

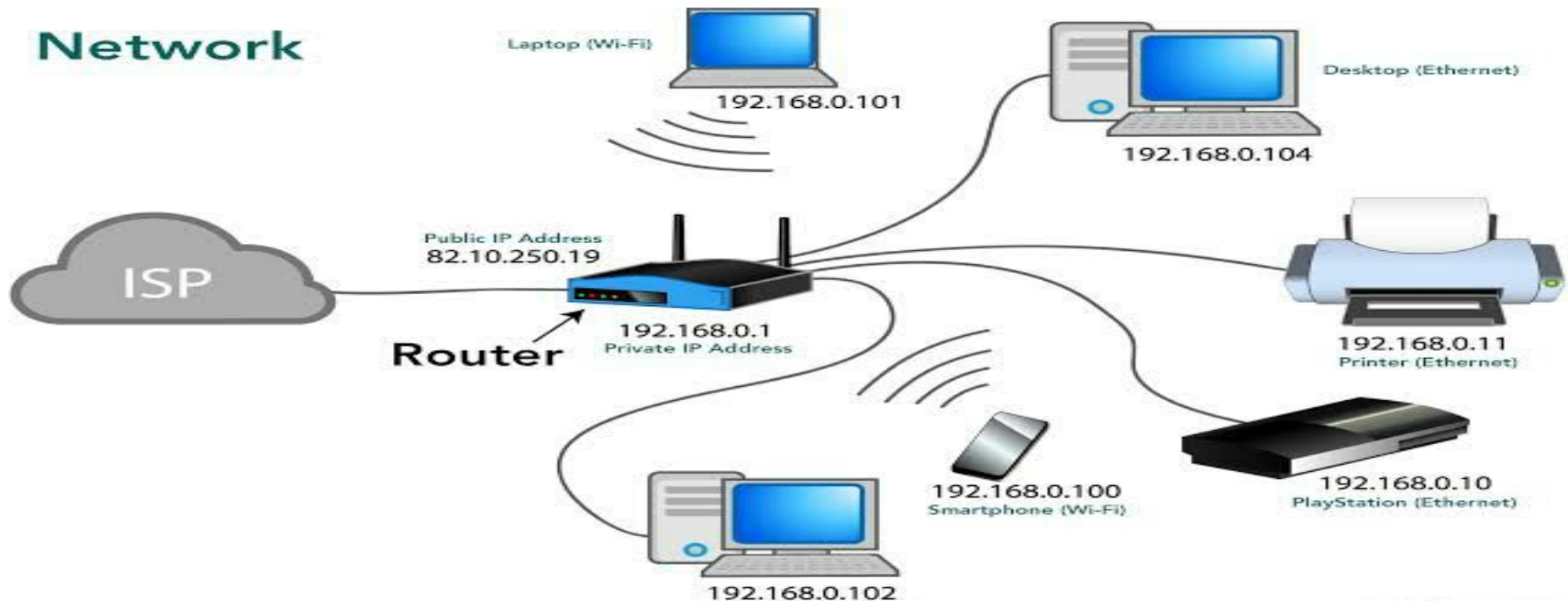


# Computer Network and Network Design

## Unit 1- Introduction

# Networks :

A “**network**” is a set of devices connected by a media links. A “**node**” can be a Computer, Printer, or any other device capable of sending and / or receiving data generated by other nodes on the network. The links connecting the devices are often called communication channels.



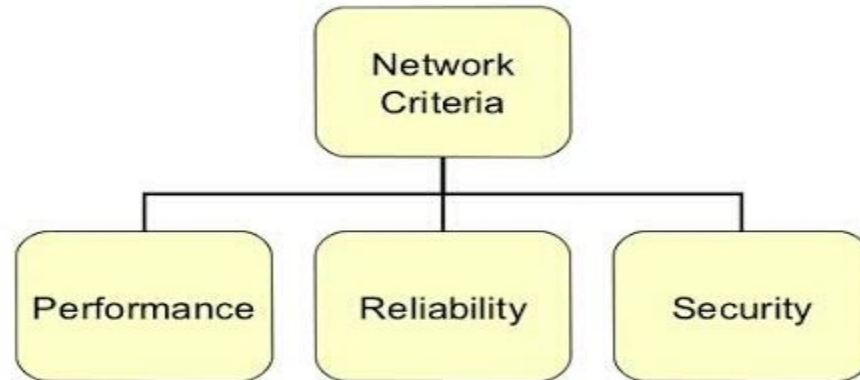
## Networks :

- Networks use “distributed processing”, in which a task is divided among multiple computers.
- Instead of a single large machine being responsible for all aspects of a process, each separate computer (usually a personal computer or workstation) handles a subset.
- Networks follow protocols, which define how communications are sent and received.

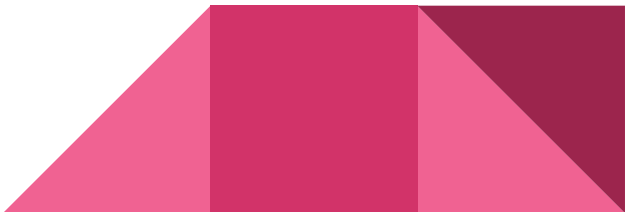


## Network Criteria :

A network must be able to meet certain number of criteria. Because it helps to improve network functionality. The most important are Performance, Reliability and Security.



# Performance:

- Performance can be measured in many ways, including transit time and response time.
  - Transit time is the amount of time required for a message to travel from one device to another.
  - Response time is the elapsed time between an inquiry and a response.
  - The performance of a network depends on a number of factors, including:
    - The number of users
    - The type of transmission medium
    - Connected hardware
    - Software
- 

# Reliability:

- It is the degree to which a network is **trustworthy, consistent**, and **dependable**.
- The Reliability of a network is measured by the frequency of failures it is undergoing and the time it takes to recover from the failures.
- Overall, the **Robustness of the Network** at times of catastrophic events is measured to check how reliable the Network is.
- “**Catastrophe**” – Network must be protected from catastrophic events such as fire, earthquake, or theft.



# Security:

- Network security issues include protecting data from unauthorised access and viruses.
- Protection can be accomplished at a number of levels. At the lowest level are user identification codes and password. At a higher level are encryption techniques.
- Network is accessible from many points, it can be susceptible to computer viruses.



# Network Physical Structures

There are two possible connection types when it comes to Networks

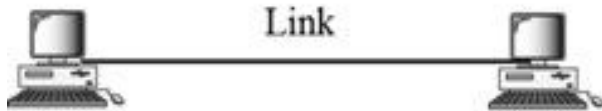
- **Point-to-point connections** – provides a dedicated link or between two devices.
- The entire capacity of the link is reserved for transmission between those two devices.
- Most point-to-point connections use an actual length of wire or cable to connect the two ends, but microwave or satellite links, are also possible.
- Changing the T.V with a remote is a point-to-point connection between the remote control and the television.



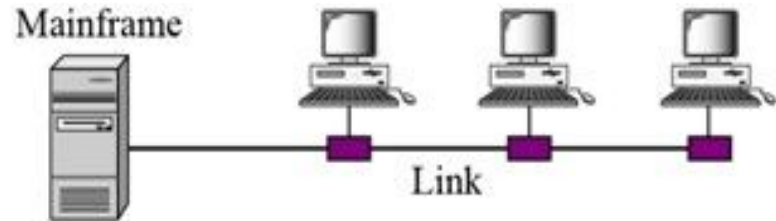


# Network Physical Structures

- **Multipoint connections** – more than two devices are sharing a link The entire capacity of the link is either shared spatially or temporally.
- This means either every computer shares a specific space of the link or each computer shares the link for a specific time when being used.



a. Point-to-point



b. Multipoint

# What is Network Topology?

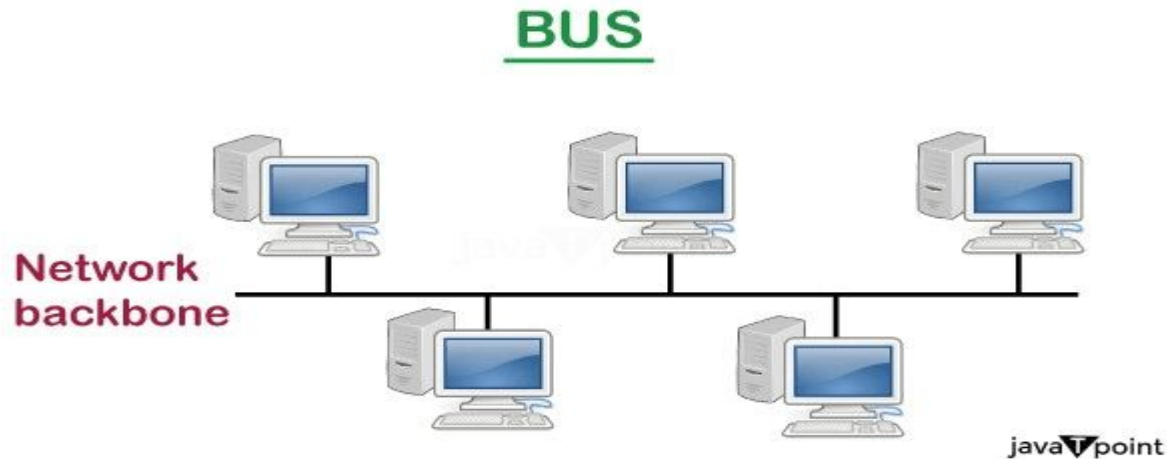
Topology defines the structure of the network of how all the components are interconnected to each other.

There are some basic topologies given:



## Bus topology-

Bus topology- use multipoint link. One long cable, called the bus acts as a backbone to link all the devices in a network.



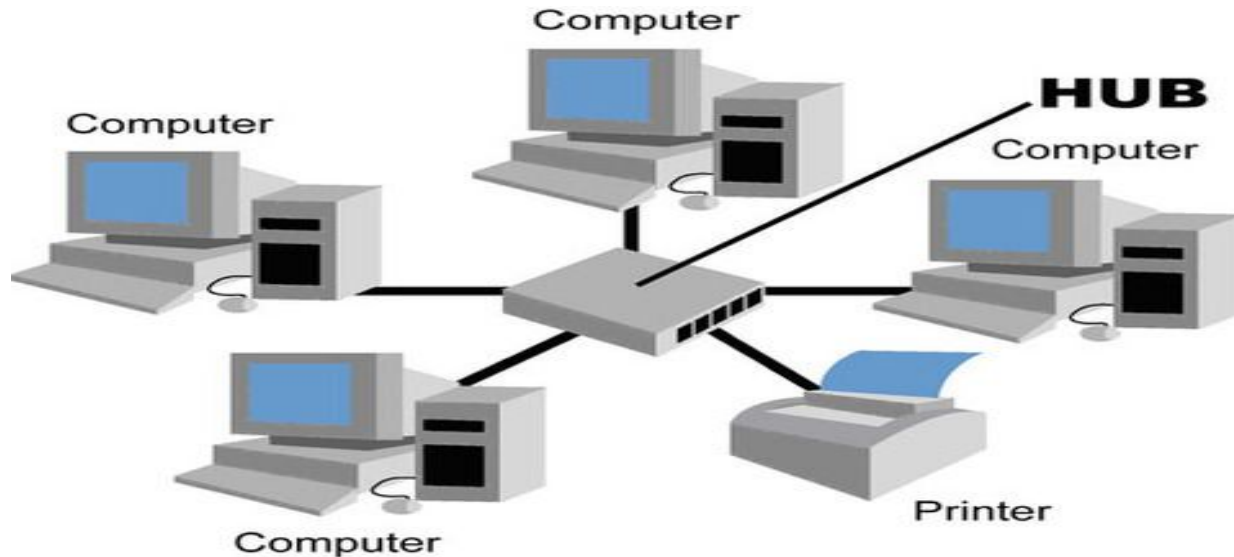
## Ring topology-

Ring topology- each device has a dedicated point-to-point connection with only the two devices on either side of it.



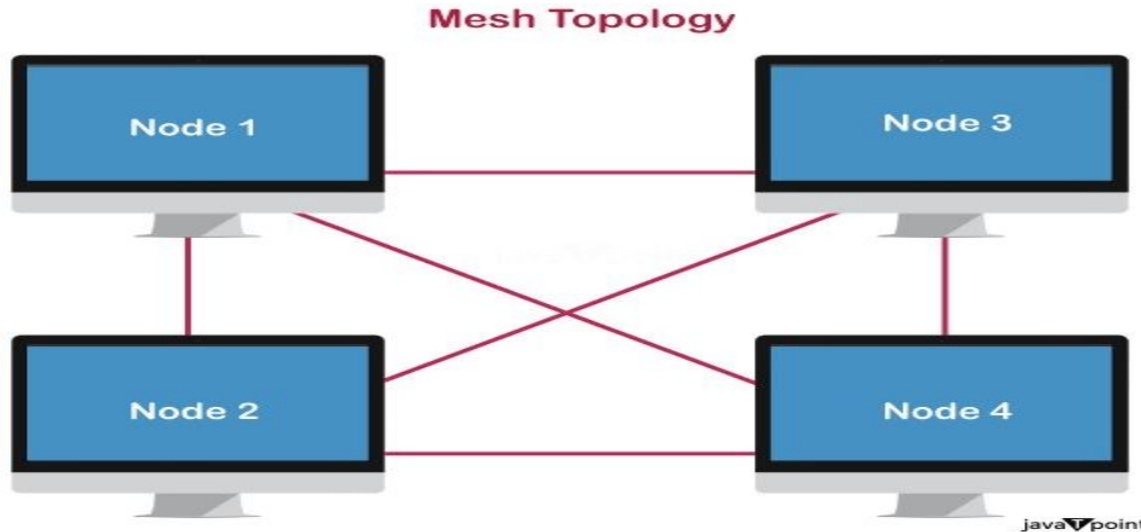
## Star topology-

Star topology- each device has a dedicated point-to-point link only to a central controller, called a hub.



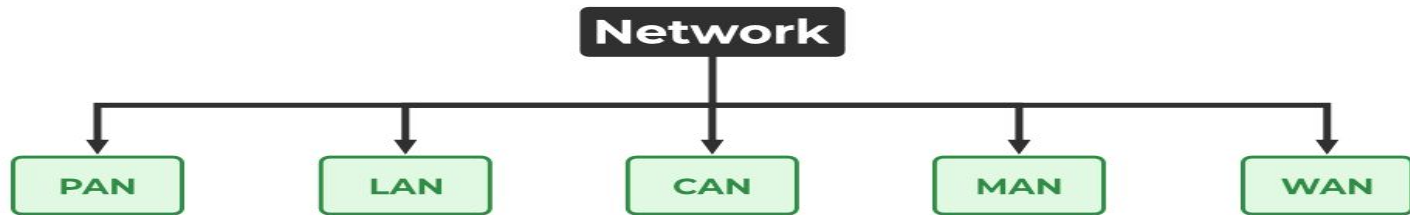
## Mesh topology-

Mesh topology- every device has a dedicated point-to-point link to every other device.



# Computer Network Types

- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- A computer network can be categorized by their size.




## LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Ne
- Local Area Network provides higher security.

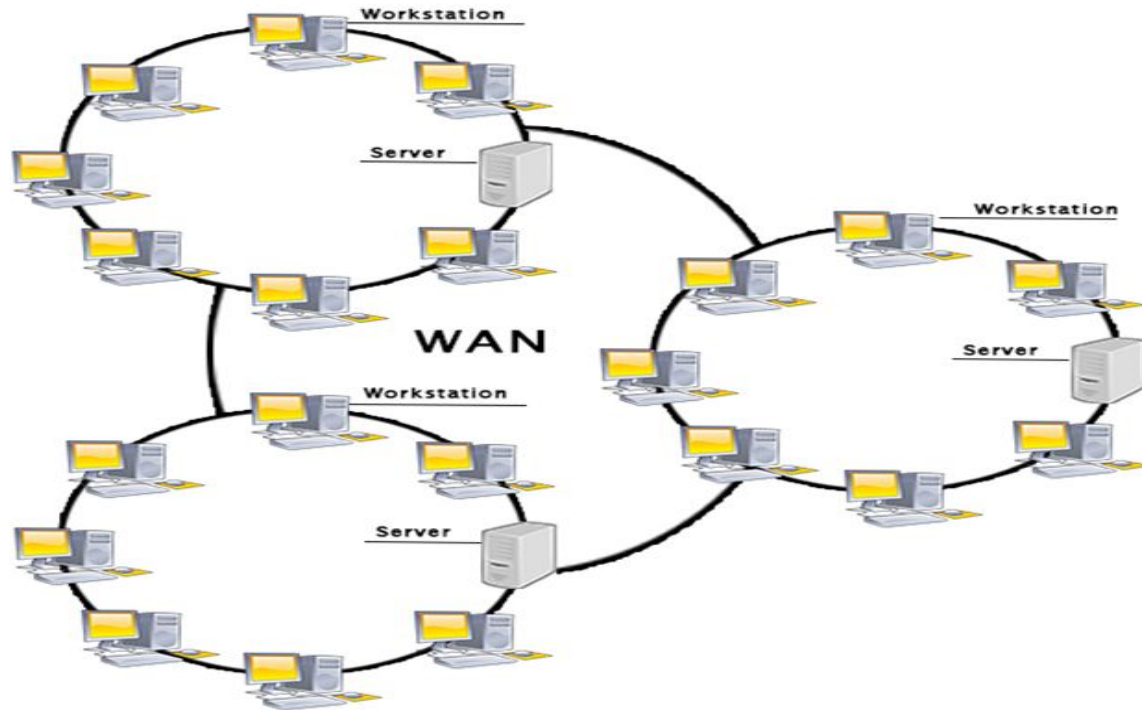




## WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
  - A Wide Area Network is quite bigger network than the LAN.
  - A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
  - The internet is one of the biggest WAN in the world.
  - A Wide Area Network is widely used in the field of Business, government, and education.
- 

# WAN(Wide Area Network)



# Switching:

- An internet is a **switched network** in which a switch connects at least two links together.
- A switch needs to forward data from a link to another link when required.
- The two most common types of switched networks are: **Circuit Switching** and **Packet Switching**.



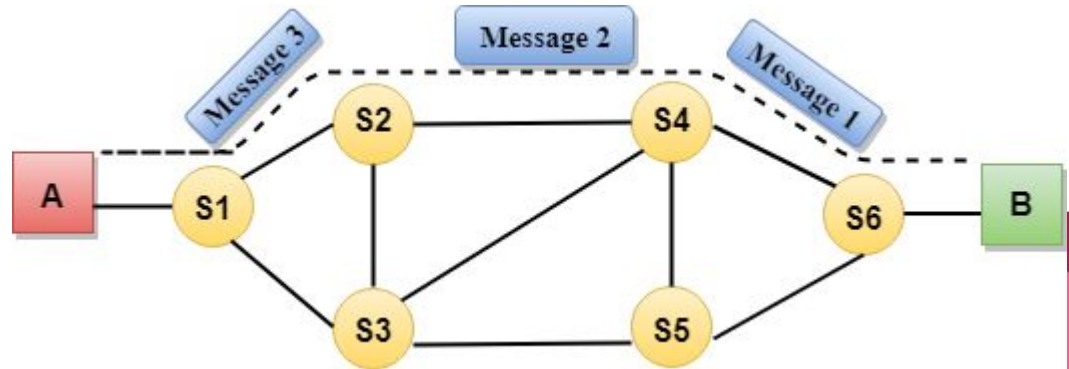
# Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, 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.
- A complete end-to-end path must exist before the communication takes place.
- In case of 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.
- Fixed data can be transferred at a time in circuit switching technology.

# Circuit Switching

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



# Circuit Switching


## Advantages Of Circuit Switching:

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

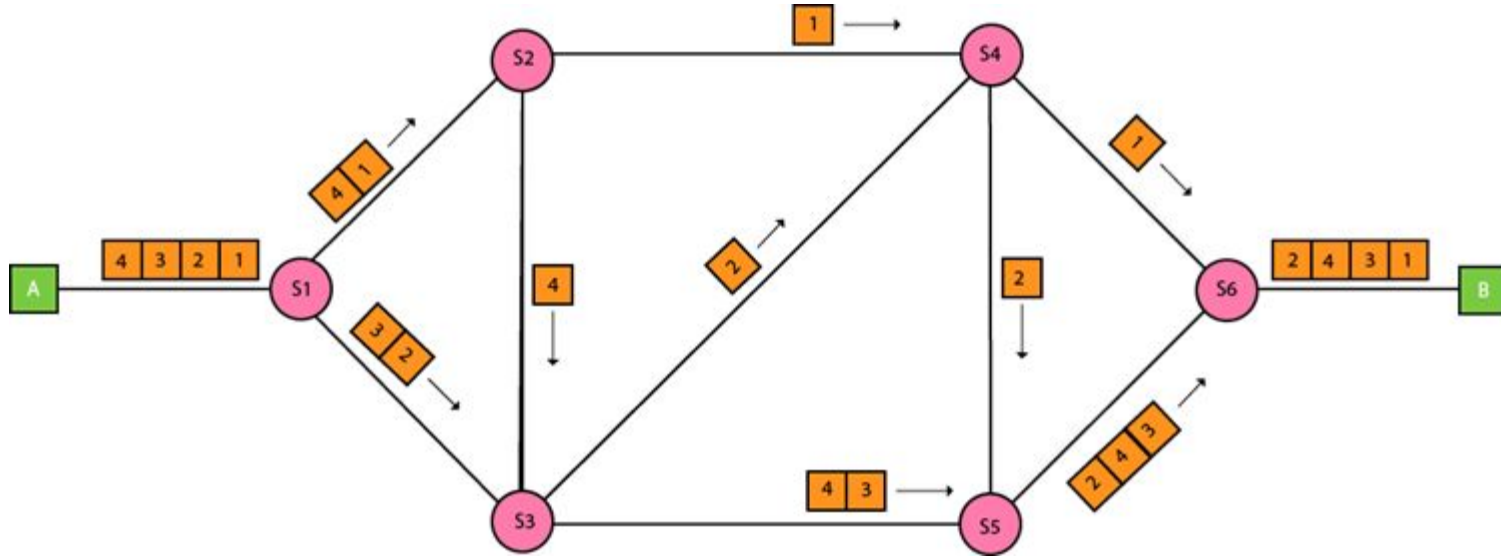
## Disadvantages Of Circuit Switching:

- 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.

# 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





# Packet Switching

## Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. 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.




# Packet Switching

## Disadvantages Of Packet Switching:

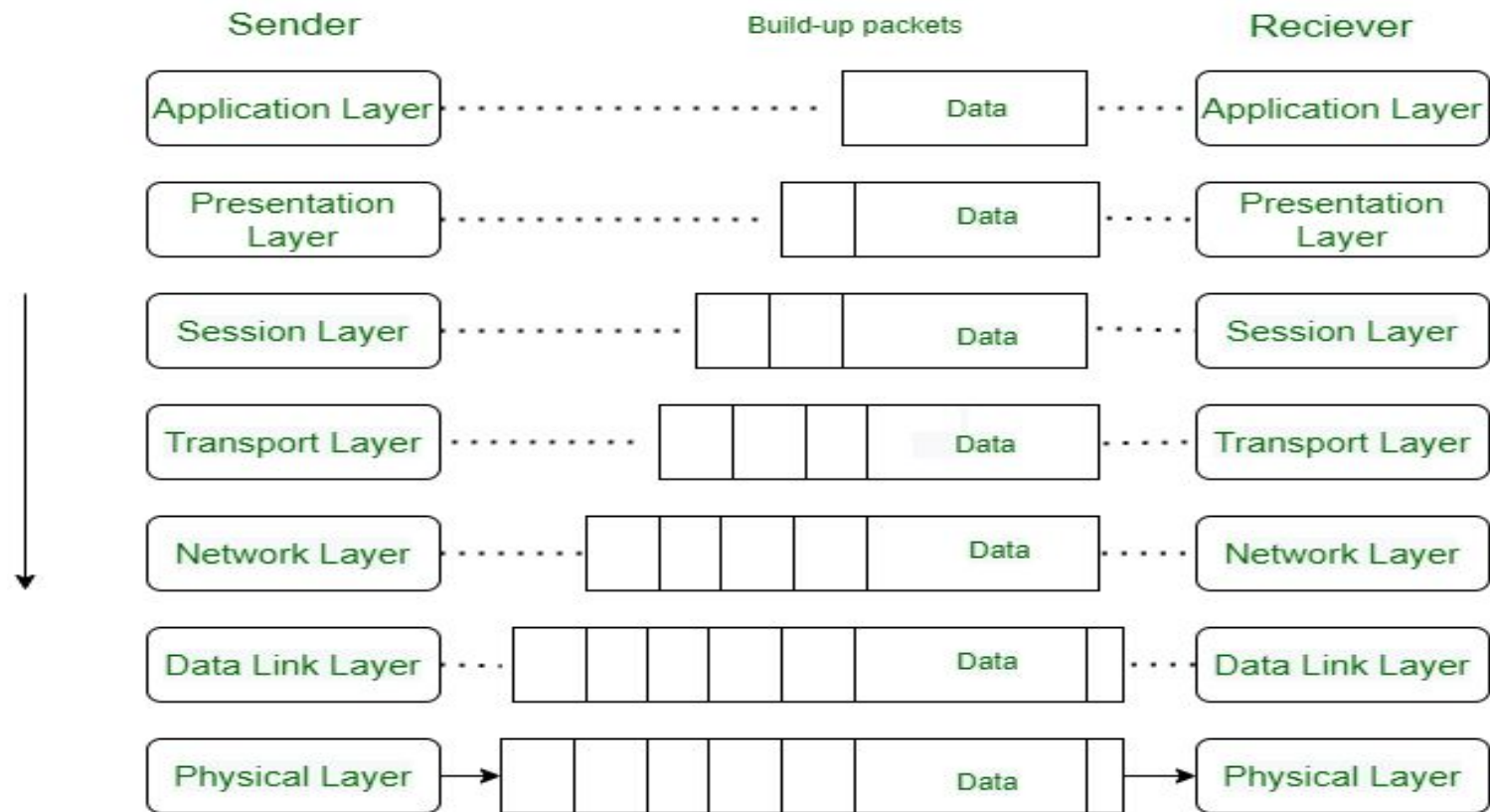
- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission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



# The OSI Model:

- OSI stands for Open Systems Interconnection.
  - It was developed by ISO – ‘International Organization for Standardization’, in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform.
  - All these 7 layers work collaboratively to transmit the data from one person to another across the globe.
  - The OSI model, created in 1984 by ISO, is a reference framework that explains the process of transmitting data between computers.
  - It is divided into seven layers that work together to carry out specialised network functions, allowing for a more systematic approach to networking.
- 

# The OSI Model:



# Layers of the OSI Model:

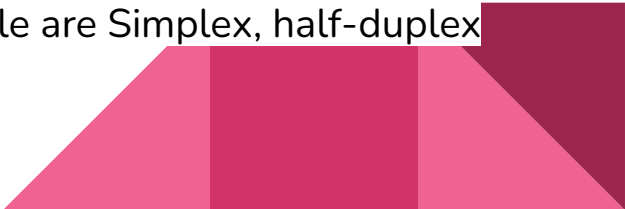
## Physical Layer – Layer 1

- The lowest layer of the OSI reference model is the physical layer.
- It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of **bits**.
- It is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



# Layers of the OSI Model:

## Functions of the Physical Layer

- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
  - **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
  - **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
  - **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.
- 

# Layers of the OSI Model:

## Data Link Layer (DLL) – Layer 2


The data link layer is responsible for the node-to-node delivery of the message.

The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.



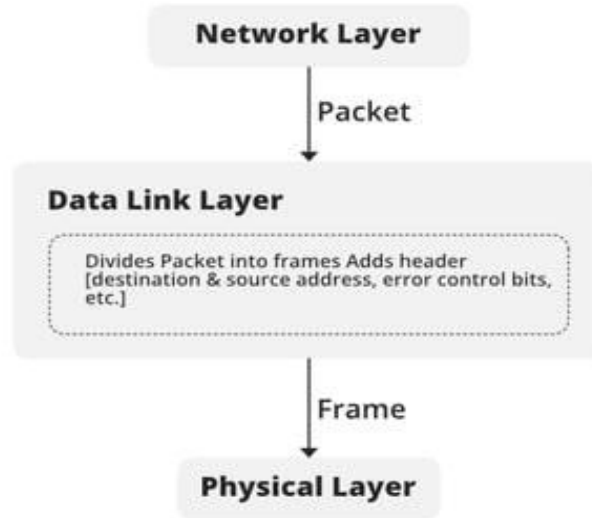
# Layers of the OSI Model:

## Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
  - **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
  - **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
  - **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- 



## Layers of the OSI Model:




# Layers of the OSI Model:

## Network Layer – Layer 3

- The network layer works for the transmission of data from one host to the other located in different networks.
- It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP addresses are placed in the header by the network layer.

## Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
  - **Logical Addressing:** To identify each device on Internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.
- 

# Layers of the OSI Model:

## Transport Layer – Layer 4

- The transport layer provides services to the session layer and takes services from the network layer.
- The data in the transport layer is referred to as *Segments*.
- It is responsible for the End to End Delivery of the complete message.
- The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.
- **At the sender's side:** The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.



# Layers of the OSI Model:

## Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

## Services Provided by Transport Layer

1. Connection-Oriented Service
2. Connectionless Service



# Layers of the OSI Model:

1. **Connection-Oriented Service:** It is a three-phase process that includes
  - Connection Establishment
  - Data Transfer
  - Termination/disconnection

In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

**2. Connectionless service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.




# Layers of the OSI Model:

## session Layer – Layer 5

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

### Functions of the Session Layer


- **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
  - **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
  - **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.
- 

# Layers of the OSI Model:

## Presentation Layer – Layer 6

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

### Functions of the Presentation Layer

- **Translation:** For example, ASCII to EBCDIC.
  - **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
  - **Compression:** Reduces the number of bits that need to be transmitted on the network.
- 

# Layers of the OSI Model:

## Application Layer – Layer 7

- At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications.
- These applications produce the data, which has to be transferred over the network.
- This layer also serves as a window for the application services to access the network and for displaying the received information to the user.





# Layers of the OSI Model:

## Functions of the Application Layer

The main functions of application layer are given below.

- Network Virtual Terminal: It allows a user to log on to a remote host.
- FTAM- File transfer access and management : This application allows a user to access file in a remote host, retrieve files in remote host and manage or control files from a remote computer.
- Mail Services : Provide email service.
- Directory Services : This application provides distributed database sources and access for global information about various objects and services.



# TCP/IP suite

- The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- **TCP/IP** was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.
- The number of layers is sometimes referred to as five or four. Here, we'll study five layers. The Physical Layer and Data Link Layer are referred to as one single layer as the 'Physical Layer' or 'Network Interface Layer' in the 4-layer reference.



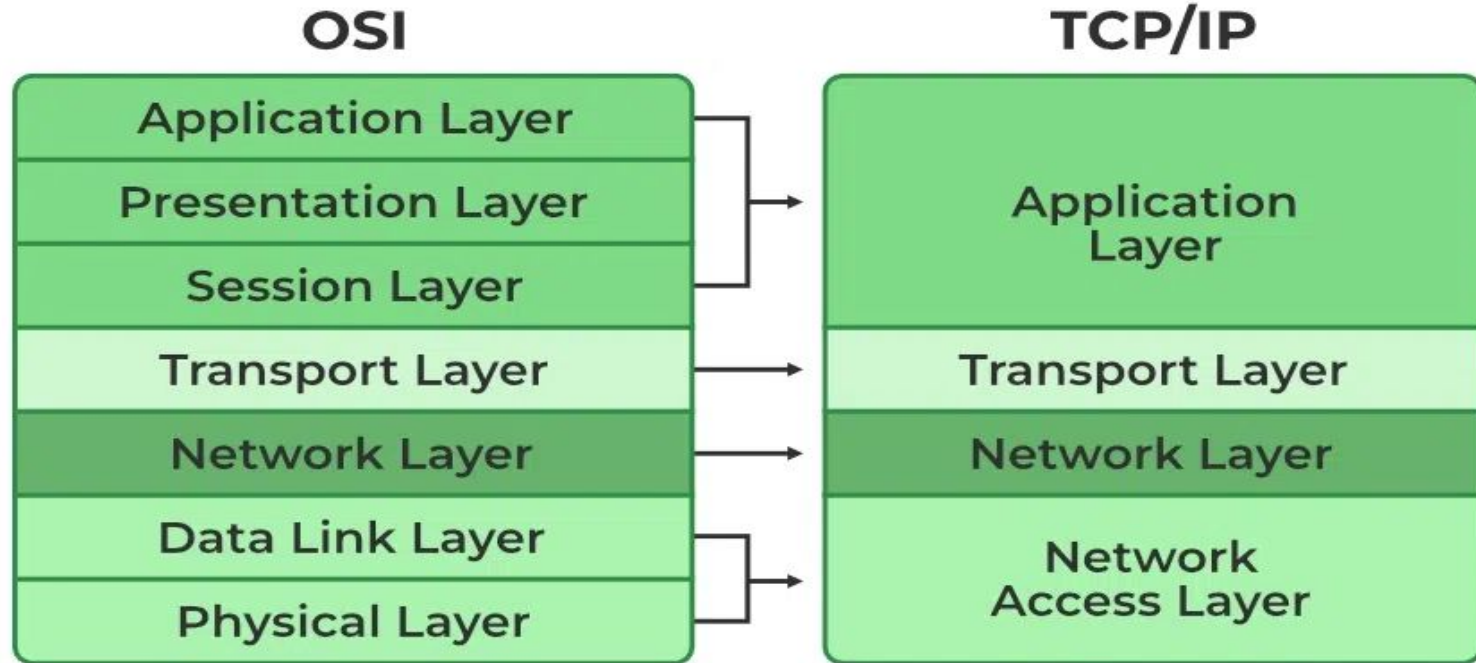
# TCP/IP suite

## Layers of TCP/IP Model

1. Application Layer
2. Transport Layer(TCP/UDP)
3. Network/Internet Layer(IP)
4. Data Link Layer (MAC)
5. Physical Layer



## TCP/IP suite



# TCP/IP suite

## 1. Physical Layer

- It is a group of applications requiring network communications.
- This layer is responsible for generating the data and requesting connections.
- It acts on behalf of the sender and the Network Access layer on the behalf of the receiver.



# TCP/IP suite

## 2. Data Link Layer


- The packet's network protocol type, in this case, TCP/IP, is identified by the data-link layer.
- Error prevention and “framing” are also provided by the data-link layer.
- Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.



# TCP/IP suite

## 3. Internet Layer


This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows:

- **IP:** 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 websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
  - **ICMP:** ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
  - **ARP:** ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.
- 

# TCP/IP suite

## 4. Transport Layer

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

- **TCP:** Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.
  - **UDP:** The datagram delivery service is provided by UDP, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.
- 



# TCP/IP suite

## Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

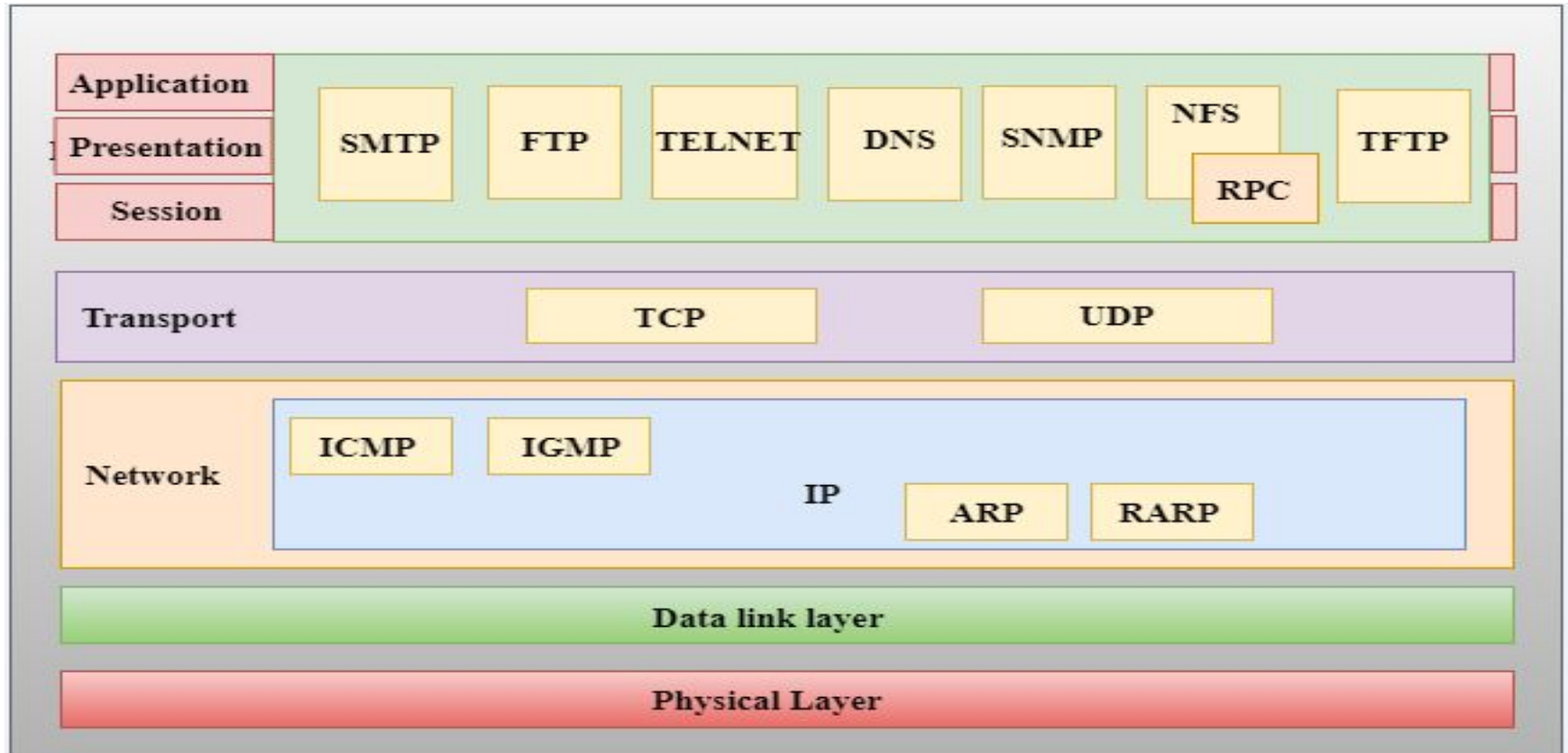


# TCP/IP suite

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

# Functions of TCP/IP layers



# Difference between OSI and TCP/IP Reference Model

TCP/IP	OSI
The full form of TCP/IP is Transmission Control Protocol/ Internet Protocol.	The full form of OSI is Open Systems Interconnection.
It is a communication protocol that is based on standard protocols and allows the connection of hosts over a network.	It is a structured model which deals with the functioning of a network.
It comprises of four layers:	It comprises seven layers:
It follows a horizontal approach.	It follows a vertical approach.
The TCP/IP is the implementation of the OSI Model.	An OSI Model is a reference model, based on which a network is created.
It is protocol dependent.	It is protocol independent.

## **Network devices.**

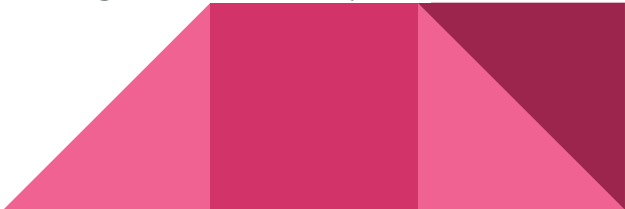
Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another.

For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.




## Network devices.

### 1. Repeater –

- A repeater operates at the physical layer.
  - Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network.
  - An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it.
  - When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.
- 

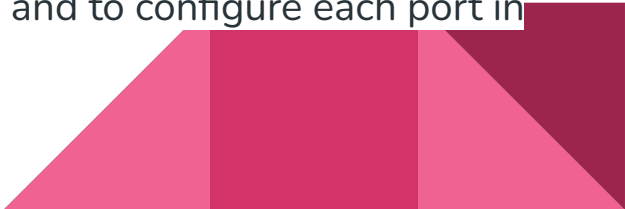
## Network devices.

### 2. Hub –

- A hub is a basically multi-port repeater.
  - A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
  - Hubs cannot filter data, so data packets are sent to all connected devices.
  - In other words, the collision domain of all hosts connected through Hub remains one.
  - Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.
- 

# Network devices.

## Types of Hub

- **Active Hub:-** These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
  - **Passive Hub:-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
  - **Intelligent Hub:-** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.
- 



## Network devices.

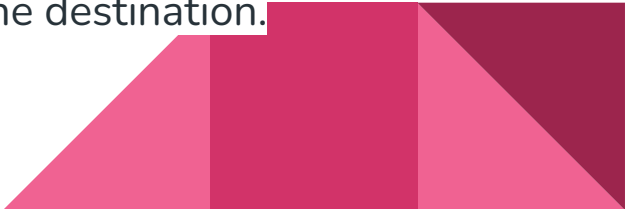
### 3. Bridge –

- A bridge operates at the data link layer.
- A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination.
- It is also used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, thus making it a 2 port device.



# Network devices

## Types of Bridges

- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
  - **Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.
- 

# Network devices

## 4. Switch –

- A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance.
- A switch is a data link layer device.
- The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.



# Network devices

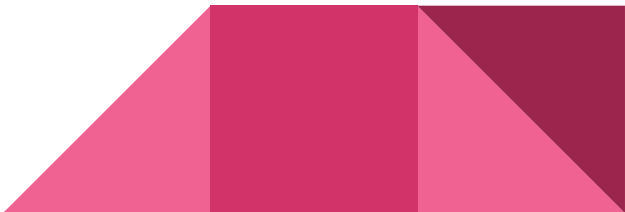
## 5. Routers –

- A router is a device like a switch that routes data packets based on their IP addresses.
- The router is mainly a Network Layer device.
- Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets.




## Network devices

### 6. Gateway –

- A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models.
  - They work as messenger agents that take data from one system, interpret it, and transfer it to another system.
  - Gateways are also called protocol converters and can operate at any network layer.
  - Gateways are generally more complex than switches or routers.
  - A gateway is also called a protocol converter.
- 

# Network devices

## 7. NIC –

- NIC or network interface card is a network adapter that is used to connect the computer to the network.
  - It is installed in the computer to establish a LAN.
  - It has a unique id that is written on the chip, and it has a connector to connect the cable to it.
  - The cable acts as an interface between the computer and the router or modem.
  - NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.
- 

# Network devices



## Network devices

