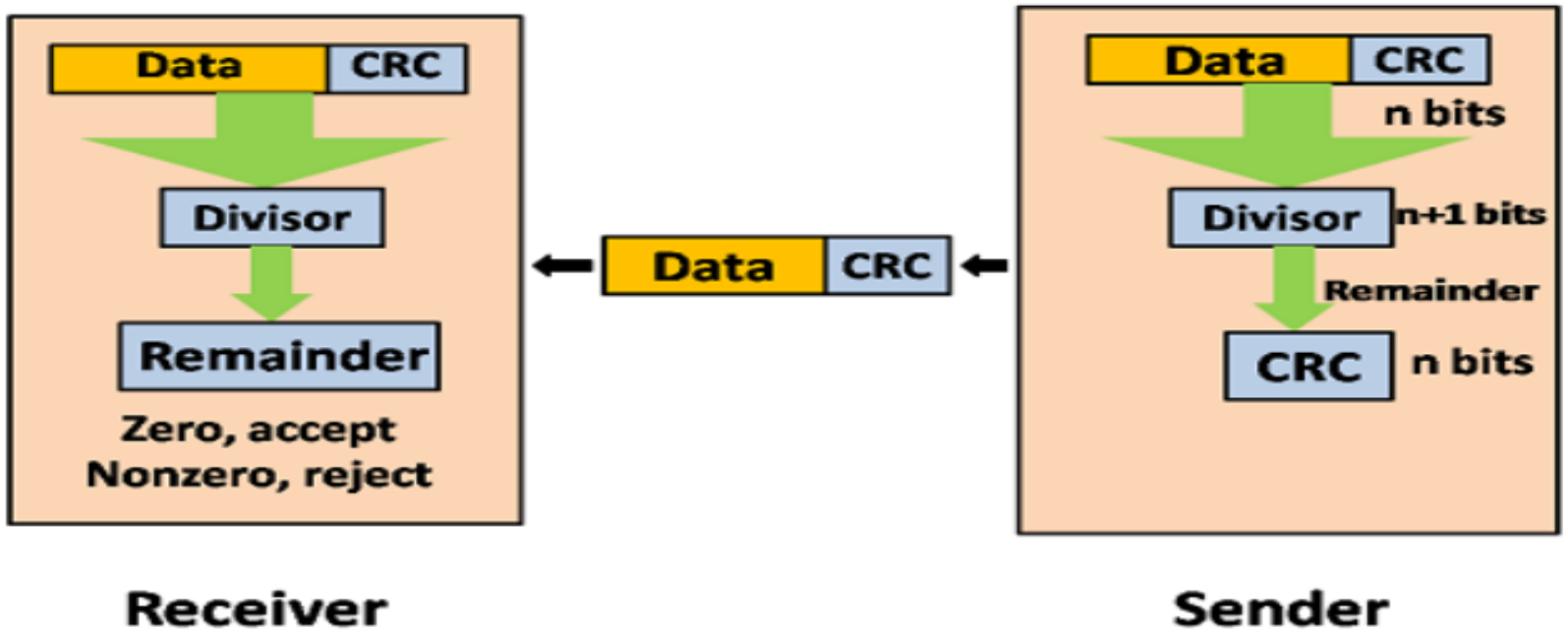
Checksum Checker

The Receiver follows the given steps:

1. The block unit is divided into k sections and each of n bits.
2. All the k sections are added together by using one's complement algorithm to get the sum.
3. The sum is complemented.
4. If the result of the sum is zero, then the data is accepted otherwise the data is discarded.


Sender
Section 1
n bits
Section 2
n bits
Checksum
All 0s
Section k
n bits
Sum
n bits
Complement
n bits
Checksum
Packet
Data + Checksum
Receiver
Section 1
n bits
Section 2
n bits
Checksum
n bits
Section k
n bits
Sum
n bits
Complement
n bits
Result
n bits
If the result is zero,
Keep; otherwise discard

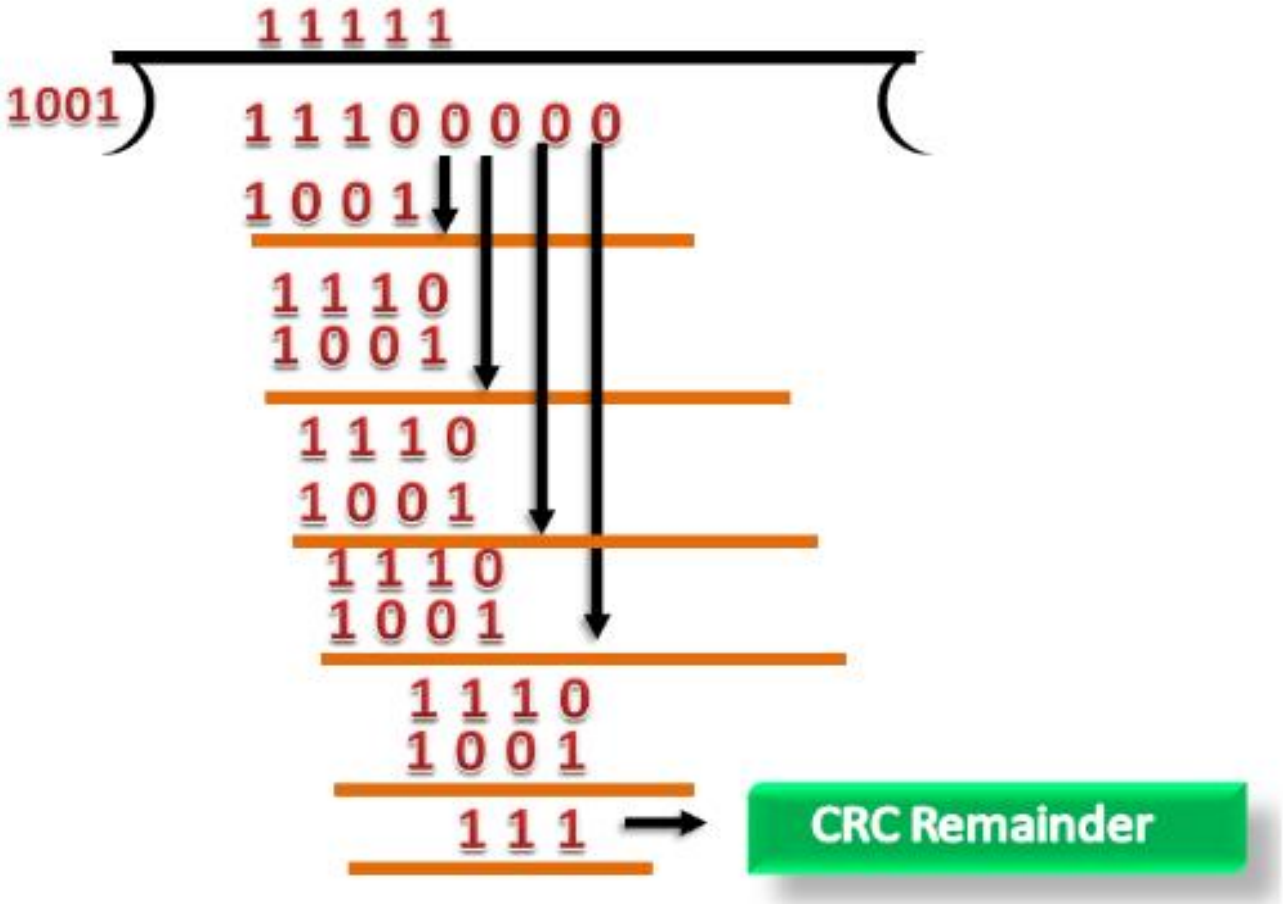
Cyclic Redundancy Check (CRC)



Suppose the original data is 11100 and divisor is 1001.

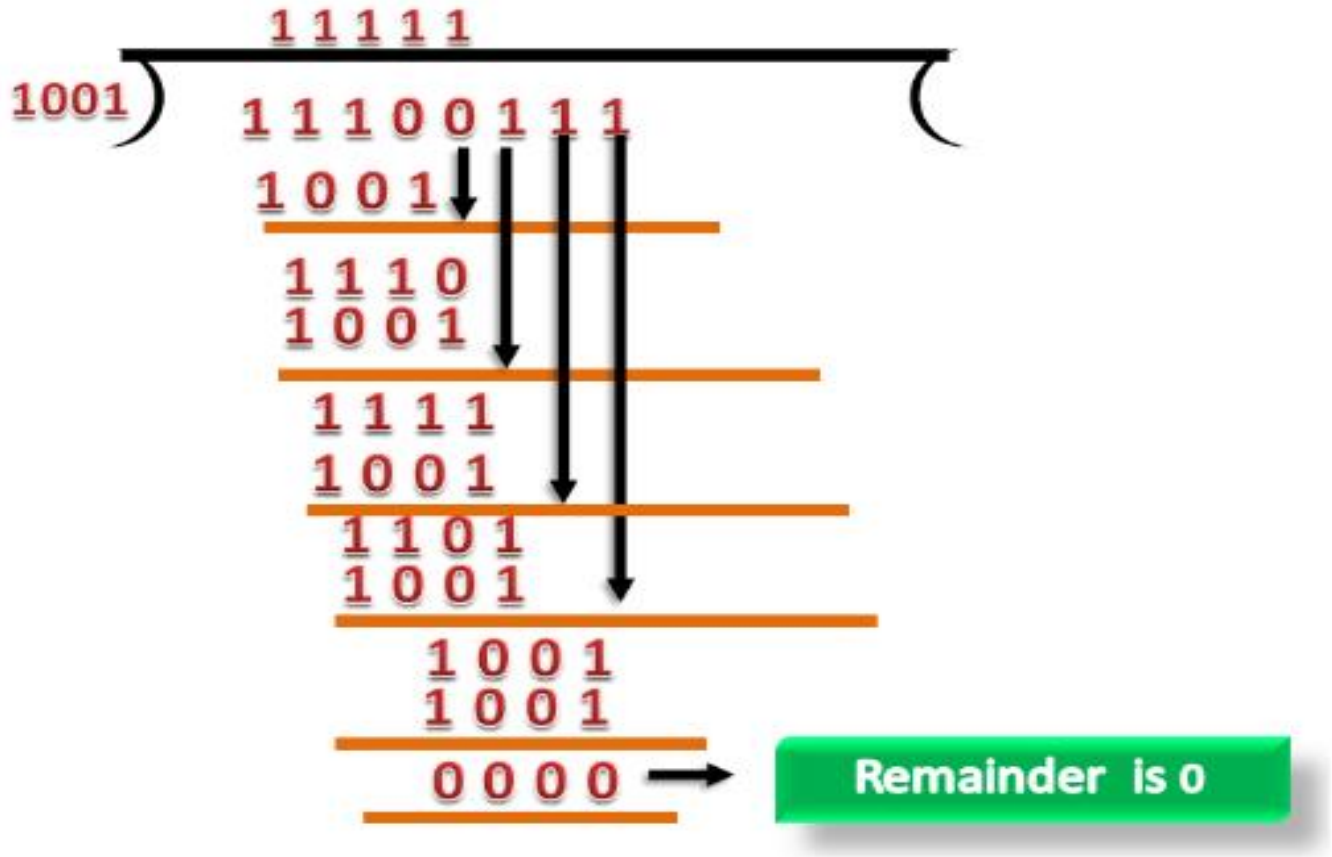
CRC Generator

- Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4.
- The string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.


1 1 1 1 1
1001
1 1 1 0 0 0 0 0
1 0 0 1
1 1 1 0
1 0 0 1
1 1 1 0
1 0 0 1
1 1 1 0
1 0 0 1
1 1 1 0
1 0 0 1
1 1 1
CRC Remainder

CRC Checker

- The functionality of the CRC checker is similar to the CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.


1 1 1 1 1
1001
1 1 1 0 0 1 1 1
1 0 0 1
1 1 1 0
1 0 0 1
1 1 1 1
1 0 0 1
1 1 0 1
1 0 0 1
1 0 0 1
1 0 0 1
0 0 0 0
Remainder is 0

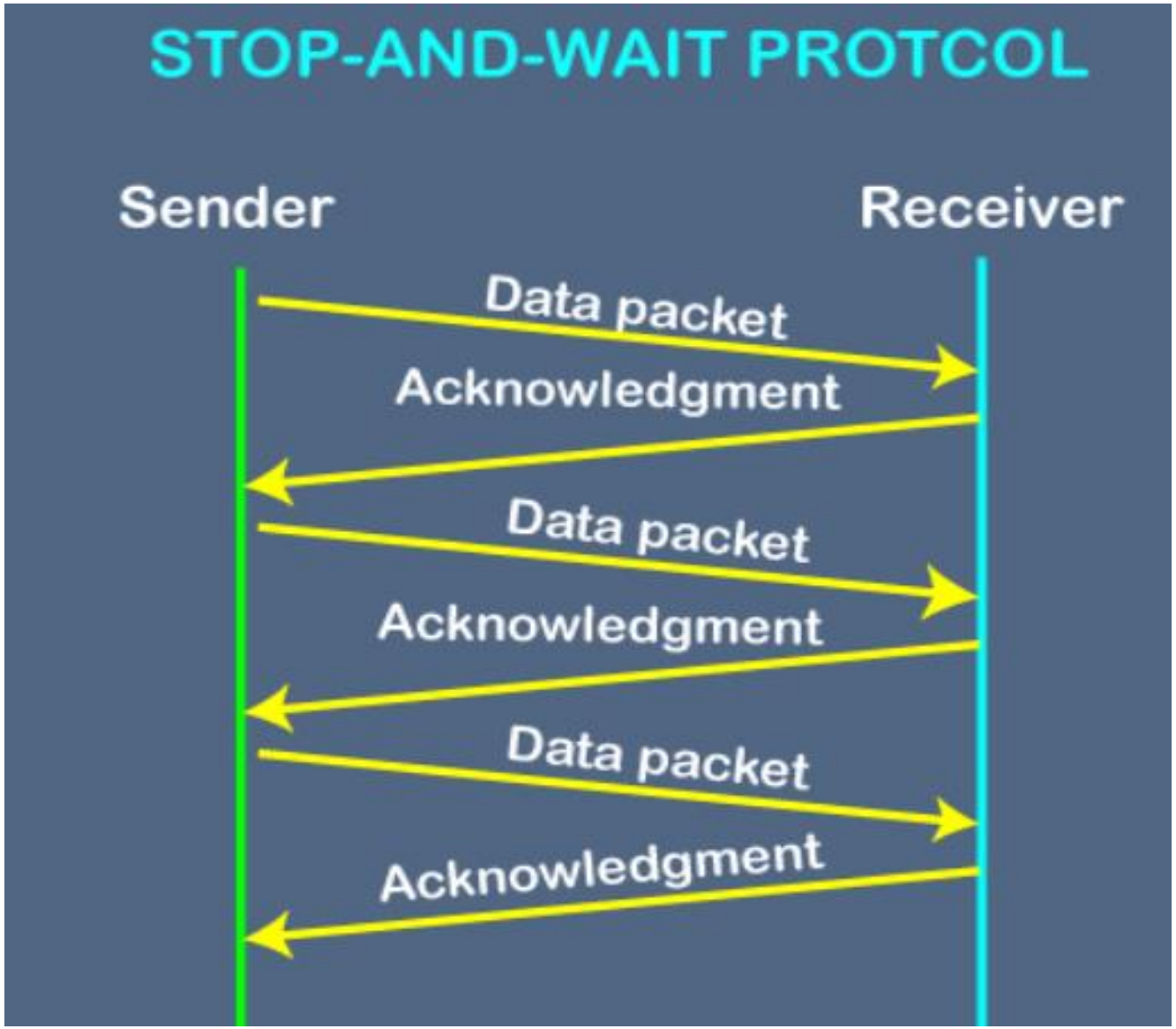
Simplex Stop and Wait Protocol

Introduction

- Error control mechanism is used so that the received data should be **exactly same** whatever sender has sent the data.
- Divided into two categories, i.e., **Stop and Wait** and **sliding window**.
- The sliding window is further divided into two categories, i.e., **Go Back N, and Selective Repeat**.
- **Based on the usage**, the people select the error control mechanism whether it is **stop and wait** or **sliding window**.

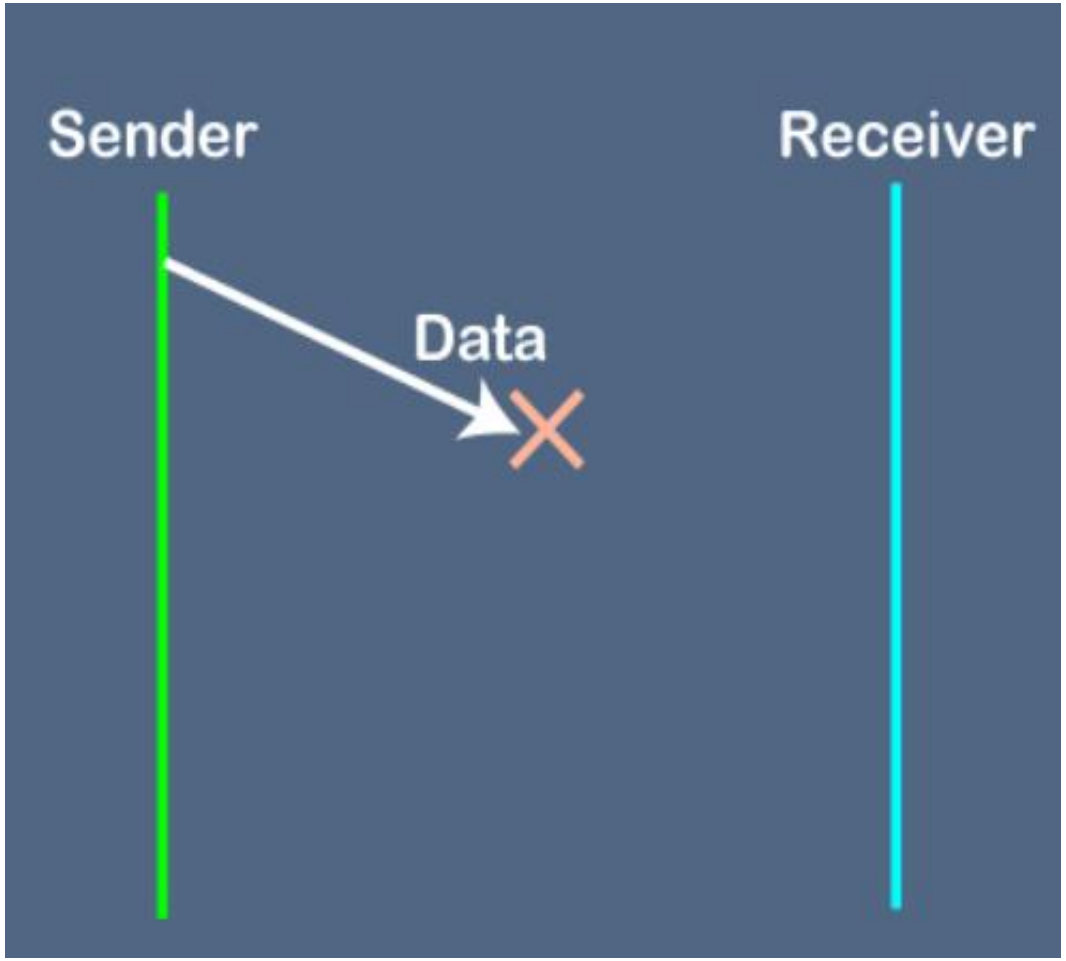
Stop and Wait protocol

- Sender sends the data to the receiver then sender stops and waits until sender receives the **acknowledgement** from the receiver.
- It is a data-link layer protocol which is used for transmitting the data over the **noiseless channels**.
- It provides **unidirectional data transmission** which means that either sending or receiving of data will take place at a time.

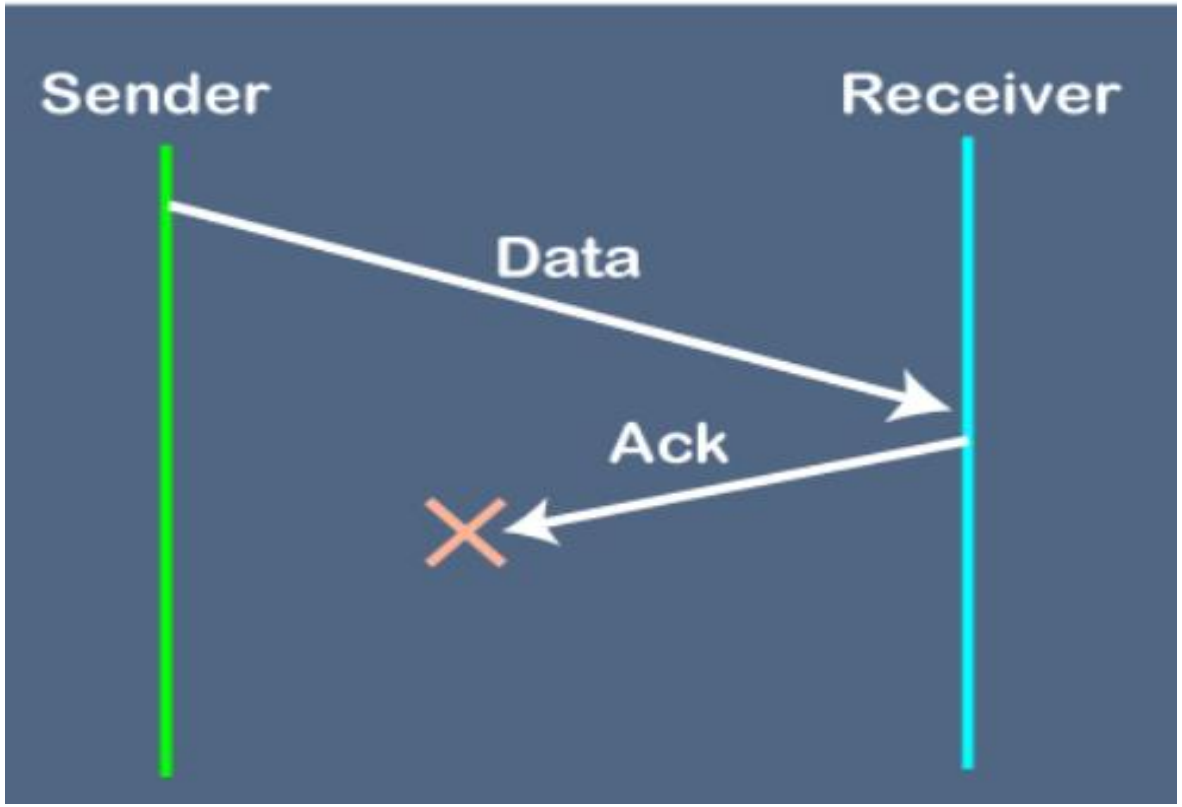

STOP-AND-WAIT PROTCOL
Sender
Receiver
Data packet
Acknowledgment
Data packet
Acknowledgment
Data packet
Acknowledgment

Disadvantages of Stop and Wait protocol

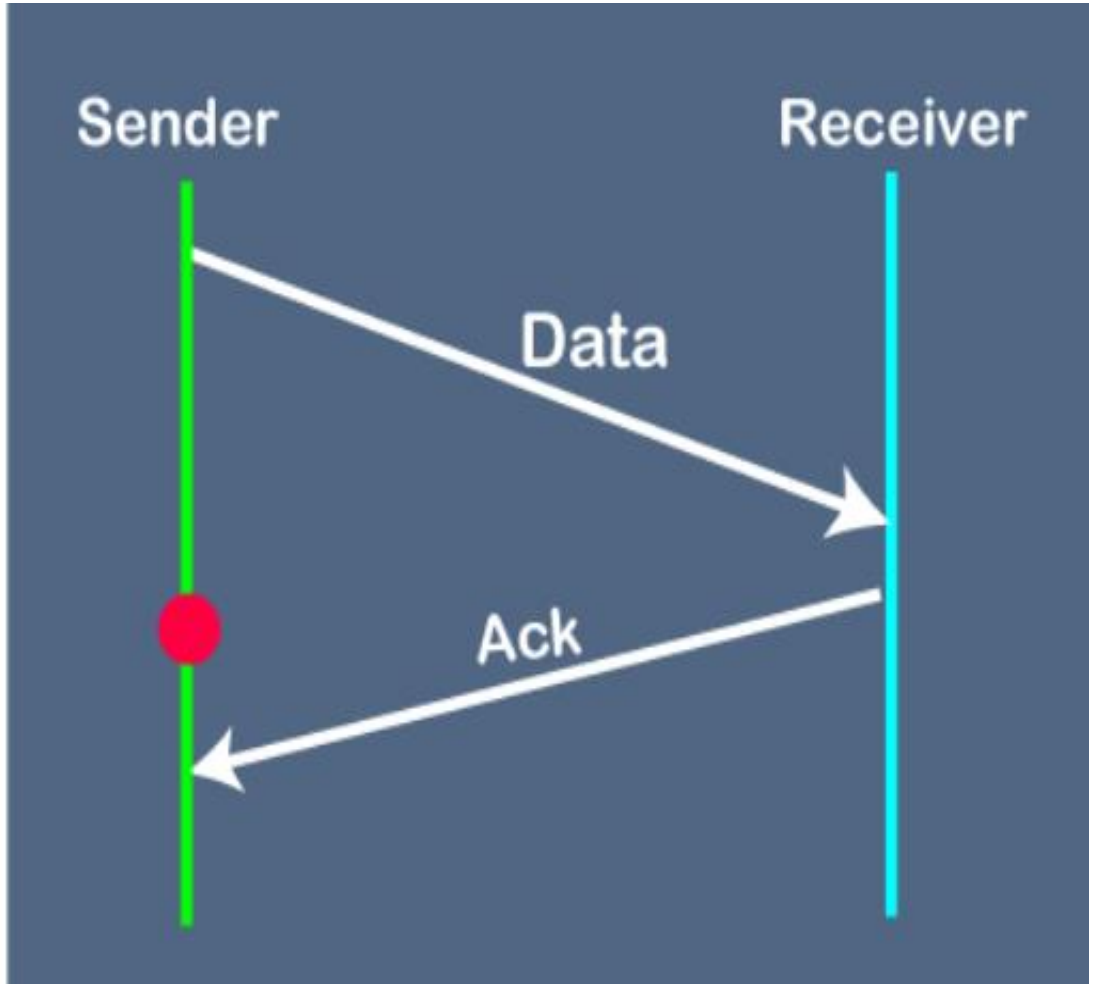
1. Problems occur due to lost data



2. Problems occur due to lost acknowledgment



3. Problem due to the delayed data or acknowledgment



Congestion Control

Definition of Congestion Control

- A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

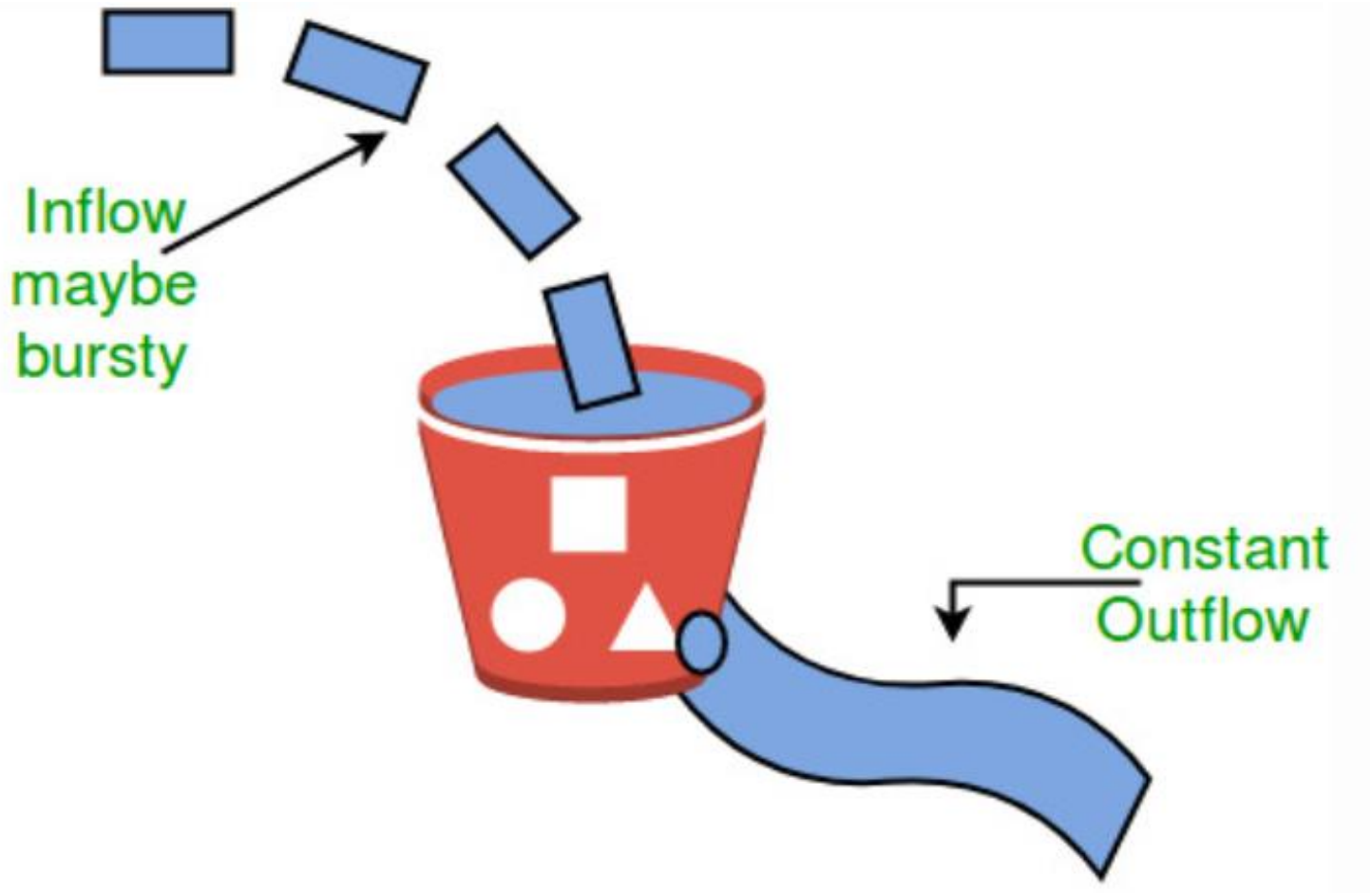
Effects of Congestion

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

Congestion Control Algorithms

Leaky Bucket Algorithm

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.


Inflow
maybe
bursty
Constant
Outflow

leaky bucket Algorithm

1.When host wants to send packet, packet is thrown into the bucket.

2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.

3. Bursty traffic is converted to a uniform traffic by the leaky bucket.

4.In practice the bucket is a finite queue that outputs at a finite rate.

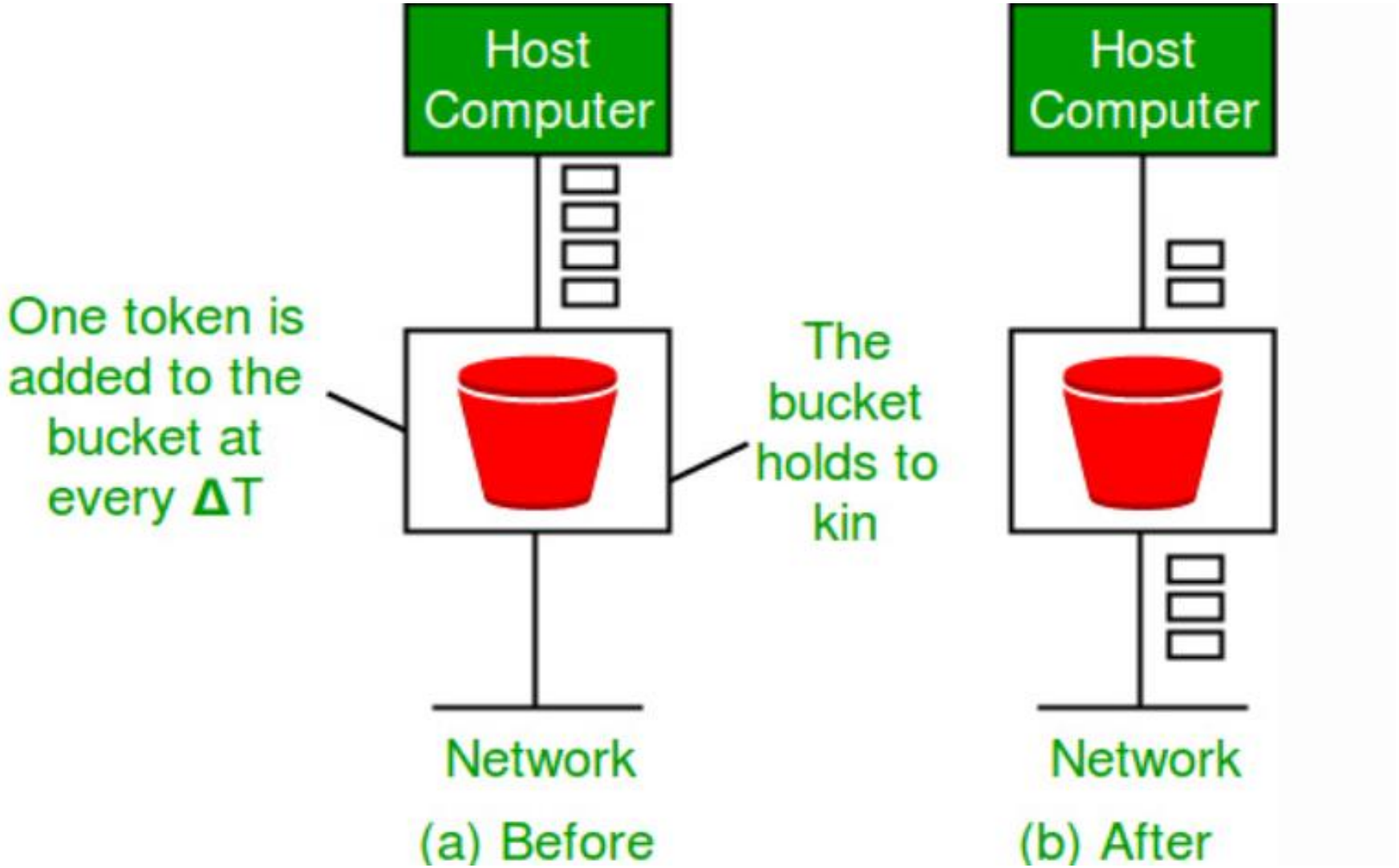
Token bucket Algorithm

- The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is, So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket.
2. The bucket has a maximum capacity
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

- In the token bucket, algorithm tokens are generated at each tick (up to a certain limit).
- For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate.
- Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.


Host Computer
One token is added to the bucket at every ΔT
Network
(a) Before
Host Computer
The bucket holds to kin
Network
(b) After

Elements of Transport Protocols

Elements of Transport Protocols

- To establish a reliable service between **two machines on a network**, transport protocols are implemented.
- The major difference lies in the fact that the **data link layer** uses a **physical channel** between two routers while the **transport layer uses a subnet**.

Error Control

- **Error detection and error recovery** are an integral part of reliable service, and therefore they are necessary to perform error control mechanisms on an end-to-end basis.
- To control errors from lost or duplicate segments, the transport layer enables **unique segment sequence numbers to the different packets** of the message, **creating virtual circuits**, allowing only **one virtual circuit per session**.

Flow Control

- Flow control is to maintain a **synergy between a fast process and a slow process**.
- **Acknowledgements** are sent back to manage end-to-end flow control.
- **Go back N algorithms** are used to request retransmission of packets starting with packet number.
- **Selective Repeat** is used to request specific packets to be retransmitted.

Multiplexing/De multiplexing

- The transport layer **establishes a separate network connection** for each transport connection required by the session layer.
- **To improve throughput**, the transport layer establishes **multiple network connections**.
- When the issue of throughput is not important, it **multiplexes several transport connections onto the same network** connection, thus reducing the cost of establishing and maintaining the network connections.

- When several connections are multiplexed, they call for **demultiplexing at the receiving end**.
- In the case of the transport layer, the **communication takes place only between two processes** and not between two machines.
- Hence, communication at the transport layer is also known as **peer-to-peer or process-to-process communication**.

Fragmentation and re-assembly

- When the transport layer receives a large message from the session layer, it **breaks the message into smaller units** depending upon the requirement. This process is called fragmentation.
- Thereafter, it is passed to the network layer. Conversely, when the **transport layer acts as the receiving process, it reorders the pieces of a message** before reassembling them into a message.

Addressing

- Transport Layer deals with addressing or **labelling a frame**.
- It also differentiates between a **connection and a transaction**. Connection identifiers are **ports or sockets** that **label each frame**, so the receiving device knows which process it has been sent from. This helps in keeping **track of multiple-message conversations**. Ports or sockets address multiple conservations in the **same location**.

Routing Algorithms

PART I

The Optimality Principle

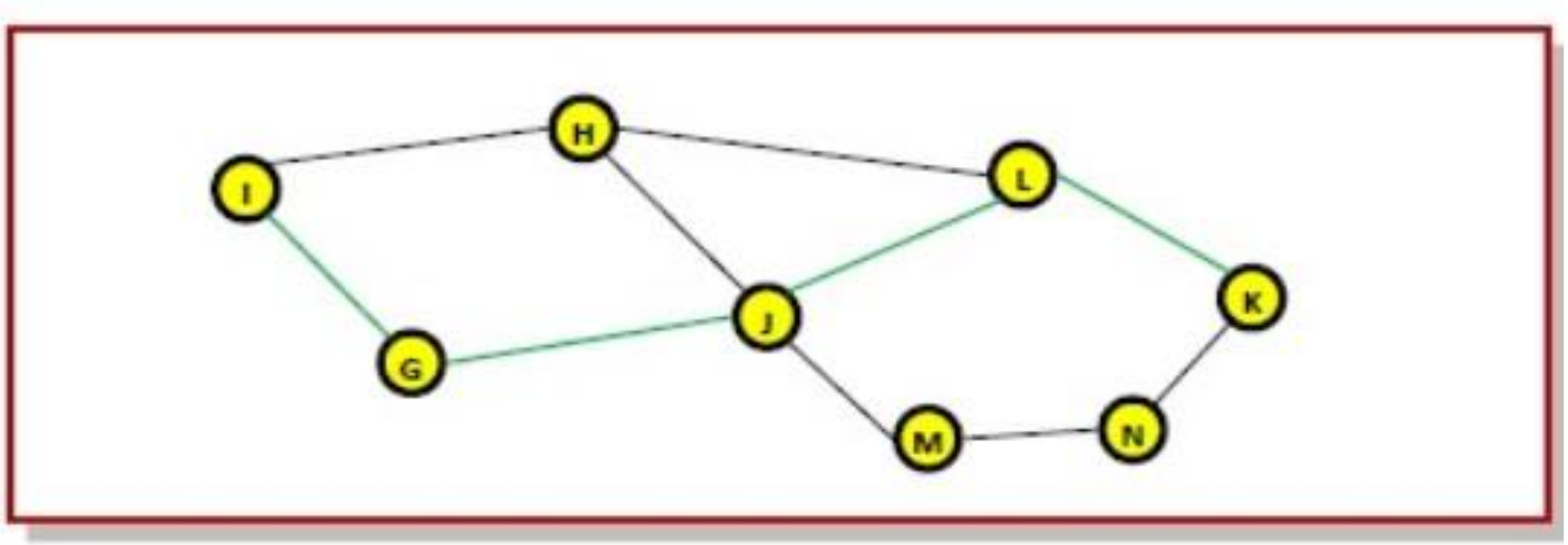
- The purpose of a routing algorithm at a router is to **decide which output line an incoming packet should go**.
- The optimal path from a particular router to another may be the **least cost path, the least distance path, the least time path, the least hops path** or a combination of any of the above.

The optimality principle can be logically proved as follows –

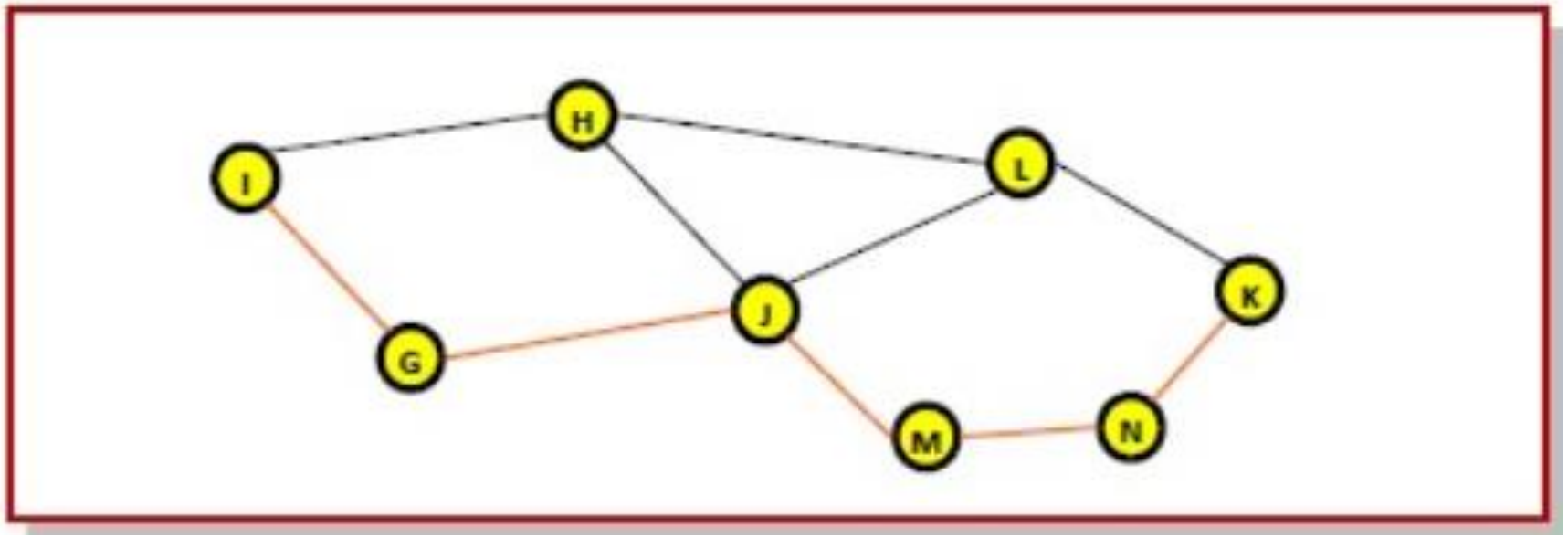
- If a better route could be found between router J and router K, the path from router I to router K via J would be updated via this route. Thus, the optimal path from J to K will again lie on the optimal path from I to K.

Example

Consider a network of routers, {G, H, I, J, K, L, M, N} as shown in the figure. Let the optimal route from I to K be as shown via the green path, i.e. via the route I-G-J-L-K. According to the optimality principle, the optimal path from J to K with be along the same route, i.e. J-L-K.



Suppose we find a better route from J to K is found, say along J-M-N-K. Consequently, we will also need to update the optimal route from I to K as I-GJ- M-N-K, since the previous route ceases to be optimal in this situation.



Shortest path routing algorithm

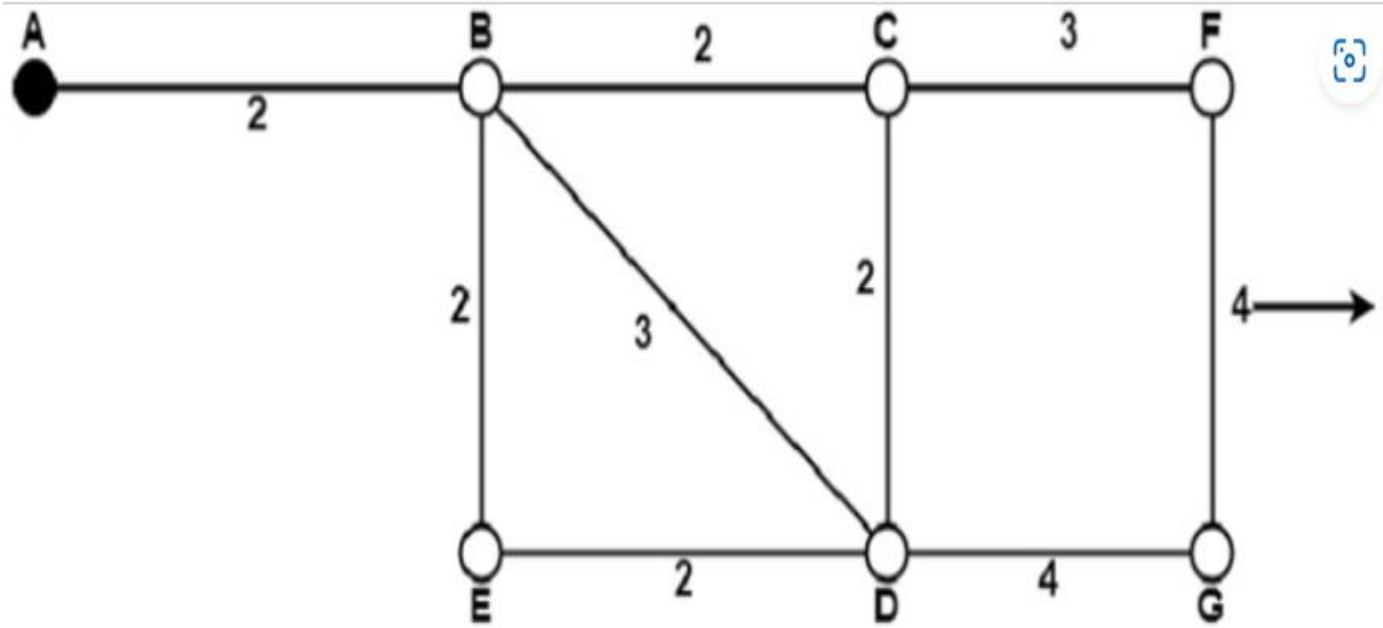
- In this algorithm, to select a route, **the algorithm discovers the shortest path between two nodes**.
- It can use multiple hops, the geographical area in kilometres or labelling of arcs for measuring path length.
- The labelling of arcs can be done with mean queuing, transmission delay for a standard test packet on an hourly basis, or computed as a function of bandwidth, average distance traffic, communication cost, mean queue length, measured delay or some other factors.

- In shortest path routing, the topology communication network is defined using a **directed weighted graph**.
- The **nodes** in the graph define **switching components** and the **directed arcs** in the graph define **communication connection** between switching components.
- Each **arc has a weight** that defines the **cost of sharing a packet** between two nodes in a specific direction.

- This **cost** is usually a positive value that can denote such factors as **delay, throughput, error rate, financial costs**, etc.
- A **path** between two nodes can go through various intermediary nodes and arcs..
- The goal of shortest path routing is to **find a path** between two nodes that has the **lowest total cost**, where the total cost of a path is the sum of arc costs in that path.

Example

Dijikstra uses the nodes labelling with its distance from the source node along the better-known route. Initially, all nodes are labelled with infinity, and as the algorithm proceeds, the label may change.



Graphical Representation of Nodes with labeled path

It can be done in various passes as follows, with A as the source

Pass 1. B (2, A), C(∞,–), F(∞,–), e(∞,–), d(∞,–), G 60

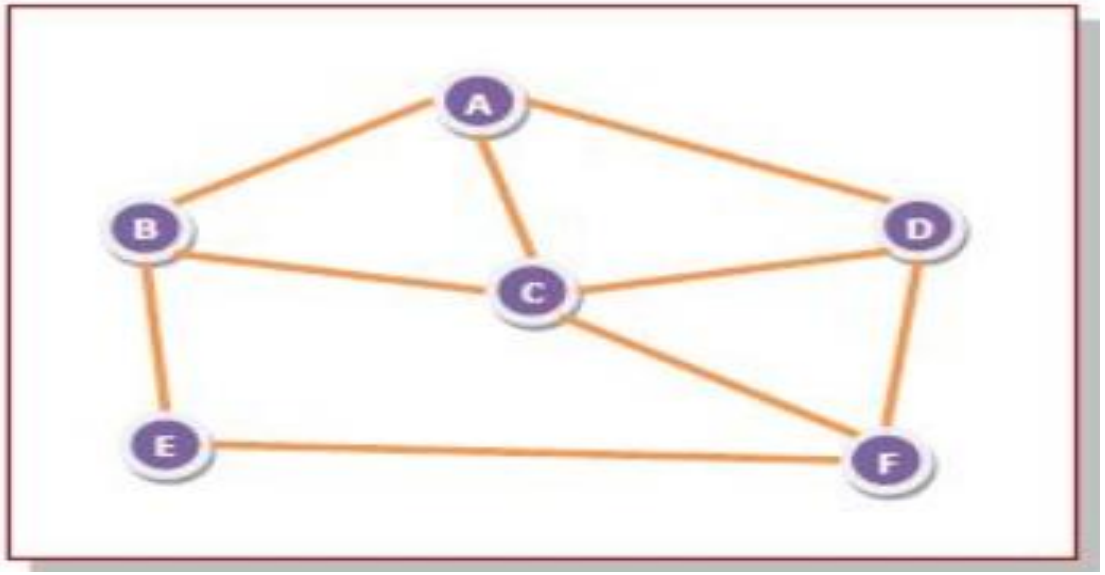
Pass 2. B (2, A), C(4, B), D(5, B), E(4, B), F(∞,–),G(∞,–)

Pass 3. B(2, A), C(4, B), D(5, B), E(4, B), F(7, C), G(9, D)

- There can be two paths between A and G. One follows through ABCFG and the other through ABDG. The first one has a path length of 11, while the second one has 9. Hence, the second one, as G (9, D), is selected. Similarly, Node D has also three paths from A as ABD, ABCD and ABED. The first one has a path length of 5 rest two have 6. So, the first one is selected.

Flooding

- when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on.
- For example, lconsider the network in the figure, having six routers that are connected through transmission lines.



Using flooding technique –

- An incoming packet to A, will be sent to B, C and D.
- B will send the packet to C and E.
- C will send the packet to B, D and F.
- D will send the packet to C and F.
- E will send the packet to F.
- F will send the packet to C and E.

Types of Flooding

- **Uncontrolled flooding** – Here, each router unconditionally transmits the incoming data packets **to all its neighbours**.
- **Controlled flooding** – They use some methods to control the transmission of packets to the neighbouring nodes. The two popular algorithms for controlled flooding are Sequence Number Controlled Flooding (SNCF) and Reverse Path Forwarding (RPF).
- **Selective flooding** – the routers don't transmit the incoming packets only along those paths which are heading towards approximately in the right direction, instead of every available paths.

Advantages of Flooding

- It is very simple to setup and implement, since a router may know only its neighbours.
- It is extremely robust**. Even in case of malfunctioning** of a large number routers, the packets find a way to reach the destination.
- All nodes which are **directly or indirectly connected are visited**. So, there are no chances for any node to be left out. This is a main criteria in case of broadcast messages.
- The shortest path is always chosen by flooding.

Limitations of Flooding

- Flooding tends to create an i**nfinite number of duplicate data packets**, unless some measures are adopted to damp packet generation.
- It is wasteful if a single destination needs the packet, since it delivers the **data packet to all nodes irrespective of the destination.**
- The network may be **clogged** with unwanted and duplicate data packets. This may hamper delivery of other data packets.

Routing Algorithms

PART II

Link State Routing

- While distance-vector routers use a **distributed algorithm** to compute their **routing tables**, **link-state routing uses link-state routers** to exchange messages that allow each router to **learn the entire network topology**.
- Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

Features of link state routing protocols

- **Link state packet –** A small packet that contains routing information.
- **Link state database –** A collection of information gathered from the link-state packet.
- **Shortest path first algorithm (Dijkstra algorithm) –** A calculation performed on the database results in the shortest path
- **Routing table –** A list of known paths and interfaces.

Calculation of shortest path –

To find the shortest path, each node needs to run the famous **Dijkstra algorithm**. This famous algorithm uses the following steps:

- **Step-1:** The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database
- **Step-2:** Now the node selects one node, among all the nodes not in the tree-like structure, which is nearest to the root, and adds this to the tree. The shape of the tree gets changed.
- **Step-3:** After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.
- **Step-4:** The node repeats Step 2. and Step 3. until all the nodes are added to the tree

Link State protocols in comparison to Distance Vector protocols:

1. It requires a large amount of memory.

2. Shortest path computations require many CPU circles.

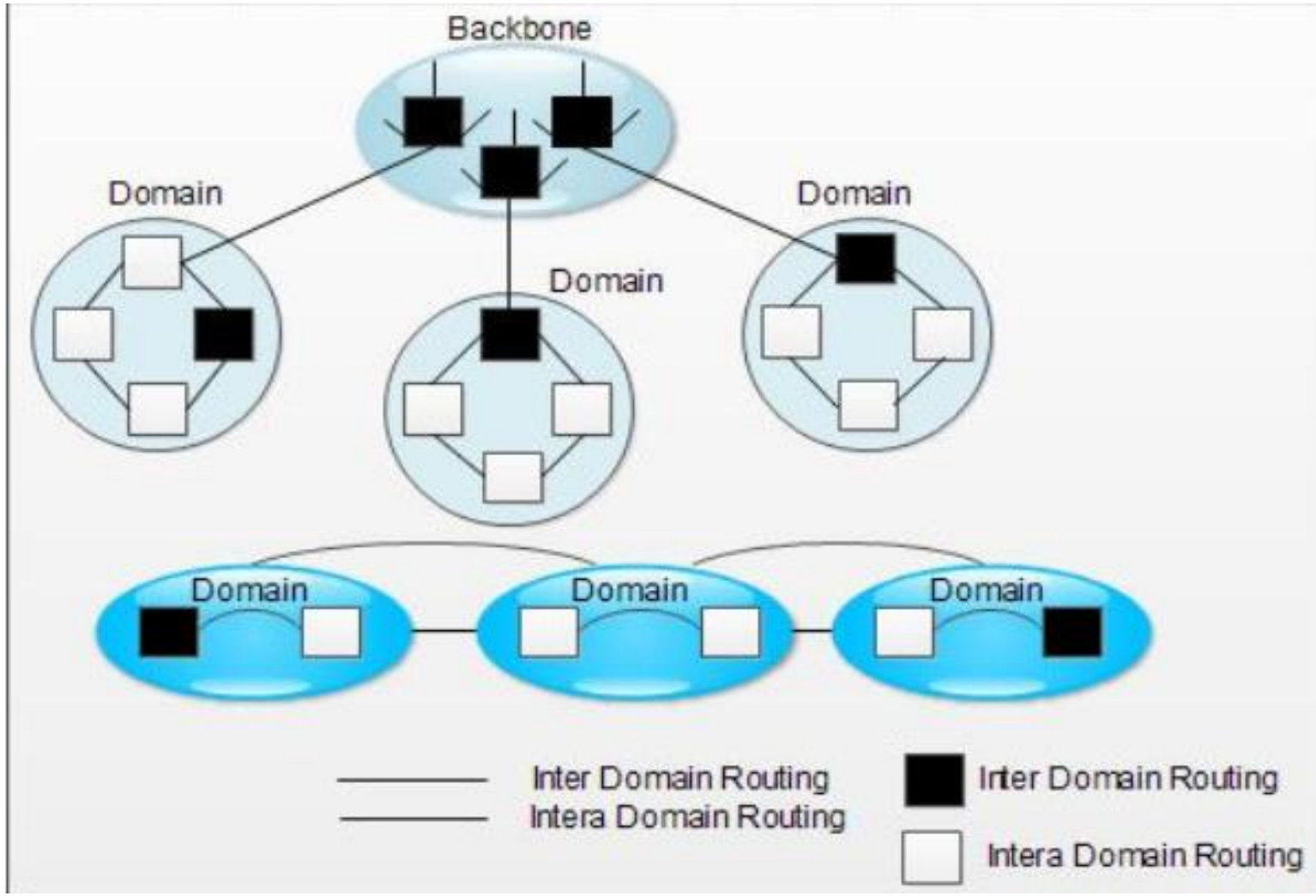
3. If a network uses little bandwidth; it quickly reacts to topology changes

4. All items in the database must be sent to neighbors to form link-state packets.

5. All neighbors must be trusted in the topology.

Hierarchical routing

The global nature of Internet system, it becomes more difficult to centralize the system management and operation. For this reason, the system must be hierarchical such that it is organized into multiple levels with several group loops connected with one another at each level. Therefore, hierarchical routing is commonly used for such a system.


Backbone
Domain
Domain
Domain
Domain
Domain
Domain
Inter Domain Routing
Intera Domain Routing
Inter Domain Routing
Intera Domain Routing

1. A set of networks interconnected by routers within a specific area using the same routing protocol is called domain.

2. Two or more domains may be further combined to form a higher-order domain.

3. A router within a specific domain is called intra-domain router. A router connecting domains is called inter-domain router.

4. A network composed of inter-domain routers is called backbone.

Routing protocol in such an Internet system can be broadly divided into two types:

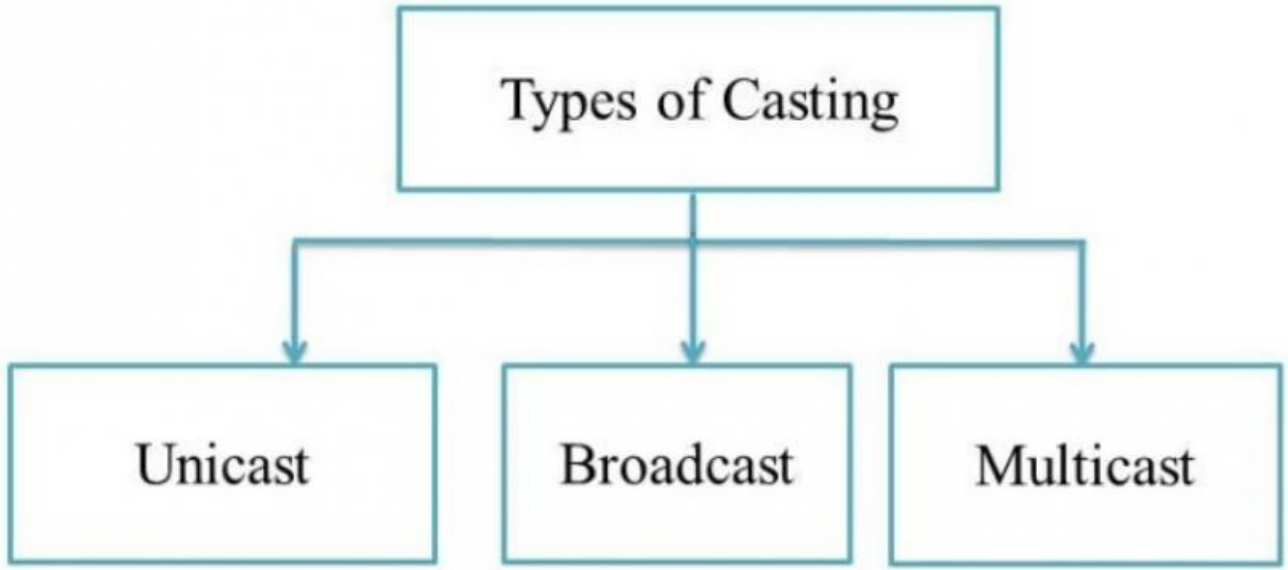
1.Intra-domain routing

2.Inter-domain routing

Each of these protocols is hierarchically organized. For communication within a domain, only the former routing is used. However, both of them are used for communication between two or more domains.

Unicast, Broadcast, and Multicast

Casting in computer networks means transmitting data (stream of packets) over a network.



Unicast Transmission (One-to-One)

- The data is transferred from a **single sender to a single receiver**.
- The network **switches hear the MAC addresses** of the devices on the networks to which they are connected.
- They can then forward packets only onto those networks containing devices with the connected MAC addresses.
- Unicast gradually becomes less efficient as more receivers need to see identical data.

Host A sends the IP address 11.1.2.2 data to the Host B IP address 20.12.4.3.

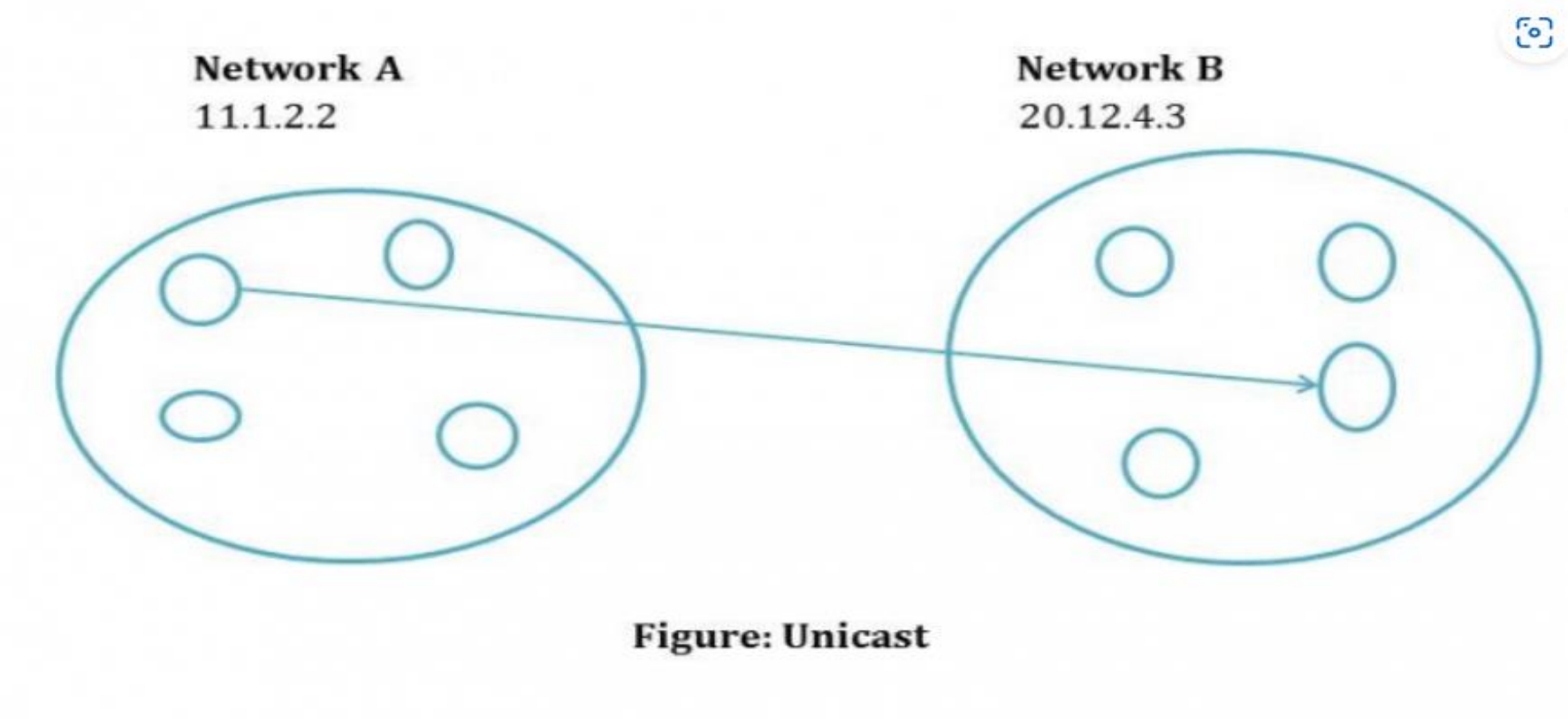


Figure: Unicast

Broadcast Transmission (One-to-All)

- In Broadcast transmission, the data is transmitted from one or more senders to all the receivers within the same network or in other networks.
- This type of transmission is useful in network management packets such as ARP (Address Resolution Protocol) and RIP (Routing Information Protocol) where all the devices must see the data.

Directed Broadcast

- Directed Broadcast transmits data from one source host to all the other hosts that exist in some other network.

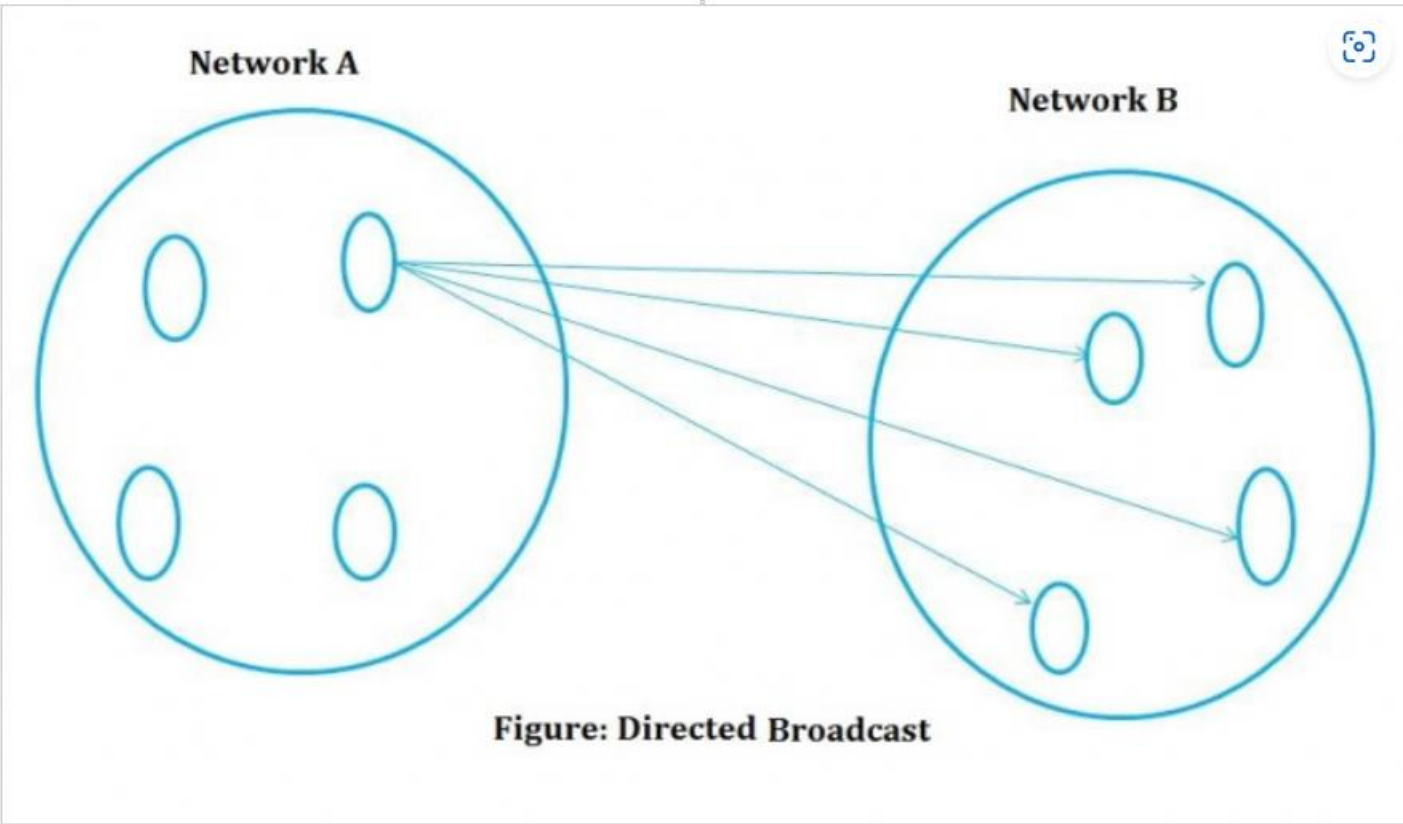


Figure: Directed Broadcast

Limited Broadcast

- In Limited Broadcast, the data is transmitted from a single source host to all the other hosts residing in the same network.

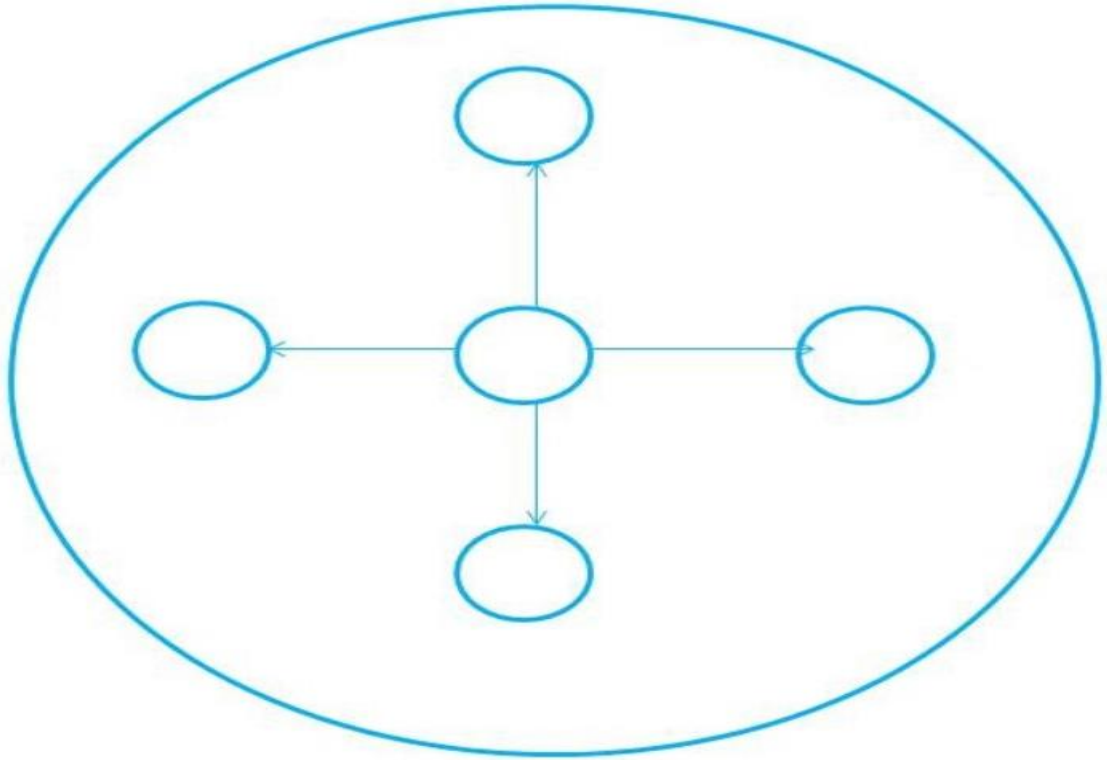


Figure: Limited Broadcast

Multicast Transmission (One-to-Many)

- When the data is transmitted from a single source host to a specific group of hosts having the interest to receive the data, it is known as multicast transmission.
- Multicast can be more efficient than unicast when different groups of receivers need to see the same data.
- **Example** – Multicast is the technique used in Internet streaming of video or audio teleconference, sending an email to a particular group of people, etc.

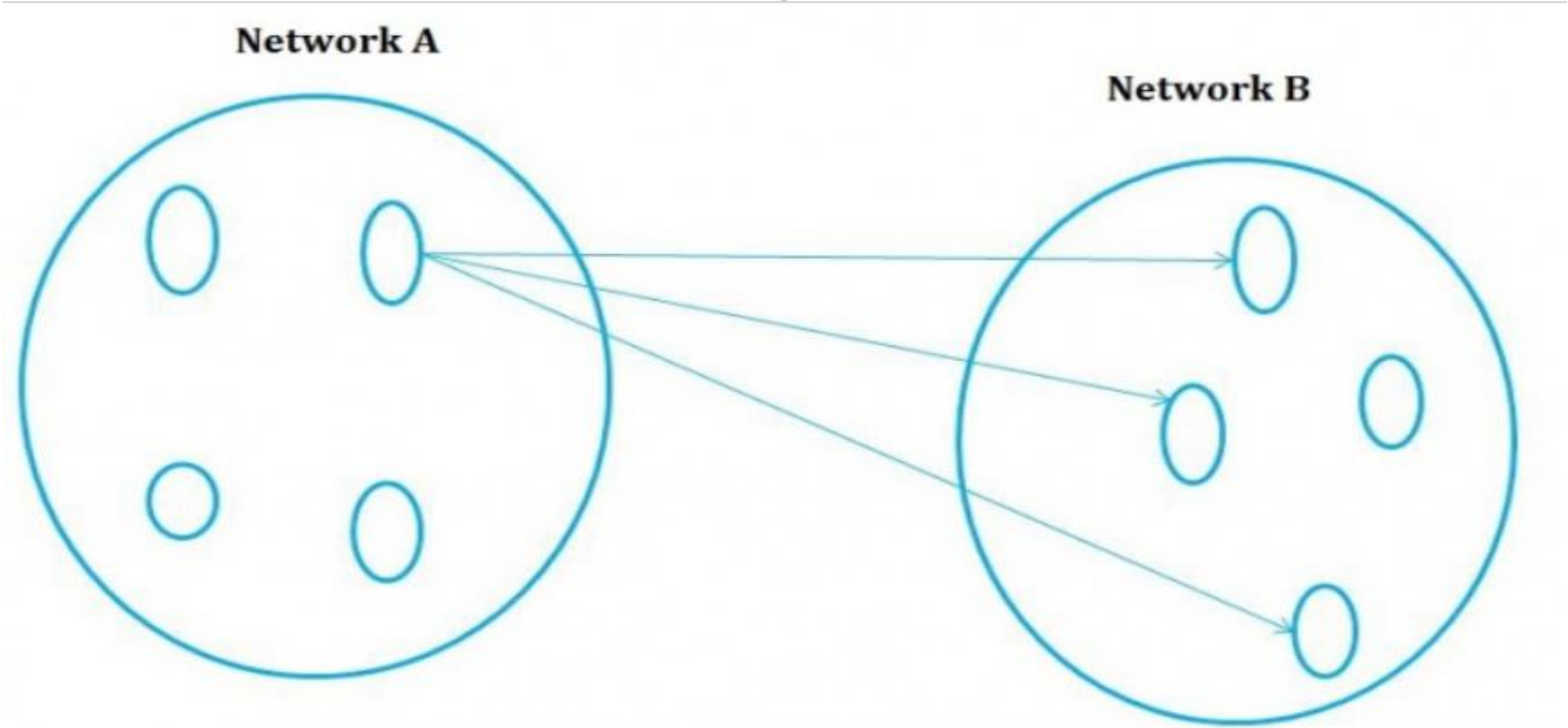


Figure: Multicast

Application Layer

Application Layer

- The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application.
- The application layer programs are based on client and servers.

The Application layer includes the following functions:

- **Identifying communication partners:** The application layer identifies the availability of communication partners for an application with data to transmit.
- **Determining resource availability:** The application layer determines whether sufficient network resources are available for the requested communication.
- **Synchronizing communication:** All the communications occur between the applications requires cooperation which is managed by an application layer.

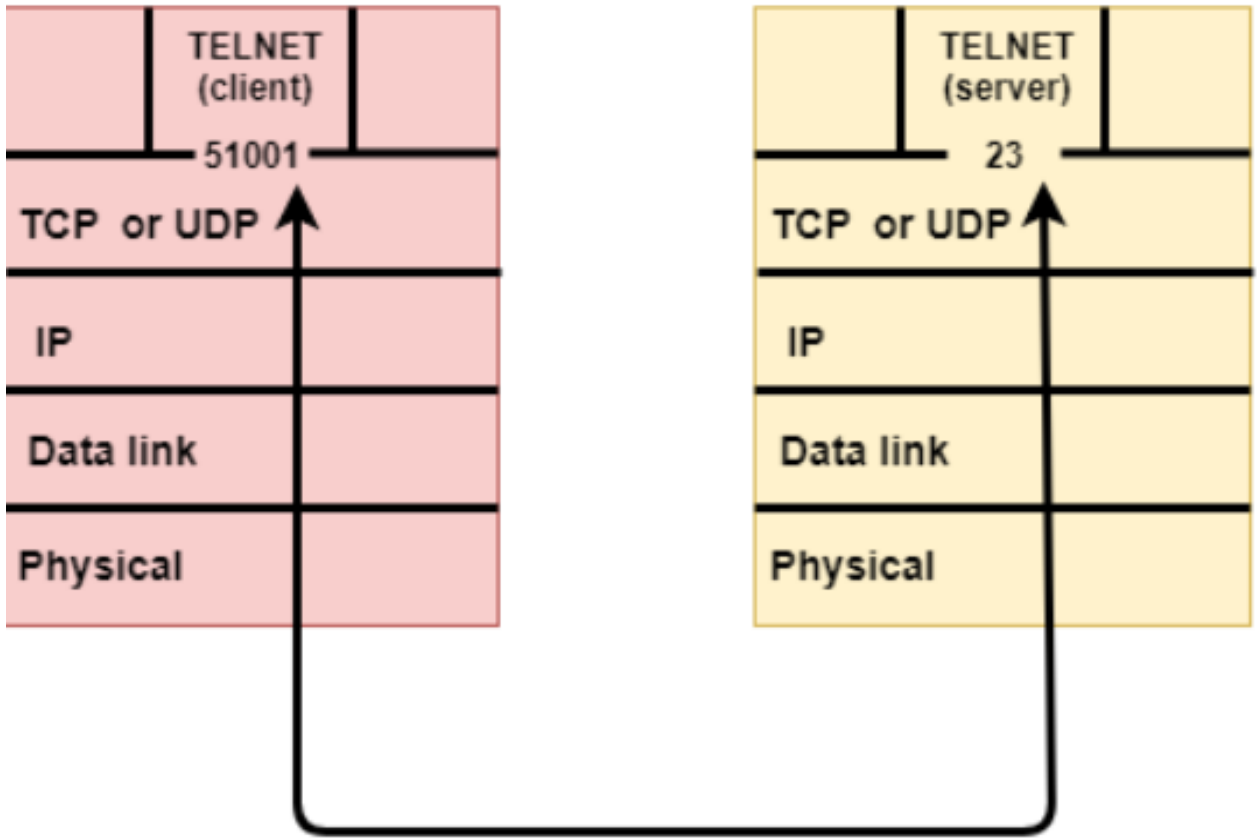
Services of Application Layers

- **Network Virtual terminal:** An application layer allows a user to ***log on to a remote host***. The user's computer talks to the software terminal, which in turn, talks to the host. The remote host thinks that it is communicating with one of its own terminals, so it allows the user to log on.
- **File Transfer, Access, and Management (FTAM):** An application allows a user to ***access files in a remote computer***, to retrieve files from a computer and to manage files in a remote computer.

- **Addressing:** To obtain communication between client and server, there is a need for addressing. When a client made a request to the server, the request contains the server address and its own address. The server response to the client request, the request contains the destination address, i.e., client address. To achieve this kind of addressing, DNS is used.
- **Mail Services:** An application layer provides Email forwarding and storage.
- **Directory Services:** An application contains a distributed database that provides access for global information about various objects and services.
- **Authentication**: It authenticates the sender or receiver's message or both.

Internet Transport Protocols

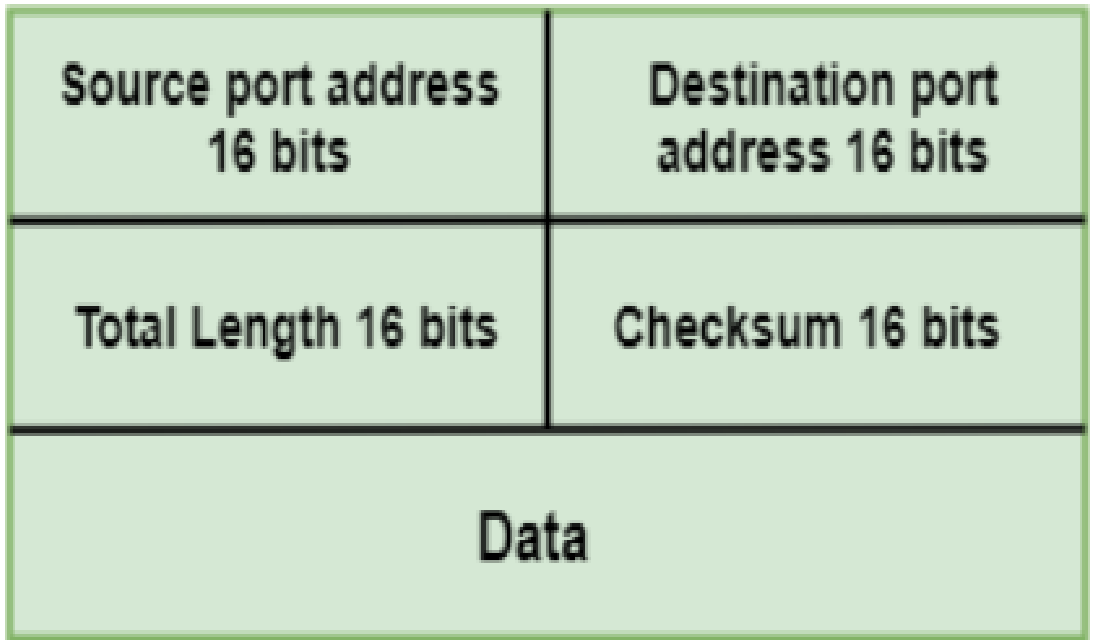
Transport Layer protocols



UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides **non sequenced transport functionality**.
- UDP is a **connectionless** protocol.
- This type of protocol is used when **reliability and security are less** important than speed and size.
- UDP is an end-to-end transport level protocol that adds **transport-level addresses, checksum error control, and length information to the data** from the upper layer.
- The packet produced by the UDP protocol is known as a **user datagram.**

User Datagram Format



- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- **Checksum:** The checksum is a 16-bit field which is used in error detection.

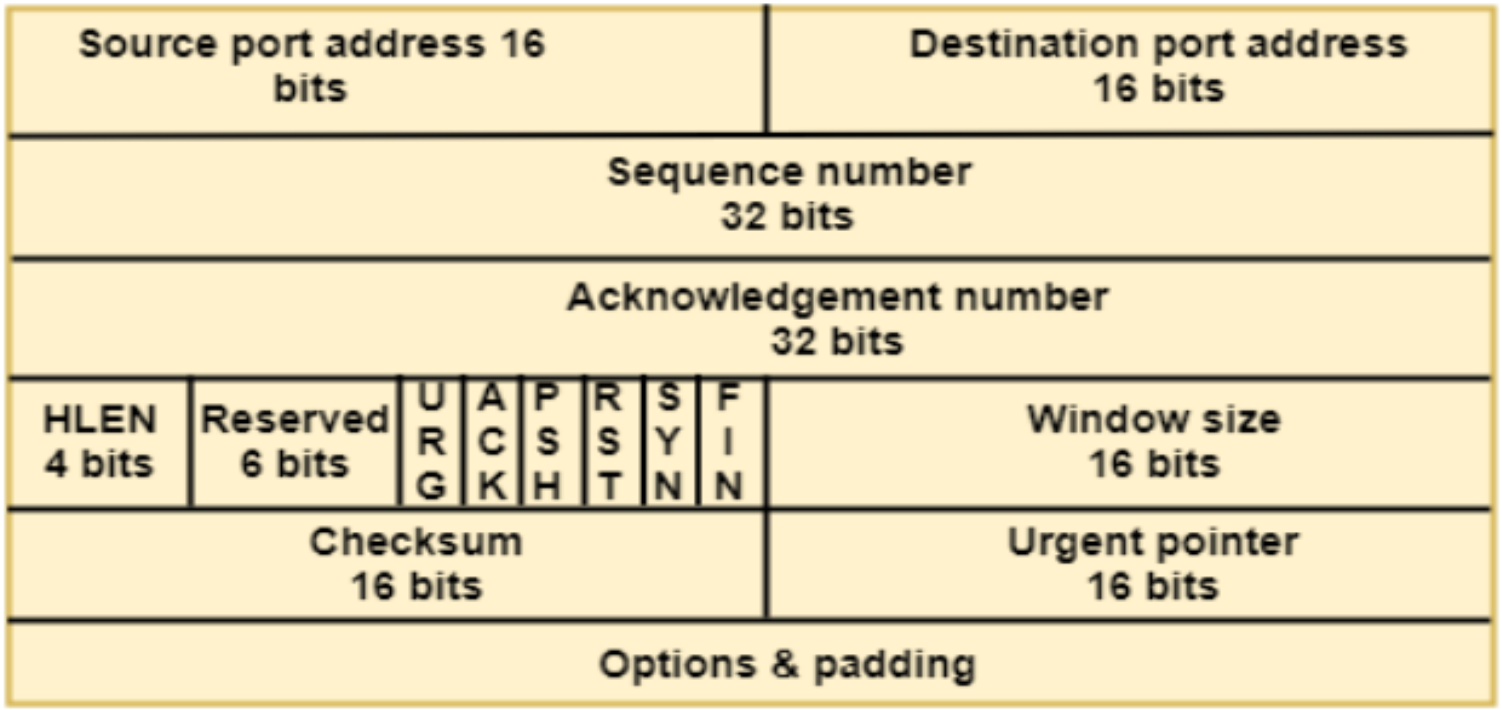
Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does **not provide any sequencing or reordering functions** and **does not specify the damaged packet** when reporting an error.
- UDP can **discover that an error has occurred**, but it does **not specify which packet has been lost** as it does not contain an ID or sequencing number of a particular data segment.

TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a **connection-oriented protocol** means the connection established between both the ends of the transmission. For creating the connection, TCP generates a **virtual circuit** between sender and receiver for the duration of a transmission.

TCP Segment Format



- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.

- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

Elements of Transport Protocols

Elements of Transport Protocols

- To establish a reliable service between **two machines on a network**, transport protocols are implemented.
- The major difference lies in the fact that the **data link layer** uses a **physical channel** between two routers while the **transport layer uses a subnet**.

Error Control

- **Error detection and error recovery** are an integral part of reliable service, and therefore they are necessary to perform error control mechanisms on an end-to-end basis.
- To control errors from lost or duplicate segments, the transport layer enables **unique segment sequence numbers to the different packets** of the message, **creating virtual circuits**, allowing only **one virtual circuit per session**.

Flow Control

- Flow control is to maintain a **synergy between a fast process and a slow process**.
- **Acknowledgements** are sent back to manage end-to-end flow control.
- **Go back N algorithms** are used to request retransmission of packets starting with packet number.
- **Selective Repeat** is used to request specific packets to be retransmitted.

Multiplexing/De multiplexing

- The transport layer **establishes a separate network connection** for each transport connection required by the session layer.
- **To improve throughput**, the transport layer establishes **multiple network connections**.
- When the issue of throughput is not important, it **multiplexes several transport connections onto the same network** connection, thus reducing the cost of establishing and maintaining the network connections.

- When several connections are multiplexed, they call for **demultiplexing at the receiving end**.
- In the case of the transport layer, the **communication takes place only between two processes** and not between two machines.
- Hence, communication at the transport layer is also known as **peer-to-peer or process-to-process communication**.

Fragmentation and re-assembly

- When the transport layer receives a large message from the session layer, it **breaks the message into smaller units** depending upon the requirement. This process is called fragmentation.
- Thereafter, it is passed to the network layer. Conversely, when the **transport layer acts as the receiving process, it reorders the pieces of a message** before reassembling them into a message.

Addressing

- Transport Layer deals with addressing or **labelling a frame**.
- It also differentiates between a **connection and a transaction**. Connection identifiers are **ports or sockets** that **label each frame**, so the receiving device knows which process it has been sent from. This helps in keeping **track of multiple-message conversations**. Ports or sockets address multiple conservations in the **same location**.

Domain Name System

Domain Name System

- The acronym for Domain Name System is DNS.
- It is a phonebook for computers on the Internet.
- It translates and maps alphabetic domain names (websites' web addresses or names) to the numeric Internet Protocol (IP) addresses of computers or servers. And it also does the reverse process.

- Computers or technically the routers (default gateway) use DNS servers to contact to get any domains translated and converted to an IP address of the server hosting a website.
- The entry for DNS servers could be few or many, as there would be multiple DNS servers. The examples are **OpenDNS servers, or Google DNS servers**.

- It translates and maps alphabetic domain names (websites' web addresses or names) to the numeric Internet Protocol (IP) addresses of computers or servers. And it also does the reverse process.
- It is a system that uses at least one DNS server to resolve DNS-names.

- DNS is used because computers and servers do not understand human-readable alphabetic domain names, where humans do not understand and remember numeric IP addresses, which the computers and servers can.

Example

Domain name = www.example.com whose Server IP address is,

```
say = 253.136.27.2
```

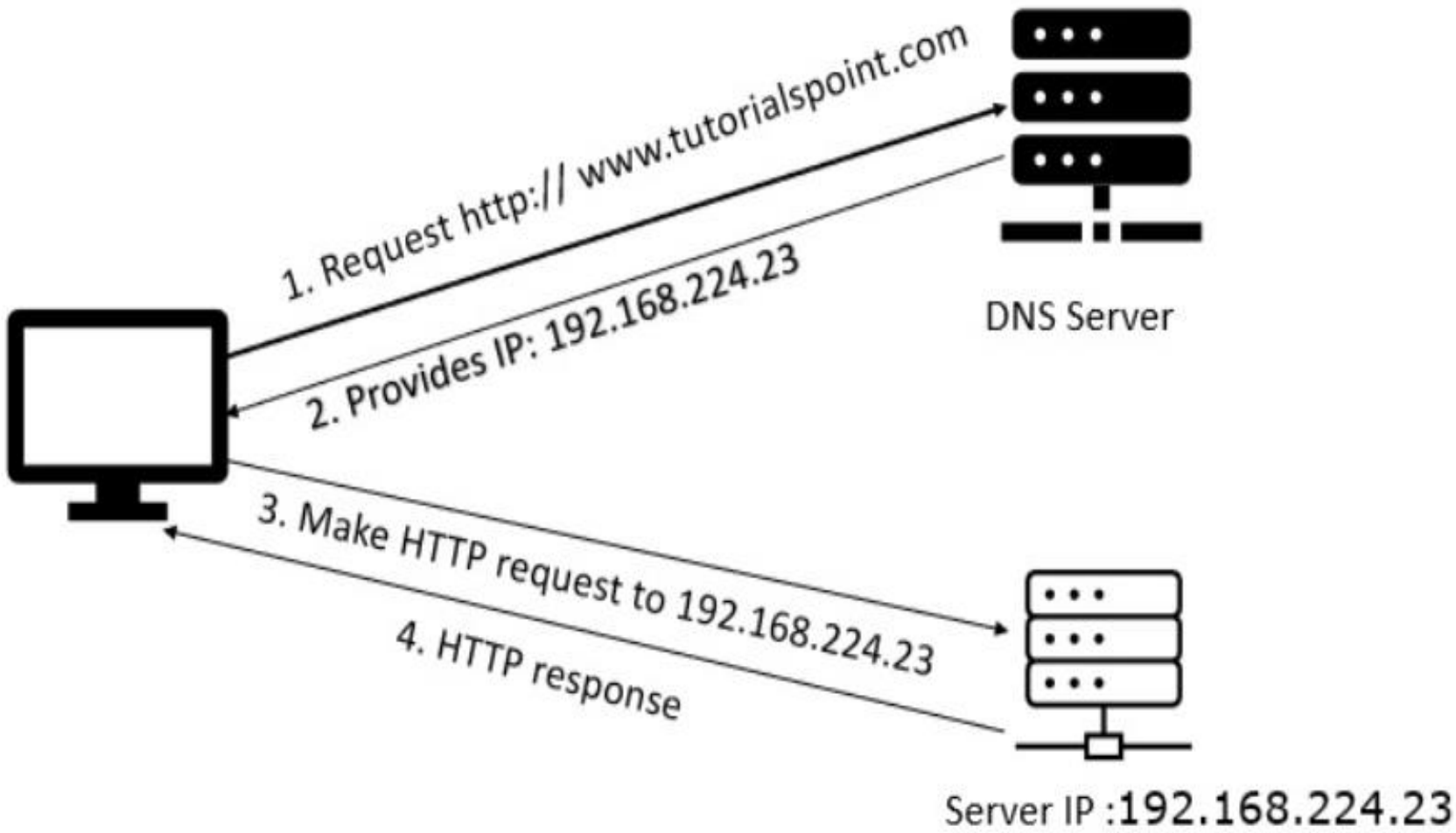
Working of DNS

Step 1 – Every website has a domain name/ IP address associated with it.

Step 2 – Now IP is a bit complicated to share (as no one wants to write 192.168.224.23 or some random IP to access google.com) so people came up with an idea of domain names which basically stores the IP address mapped to their name.

Step 3 – Now, a DNS translates every domain name to its IP address so every browser can access that particular website.

Step 4 – DNS has eased the process of web surfing as we write google.com to reach a website instead of some complicated 32-128 bit address.


1. Request http:// www.tutorialspoint.com
2. Provides IP: 192.168.224.23
DNS Server
3. Make HTTP request to 192.168.224.23
4. HTTP response
Server IP :192.168.224.23

Electronic Mail

Electronic Mail

- **Electronic Mail** (e-mail) is one of most widely used services of Internet.
- This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world.
- Message in mail not only contain text, but it also contains images, audio and videos data.
- The person who is sending mail is called **sender** and person who receives mail is called **recipient**.
- It is just like postal mail service.

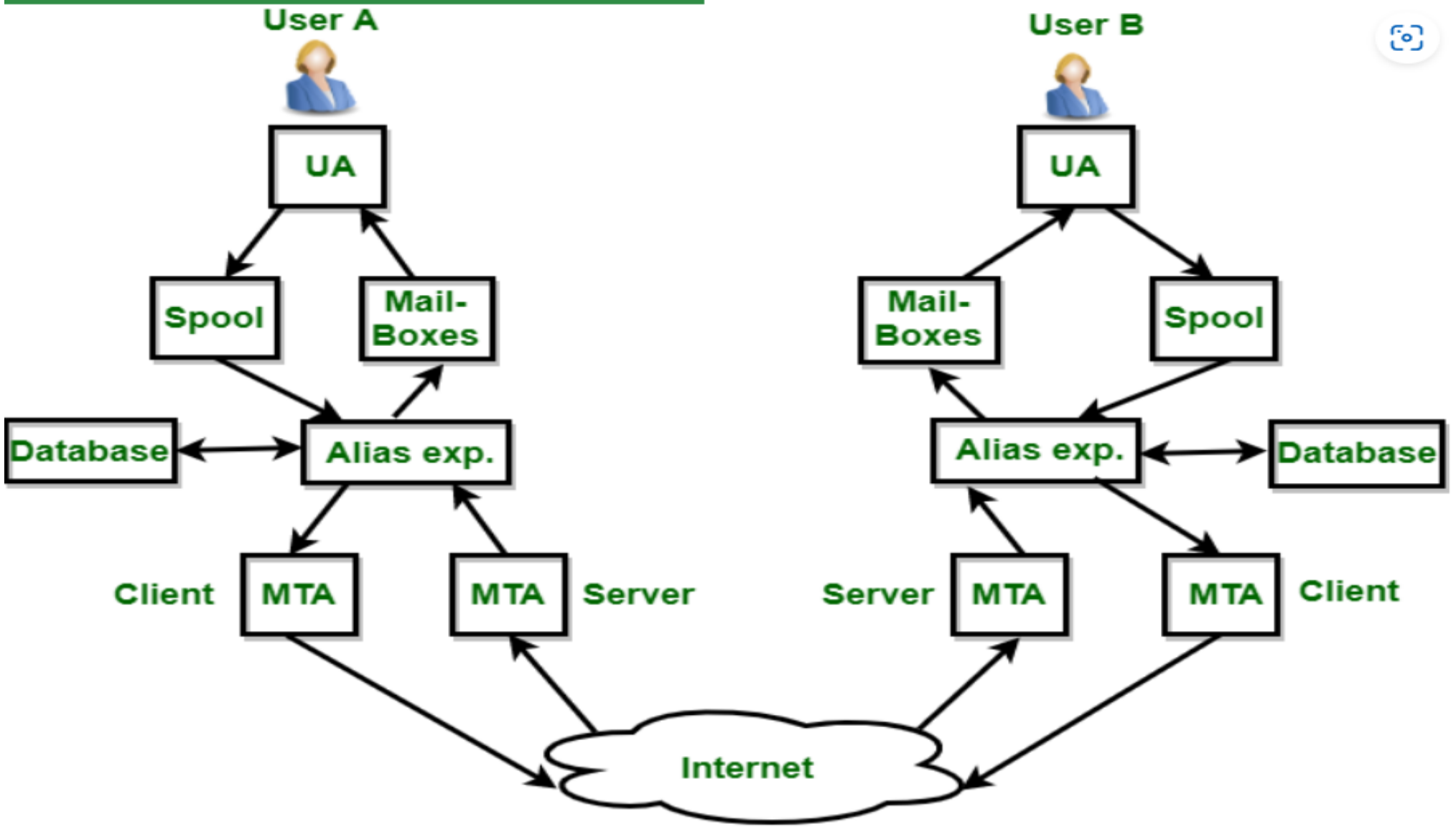
Components of E-Mail System :

- The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file.

1. User Agent (UA) : The UA is normally a **program** which is used to **send and receive mail**. Sometimes, it is called as mail reader. It accepts variety of **commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes**.

2. Message Transfer Agent (MTA) : MTA is actually responsible for **transfer of mail from one system to another**. To send a mail, a system must have **client MTA and system MTA**.

- It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine.
- The delivery from one MTA to another MTA is done by **Simple Mail Transfer Protocol**.


User A
User B
UA
UA
Spool
Mail-
Boxes
Mail-
Boxes
Spool
Database
Alias exp.
Alias exp.
Database
Client
MTA
MTA
Server
Server
MTA
MTA
Client
Internet

3. Mailbox :

- It is a **file on local hard drive to collect mails**.
- Delivered mails are present in this file.
- The user can read it delete it according to his/her requirement.
- To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.

4. Spool file :

- This file contains **mails that are to be sent**.
- User agent **appends** outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery.
- E-mail allows one name, an **alias**, to represent several different e-mail addresses. It is known as **mailing list**, Whenever user have to sent a message, system checks recipient's name against alias database.
- If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA.

Services provided by E-mail system

Composition – The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.

Transfer – Transfer means sending procedure of mail i.e. from the sender to recipient.

Reporting – Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.

Displaying – It refers to present mail in form that is understand by the user.

Disposition – This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.