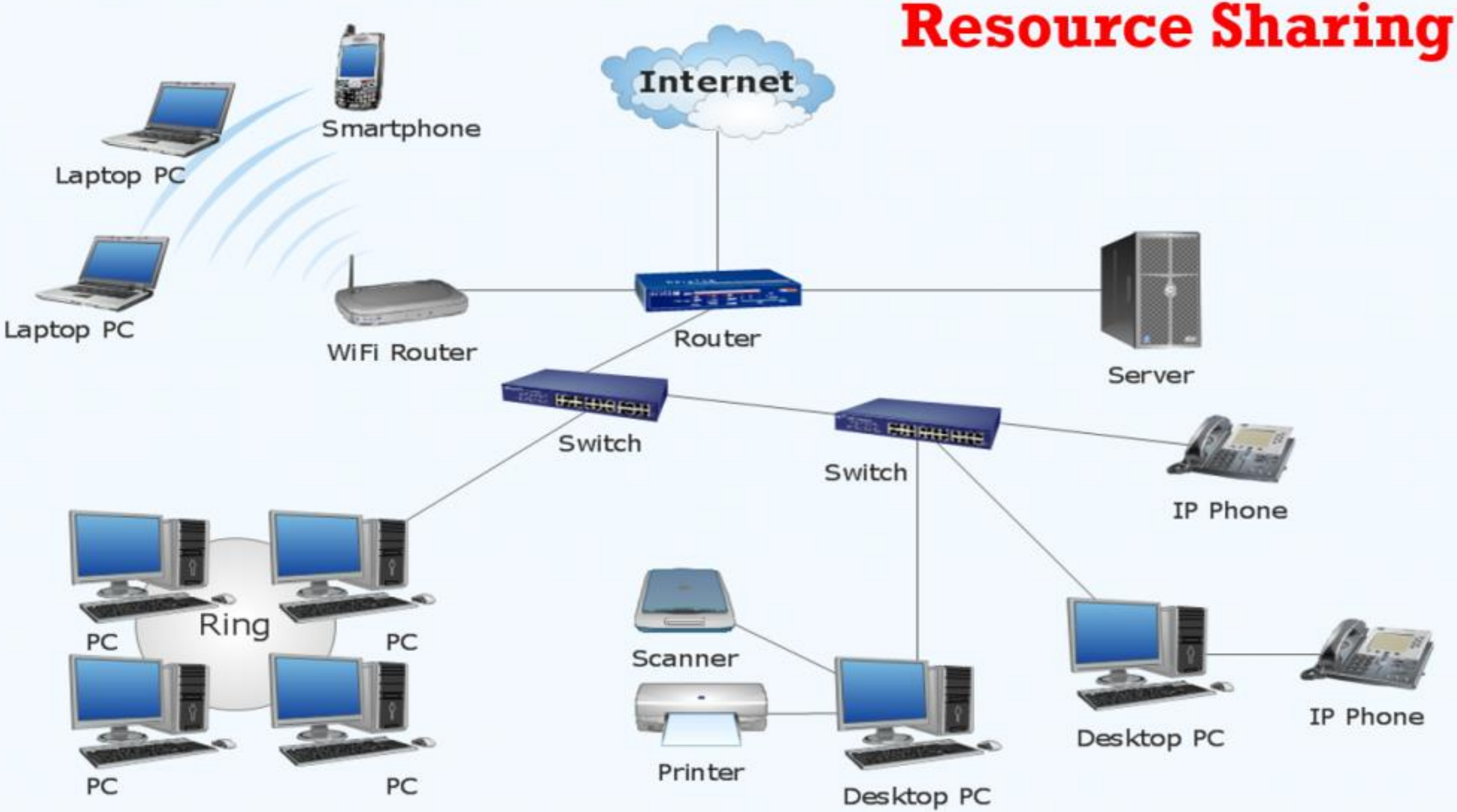
UNIT-1

B SAI BABA,M.Tech(Ph.D),VIT,Bhimavaram

What is Computer Network?

Resource Sharing

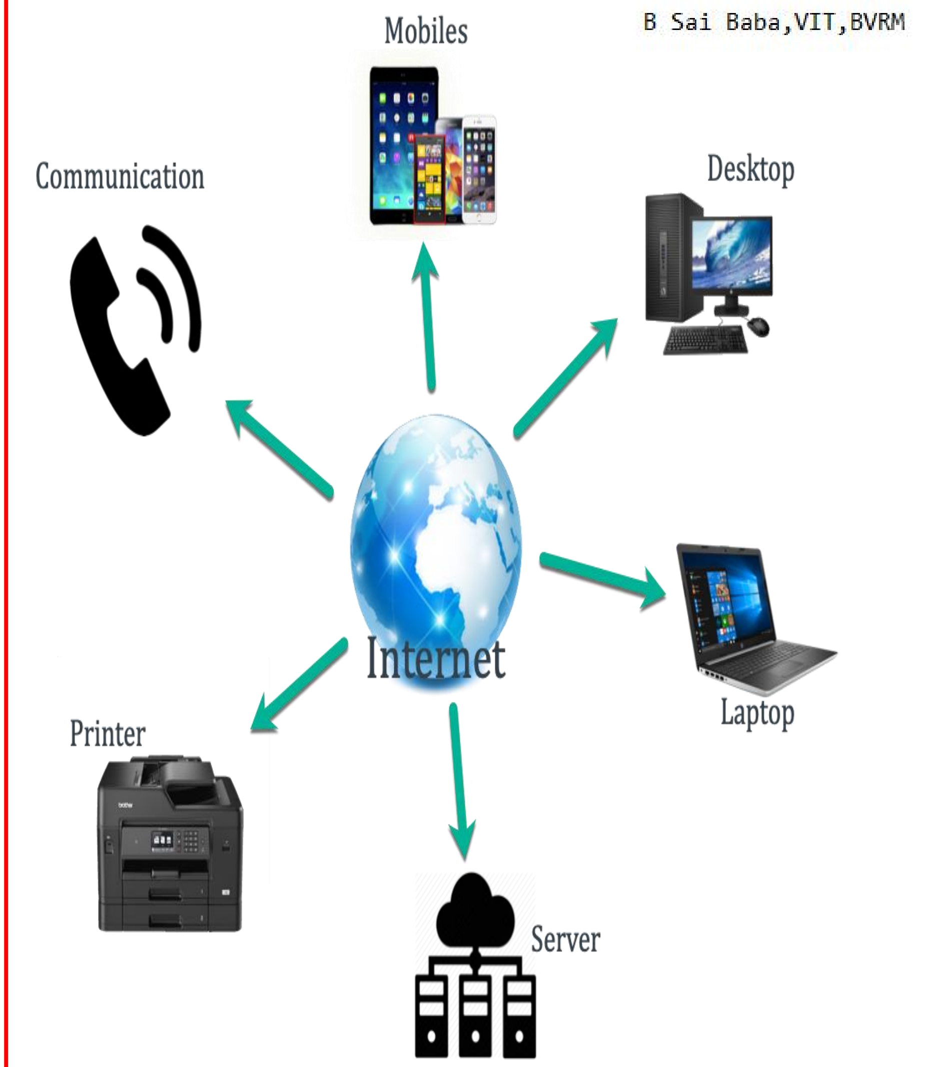


- A computer network is **a collection of interconnected computers, devices, and other hardware components t**hat are linked together to facilitate **communication, data sharing, and resource sharing.**
- It allows multiple computers and devices to exchange information, access shared resources, and collaborate effectively.

(or)

- A computer network is **a number of computers linked together to allow them to "talk" to each other and share resources**. Networked computers can **share hardware, software and data.**
- Connecting computers to form computer networks and the internet has had a huge impact on our lives.

What is Internet?


Mobiles
Communication
Desktop
Internet
Laptop
Printer
Server

- Internet is **a global network** that connects billions of computers across the world with each other and to the World Wide Web.
- It uses standard **internet protocol suite** (TCP/IP) to connect billions of computer users worldwide.
- At present, internet is the fastest mean of sending or exchanging information and data between computers across the world.

(or)

- **“ Network of networks “**

Where does **the Internet** come from?

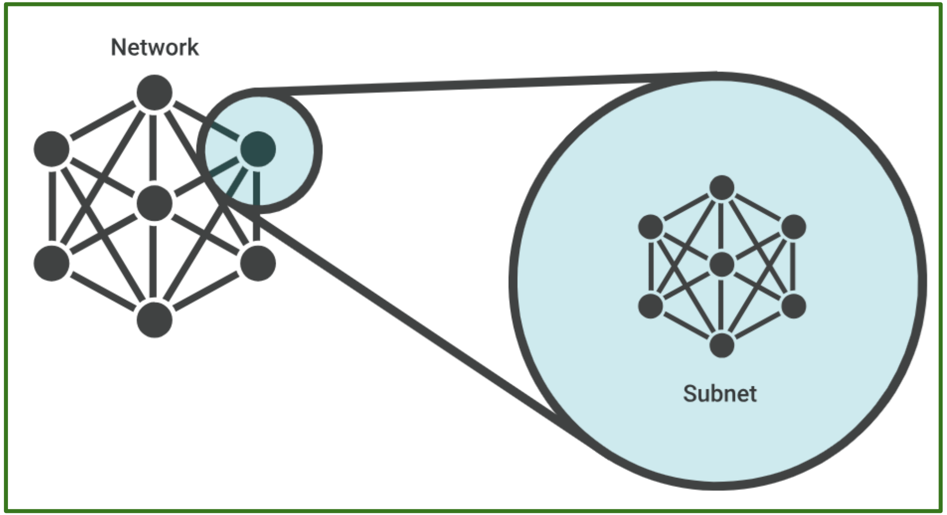
What is WWW?

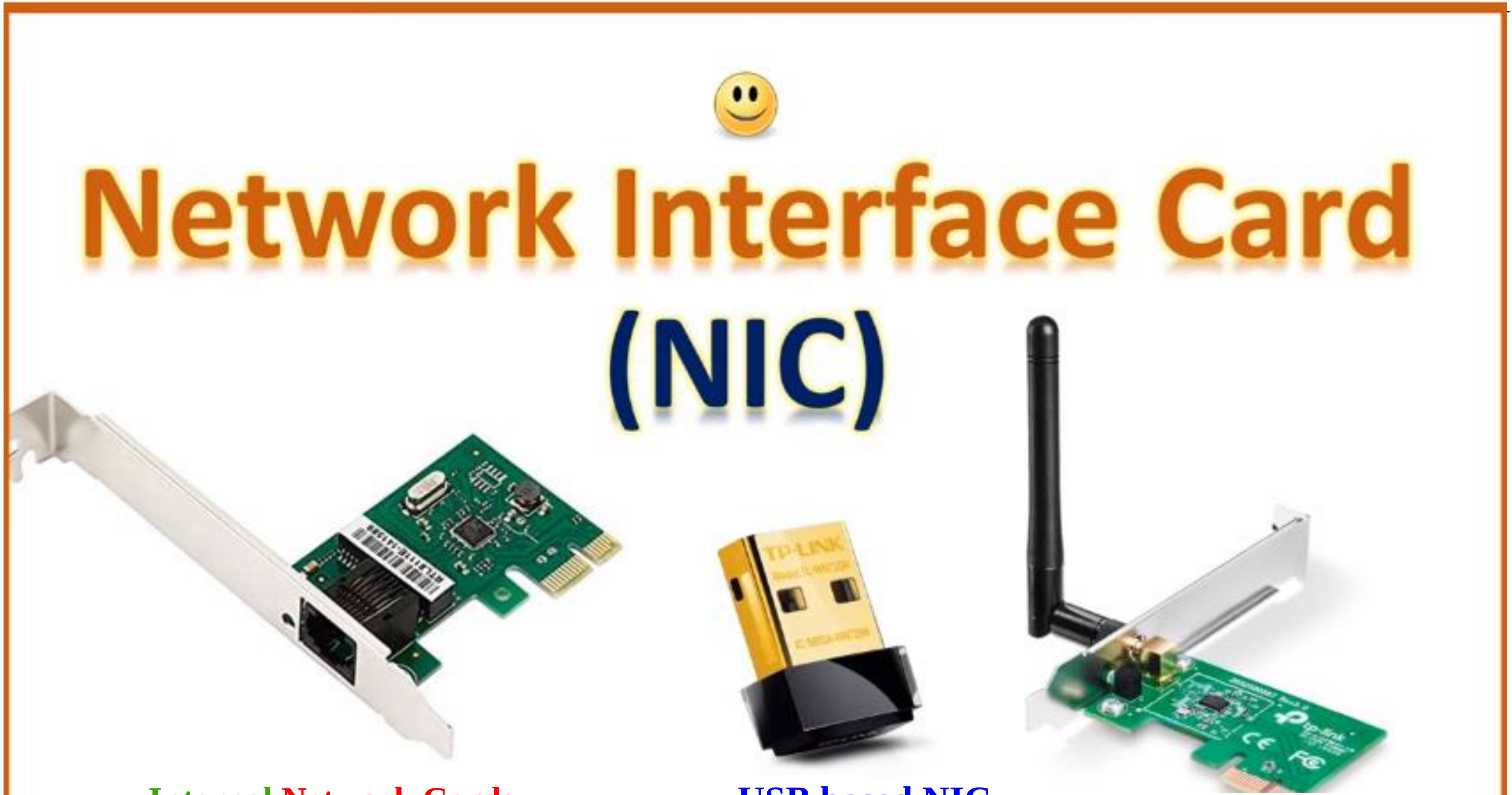
- The World Wide Web, commonly known as **the web**, is a system of interconnected **documents and resources** that are accessed via the internet.
- World Wide Web is an information system that allows users to access and navigate websites and web pages on the internet
- It is **a collection of websites, web pages, multimedia content, and hyperlinks** that allow users to navigate and access information.
- It is a common prefix used in **Uniform Resource Locators or URLs(**internet addresses**)** to identify a web server that hosts a website. **Eg: www.google.com**
- The web is just one of the many services and applications that utilize the internet infrastructure

Network Elements

Subnet ?

- A subnet, short for subnetwork, is a portion of a larger network that is divided or segmented into smaller logical networks.
- It involves dividing a single network into multiple smaller networks to improve network performance, security, and manageability.





Network Interface Card (NIC)

Internal Network Cards

USB based NIC

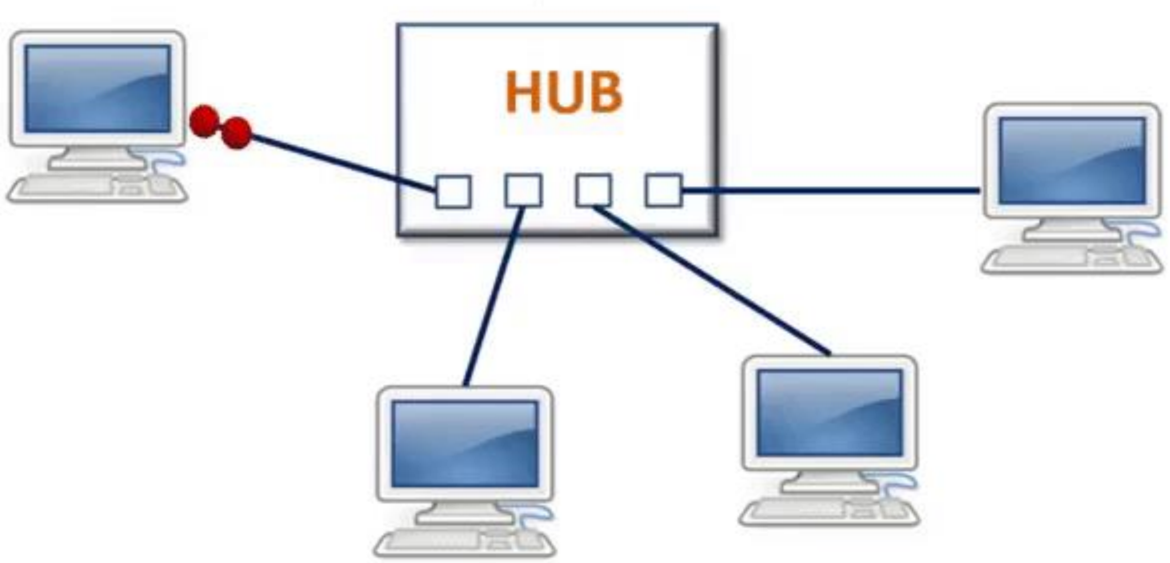
Wireless NIC

External Network Cards

NIC?

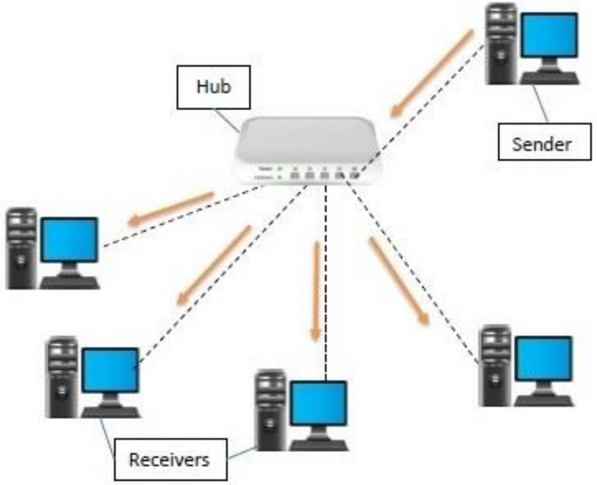
- A Network Interface Card (NIC) is a hardware component **without which a computer cannot be connected over a network.**
- It is a circuit board installed in a computer that provides a dedicated network connection to the computer.
- It is also called network interface controller, network adapter or LAN adapter.
- It can support a transfer rate of 10,100 to 1000 Mb/s.

Hub?

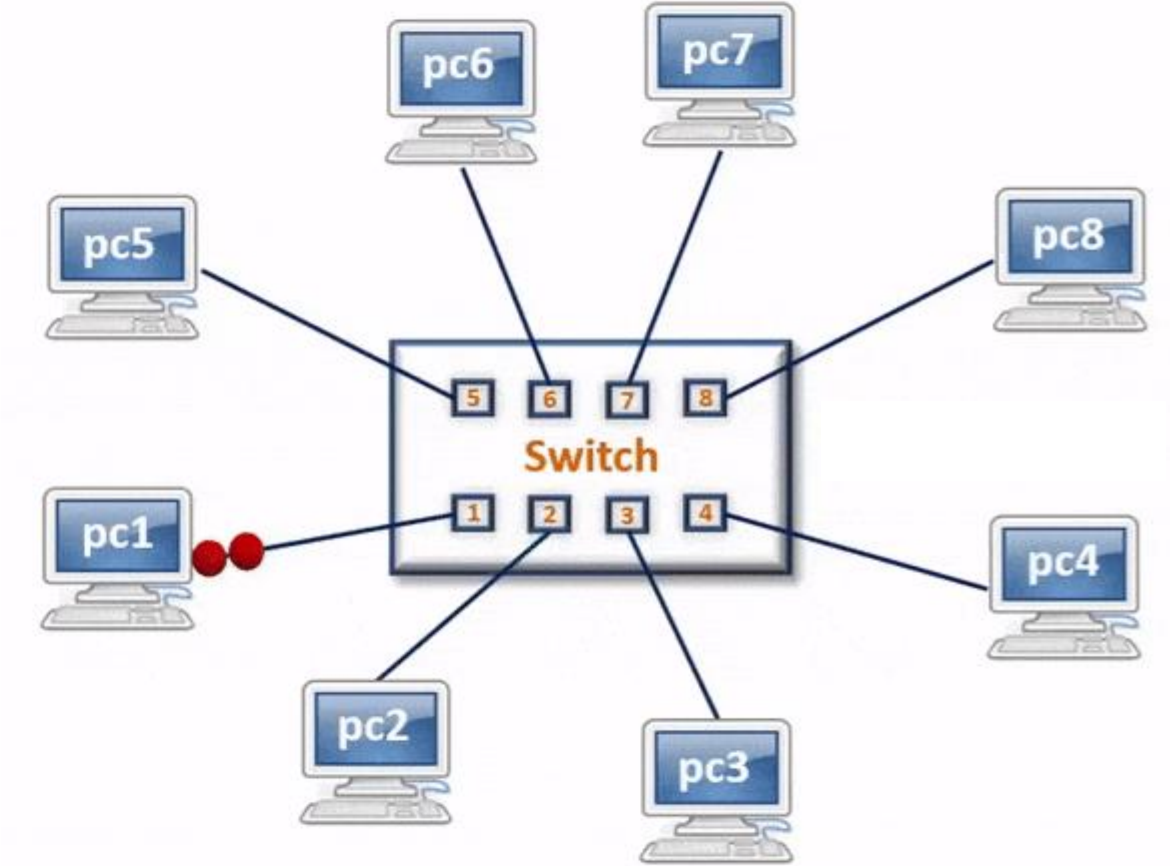


Hub?

- A hub is a physical layer networking device which is used to **connect multiple devices** in a network. They are generally used to connect computers in a LAN.
- A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports.
- When a data frame arrives at a port, **it is broadcast to every other port,** without considering whether it is destined for a particular destination or not.

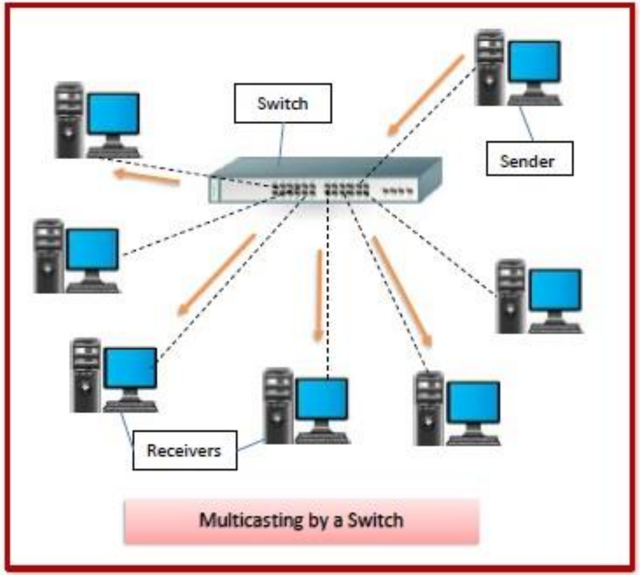


Switch?

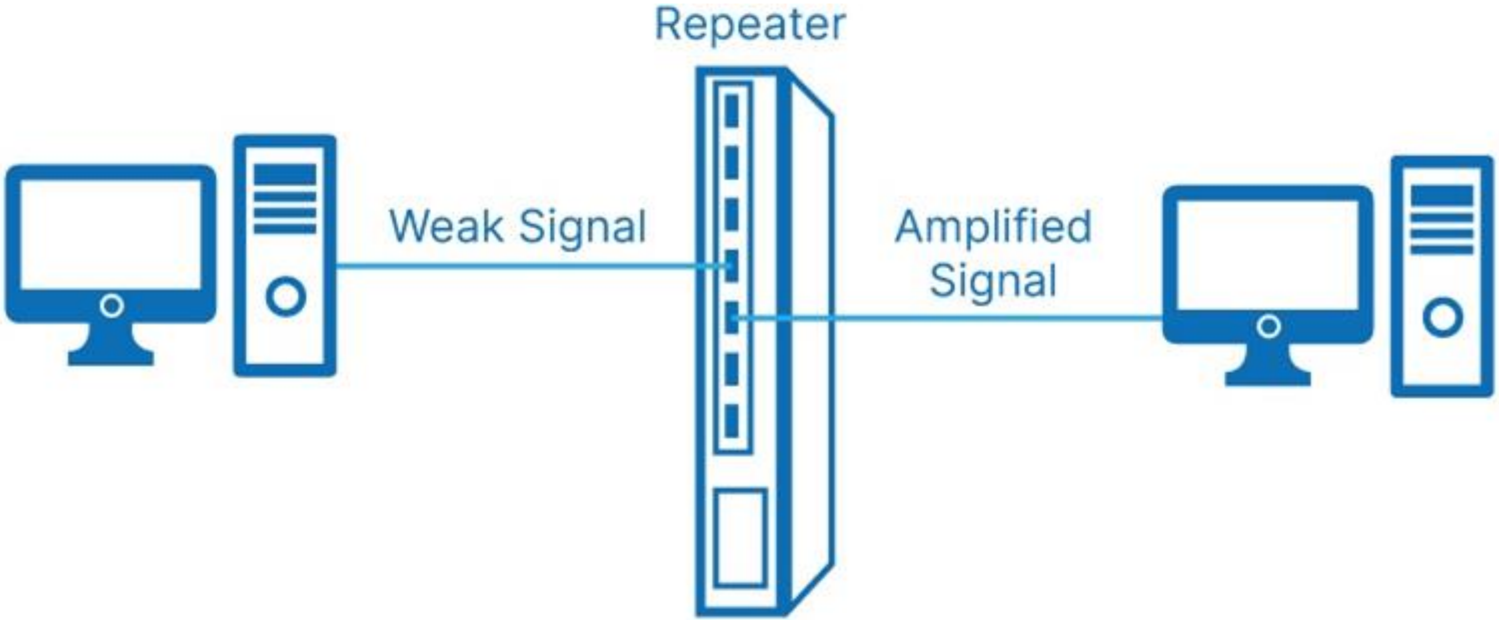


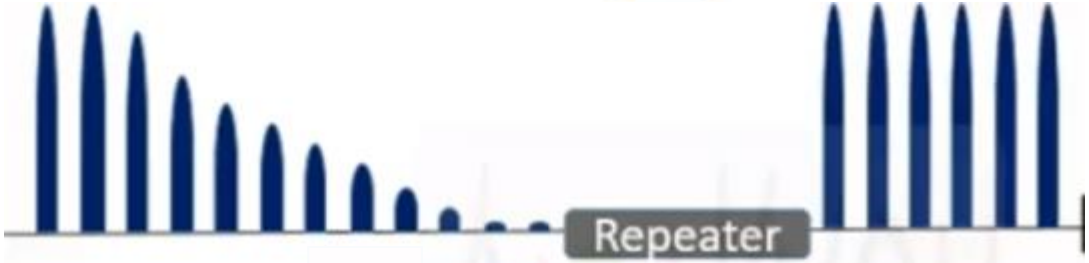
Switch?

- A switch is **a data link layer** hardware device that connects multiple devices on a computer network.
- A Switch contains **more advanced features than Hub.**
- Switch delivers the message to the correct destination based on the **physical address** present in the incoming message.
- **A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted**.



Repeater ?

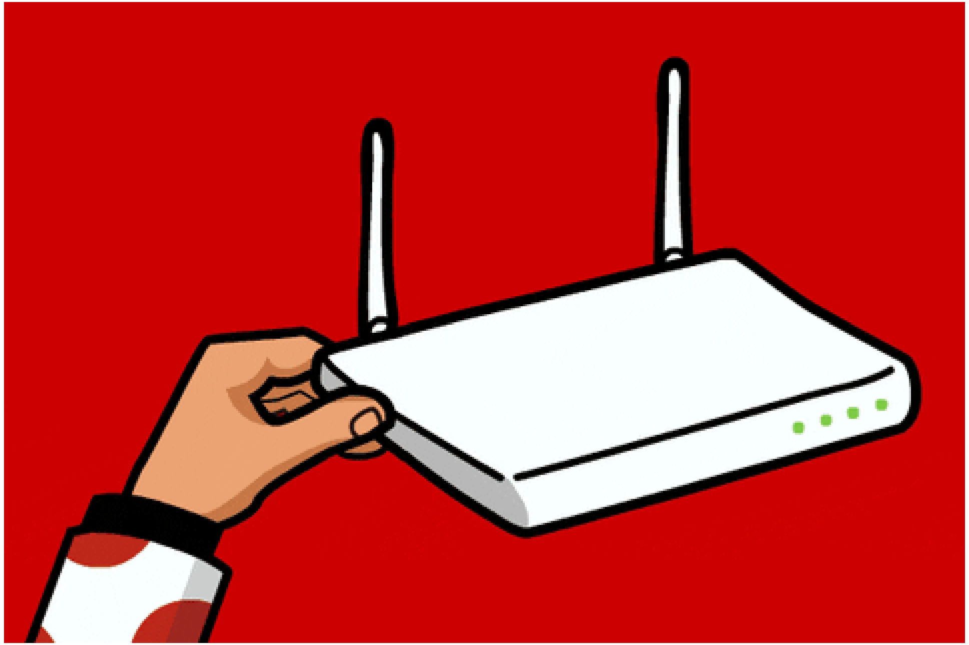




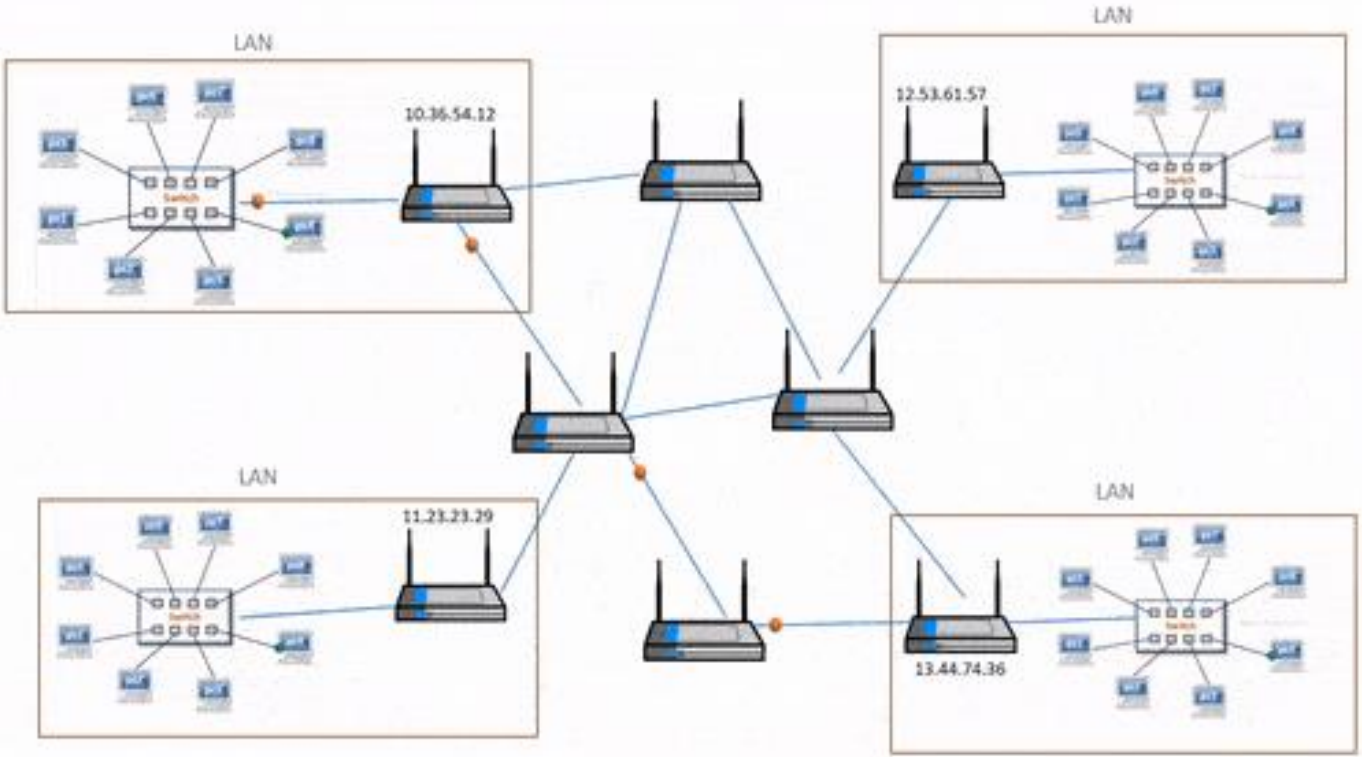
- Repeaters are used at the Physical layer of OSI model.
- A repeater is a powerful network hardware device that **regenerates an incoming signal from the sender before retransmitting it to the receiver**.
- It is also known as **a signal booster**, The primary function of a repeater is **to receive the weakened signal, amplify it, and then retransmit it at its original strength.**
- In a network, as data travels over cables (such as copper or fiber-optic cables), it tends to **weaken** or attenuate over long distances.
- This attenuation can lead to **data loss and degradation**, affecting the overall performance of the network.

Router?

- A router is a network device that operates at **the network layer** (Layer 3) of the OSI model.
- Its primary function is to forward data packets between different computer networks, such as local area networks (LANs) and wide area networks (WANs).
- A router acts as a central point of connection for multiple devices and directs network traffic based on destination IP addresses.



Router Device



Network Topologies

“ A topology is the **layout of how a network communicate with different devices**.”

(or)

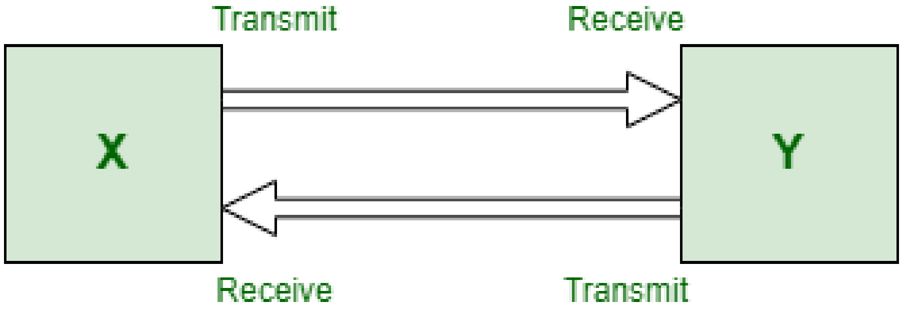
“A Network Topology **is the arrangement with which computer systems or network devices are connected to each other**. Topologies may define both physical and logical aspect of the network.”

The various network topologies are:

- ➔ **Point to Point Topology**
- ➔ **Mesh Topology**
- ➔ **Star Topology**
- ➔ **Bus Topology**
- ➔ **Ring Topology**
- ➔ **Tree Topology**
- ➔ **Hybrid Topology**

Point to Point Topology

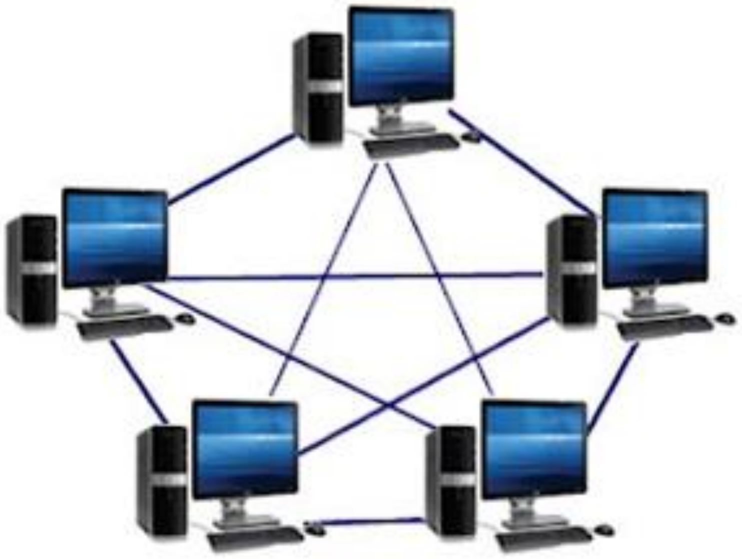
- Point-to-point topology is a network configuration where two devices or nodes are directly connected to each other without any intermediate devices.
- It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver.
- In this type of topology, data can flow directly from one point to another along **a dedicated communication channel.**



Point to Point Topology

Mesh Topology

- In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are **AHCP** (Ad Hoc Configuration Protocols), **DHCP** (Dynamic Host Configuration Protocol), etc.
- Every device is connected to another via dedicated channels. These channels are known as **links**.
- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1.
- In Figure , there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).



Mesh Topology

Advantages of Mesh Topology

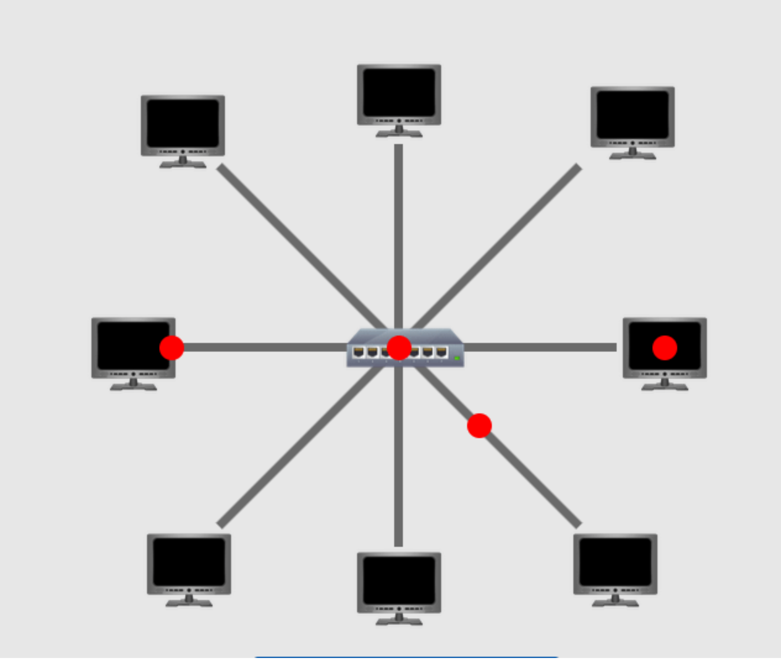
- Communication is very fast between the nodes.
- Mesh Topology is robust.
- ***Fault Tolerance:* Mesh topology provides high redundancy and fault tolerance. If one link or connection fails, there are alternative paths available for data to reach its destination, ensuring network reliability.**

Drawbacks of Mesh Topology

- **Installation and configuration are difficult.**
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high

Star Topology

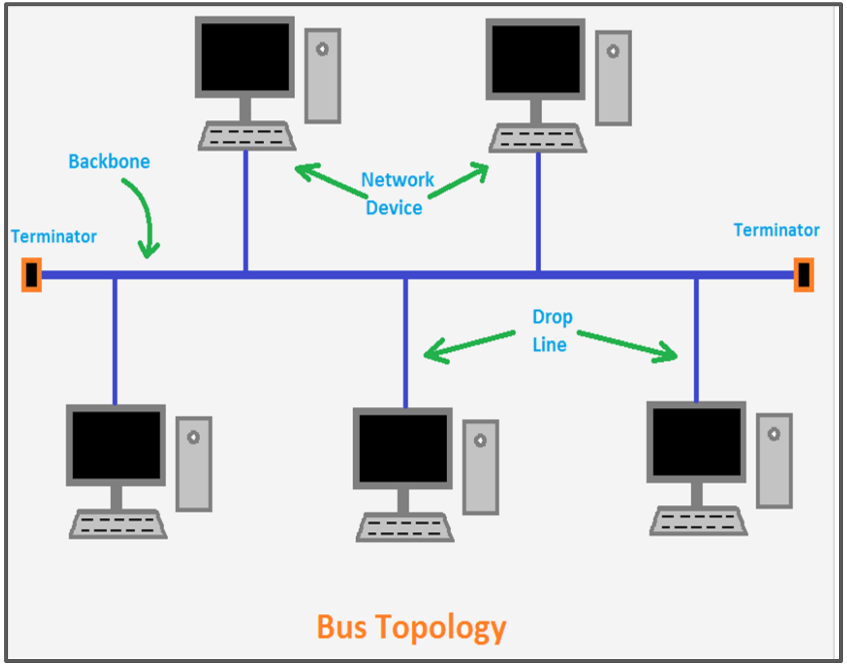
- Star topology is a network configuration in which all devices in the network are connected to **a central hub or switch.**
- In this arrangement, each device communicates directly with **the central hub and not with other devices** in the network. The hub acts as a central point of communication, managing data traffic between the connected device
- Star topology is very popular because the startup costs are low. It is also easy to create new nodes to the network.
- **If one device fails, it does not affect the rest of the network, as they are not directly connected to each other.**
- **If the central hub fails throughout the network goes down.**



Star Topology

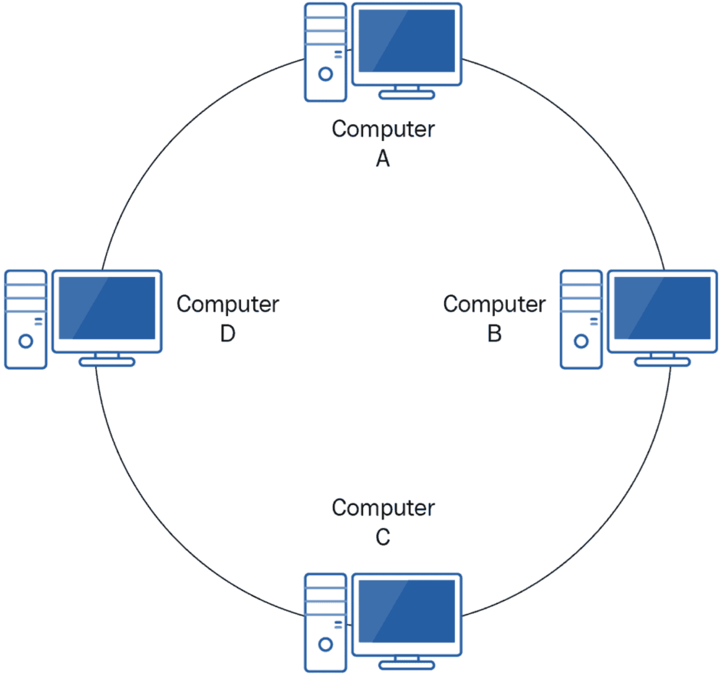
Bus Topology

- The bus topology is designed in such a way that all the stations are connected through **a single cable** known as **a backbone cable**.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- Data is transmitted in **both directions along the bus**.
- The **backbone cable** is considered as a **"single lane"** through which the message is broadcast to all the stations.
- It is a multi-point connection and a non-robust topology because **if the backbone fails the topology crashes.**



Ring Topology

- In a ring topology, devices are connected in **a closed loop**, with each device having exactly **two neighbors for communication.**
- The node that receives the message from the previous computer will retransmit to the next node.
- **The data flows in one direction, i.e., it is unidirectional.**
- The data flows in **a single loop** continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in **a clockwise direction.**
- **Failure of any device** or connection in the ring can cause the **entire network to fail,** making it less fault-tolerant.



Ring Topology

Tree Topology

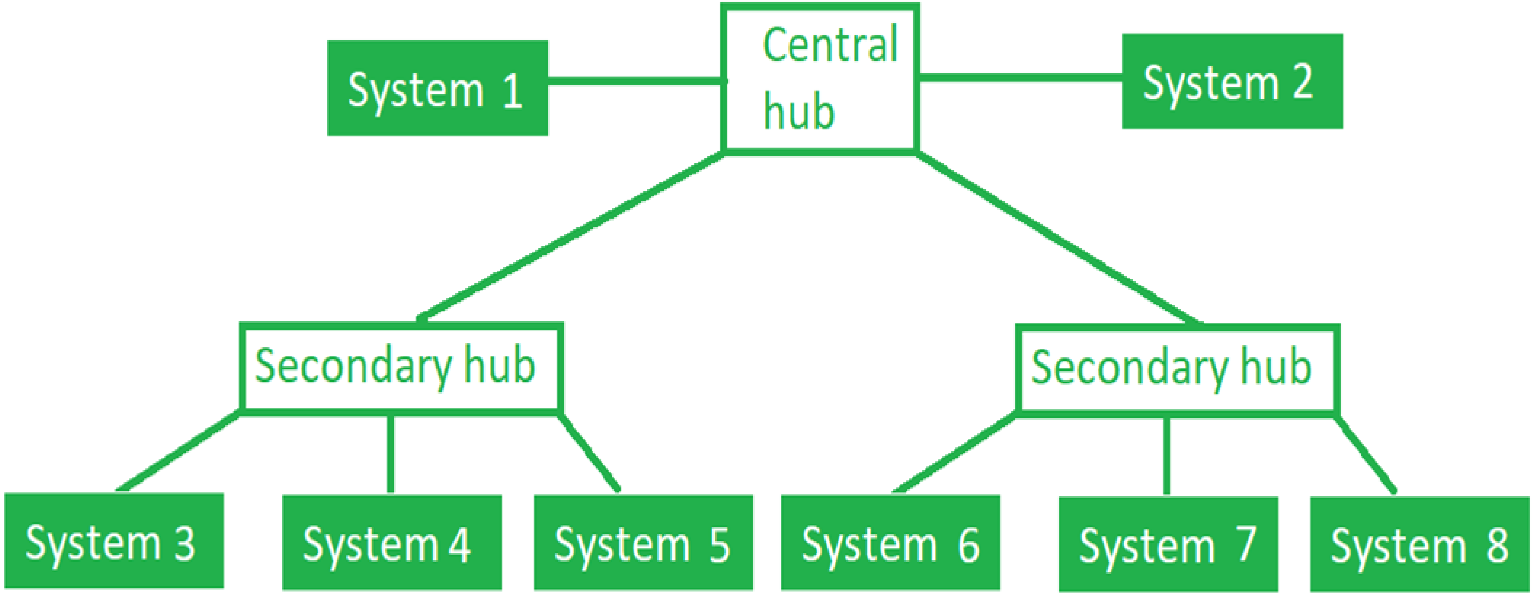


Figure : In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub.

- Tree topology, also known **as hierarchical topology**, is a network configuration that combines characteristics of both **bus and star topologies.**
- In a tree network, all devices are connected to a central hub, which acts as the root of the tree. From this central hub, branches extend out to other hubs or end devices, creating a hierarchical structure.
- It is a multi-point connection and a non-robust topology because **if the backbone fails** the topology crashes.

Key features of a tree topology:

1. **Central hub:** The central hub is the primary element of the tree topology and is responsible for connecting all the branches and end devices in the network. It acts as the main communication point for all connected devices.
2. **Secondary hub:** It is the intermediate levels of the hierarchy. Each **Secondary hub** is connected to the central hub or other intermediate hubs. These branches can be further extended into sub-branches, creating a multi-level hierarchy.

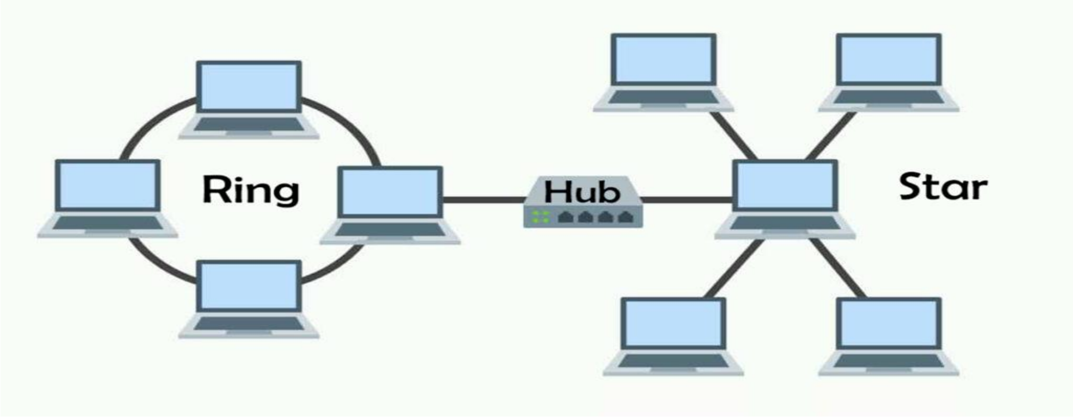
3. **End devices**: The end devices are the devices located at the leaves of the tree. These devices can be computers, printers, switches, or any other networked devices.

4.**Hierarchical structure**: The tree topology exhibits a hierarchical arrangement of devices, which makes it easy to manage and scale the network. Information generally flows from the top (root) of the tree down to the leaves and vice versa.

Advantages of tree topology:

1. **Scalability:** Tree topologies can be easily scaled by adding more branches or connecting additional end devices to the existing branches.
2. **Centralized control:** The central hub provides a single point of control and management for the entire network.
3. **Fault isolation:** If a branch or an end device fails, only the devices in that branch or connected to that branch are affected, leaving the rest of the network intact.

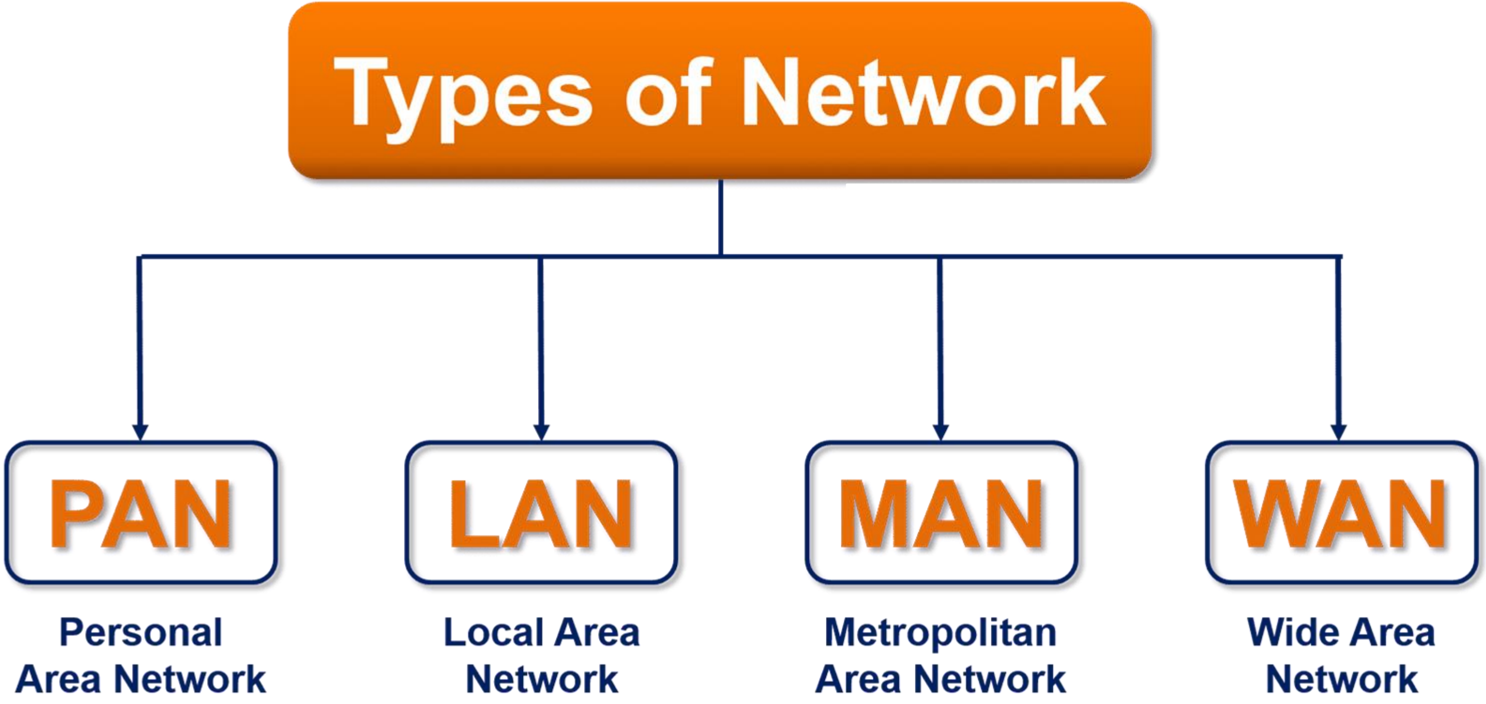
Hybrid Topology

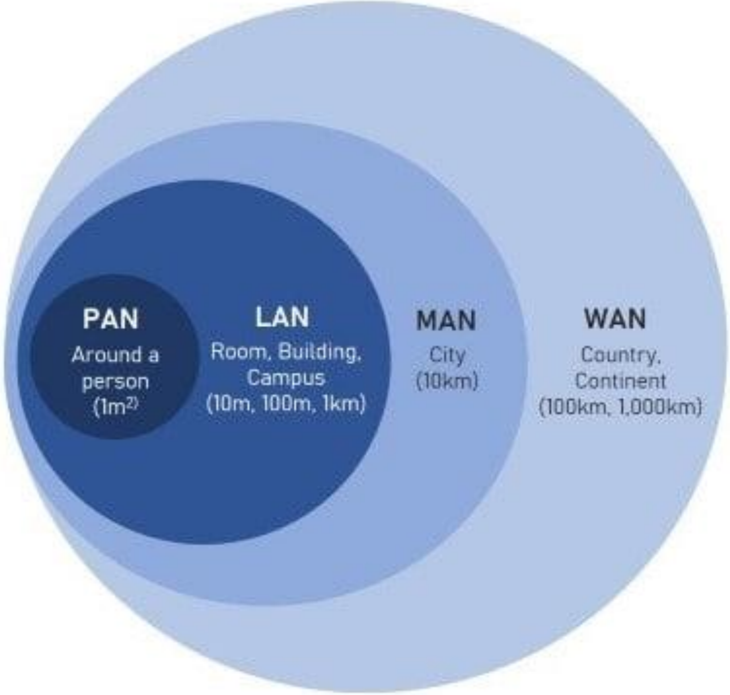


- This topological technology is the combination of all the various types of topologies we have studied above.
- Hybrid Topology is used when the nodes are free to take any form.
- It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above.

Types of Networks

- Networks can be categorized into various types based on their **size, geographical coverage, and the way they are structured**.




PAN
Around a person (1m2)
LAN
Room, Building, Campus (10m, 100m, 1km)
MAN
City (10km)
WAN
Country, Continent (100km, 1,000km)

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

PAN (Personal Area Network)

- PANs (Personal Area Networks) let devices communicate **over the range of a person.**
- A Personal Area Network (PAN) is a type of network used for connecting personal devices in close proximity to an individual.
- PANs are designed to facilitate communication and data exchange between devices such as **smartphones, tablets, laptops, personal computers, wireless headphones, smartwatches, and other wearable devices.**
- **Example: Bluetooth devices**
- In the simplest form, Bluetooth networks use the master-slave paradigm of **Fig. 1-7**.
- The system unit (the PC) is normally the **master**, talking to the mouse, keyboard, etc., as **slaves**.
- The master tells the slaves what addresses to use, when they can broadcast, how long they can transmit, what frequencies they can use, and so on.

Characteristics of a PAN are:

Limited Coverage: PANs have a very limited coverage area, typically within a range of a few meters or up to about **10 meters (33 feet).** They are intended to connect devices that are physically close to each other.

Wireless Technology: PANs typically use wireless communication technologies for connectivity.

- **Bluetooth** is one of the most common wireless technologies used in PANs due to its low power consumption and short-range capabilities.

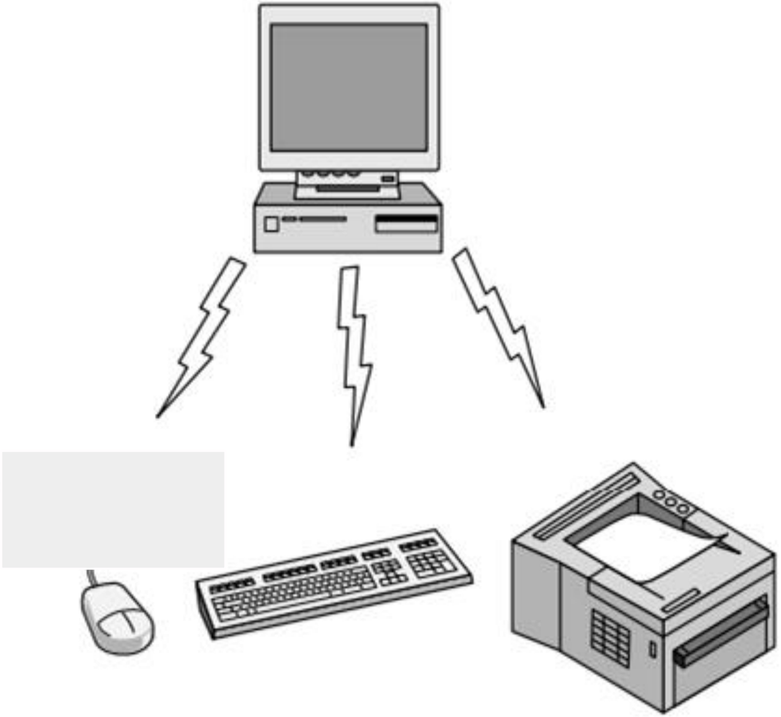


Figure 1-7. Bluetooth PAN configuration.

Examples of PAN Applications:

- ★ Pairing wireless **headphones or speakers** with a smartphone or computer.
- ★ Connecting **a wireless keyboard and mouse** to a laptop or desktop computer.
- ★ Synchronizing data between **a smartphone and a fitness tracker or smartwatch**.
- ★ Transferring files between two smartphones via Bluetooth.

LAN (Local Area Network)

- Local Area Network (LAN) is a type of network that connects devices within a limited geographical area, such as **a single building like a home, office or factory.**
- LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information.
- Types of LAN networks:
    a. **Wired LAN**
    b. **Wireless LAN**

Wired LAN:

➔ **Ethernet(IEEE 802.3)**is the most common and widely used LAN technology.

➔ It uses **twisted-pair or fiber-optic cables** to connect devices in a star topology.

➔ Wired LANs run at speeds of **100 Mbps to 1 Gbps**, have low delay(microseconds or nanoseconds), and make very few errors.

Wireless LAN:

- There is a standard for **wireless LANs called IEEE 802.11**, popularly known as **WiFi**, to connect devices without the need for physical cables.
- WLANs use **radio waves** to transmit data over the airwaves, providing wireless connectivity and mobility to devices within the network.
- It runs at speeds anywhere from **10 to hundreds of Mbps.**
- **Access Points:**
  - Access points are sometimes called **base stations**. The access points connect to the wired network, and all communication between clients goes through an access point
  - Access points provide the wireless connectivity and allow devices to connect to the WLAN.
- WLANs are widely used in homes, offices, public spaces, airports, hotels, educational institutions, and various other environments to provide wireless internet access and facilitate device connectivity.

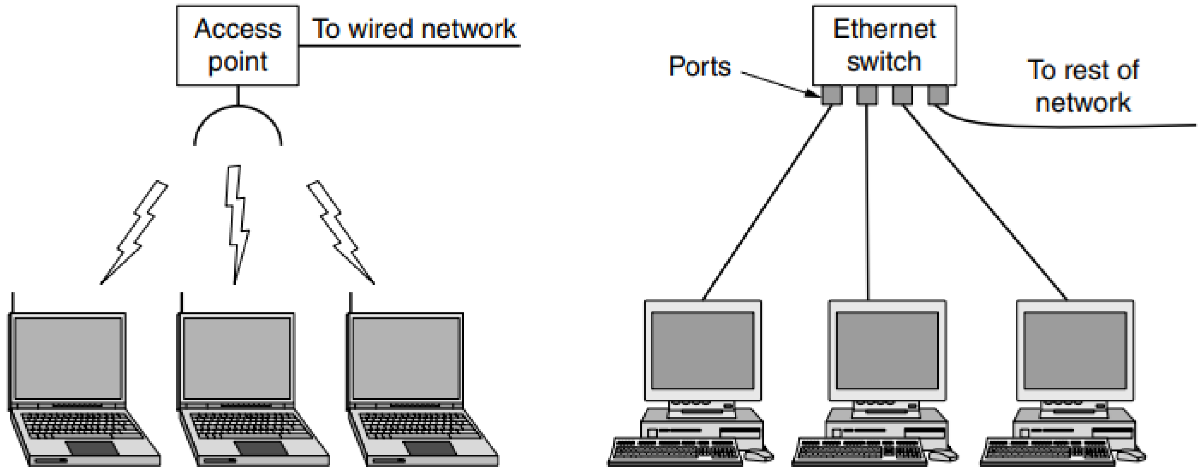
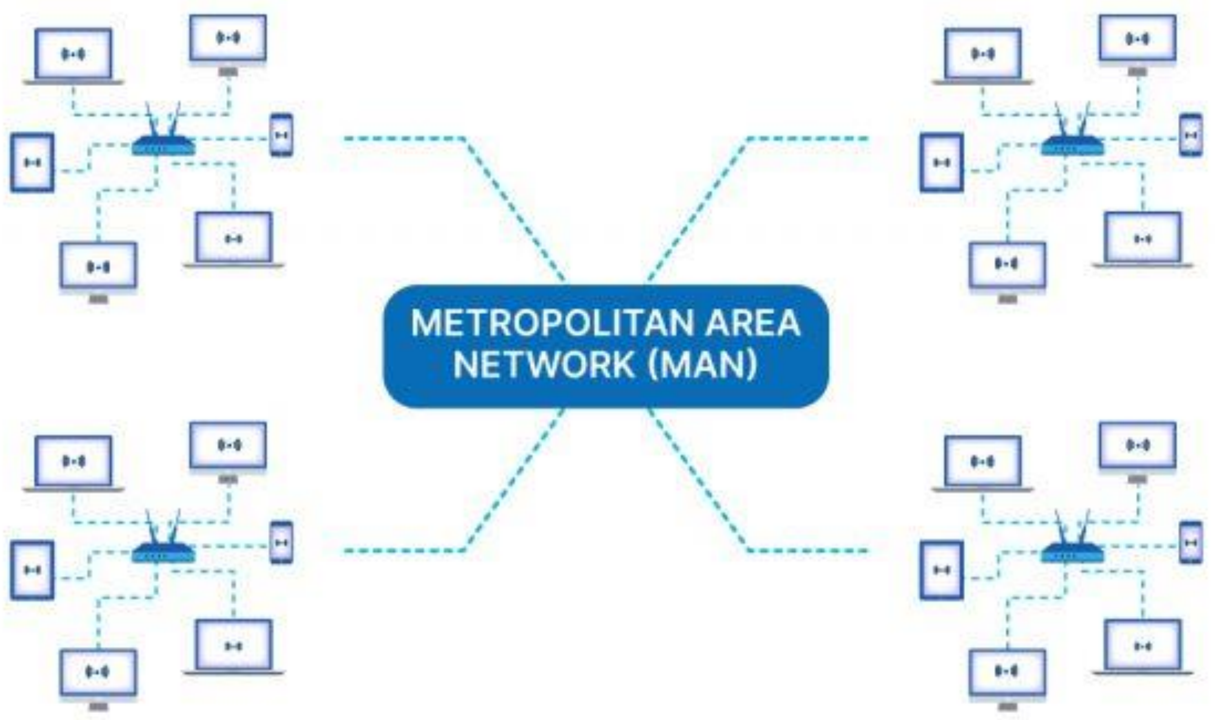


Figure 1-8. Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

- Fig. 1-8(a & b) shows a sample topology of **WLAN** and **Switched Ethernet**.
- Each computer speaks the Ethernet protocol and connects to a box called **a switch** with a point-to-point link.
- Hence the name. A switch has multiple ports, each of which can connect to one computer.
- The job of the switch is to relay packets between computers that are attached to it, using **the address in each packet** to determine which computer to send it to.

MAN (Metropolitan Area Network)



METROPOLITAN AREANETWORK (MAN)

- MAN covers a larger geographical area than a Local Area Network (LAN) but is smaller than a Wide Area Network (WAN).
- A MAN typically spans **a city or a metropolitan region**, connecting multiple LANs and data centers within the area.
- The best-known examples of MANs are **the cable television networks** available in many cities.
- These systems grew from earlier community **antenna systems** used in areas with poor over-the-air television reception.
- In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers’ houses.
- When the Internet began attracting a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum.
- At that point, the cable TV system began to morph from simply a way to distribute television to a metropolitan area network.
- a MAN might look something like the system shown in Fig. 1-9.
- In this figure we see both television signals and Internet being fed into **the centralized cable headend** for subsequent distribution to people’s homes.

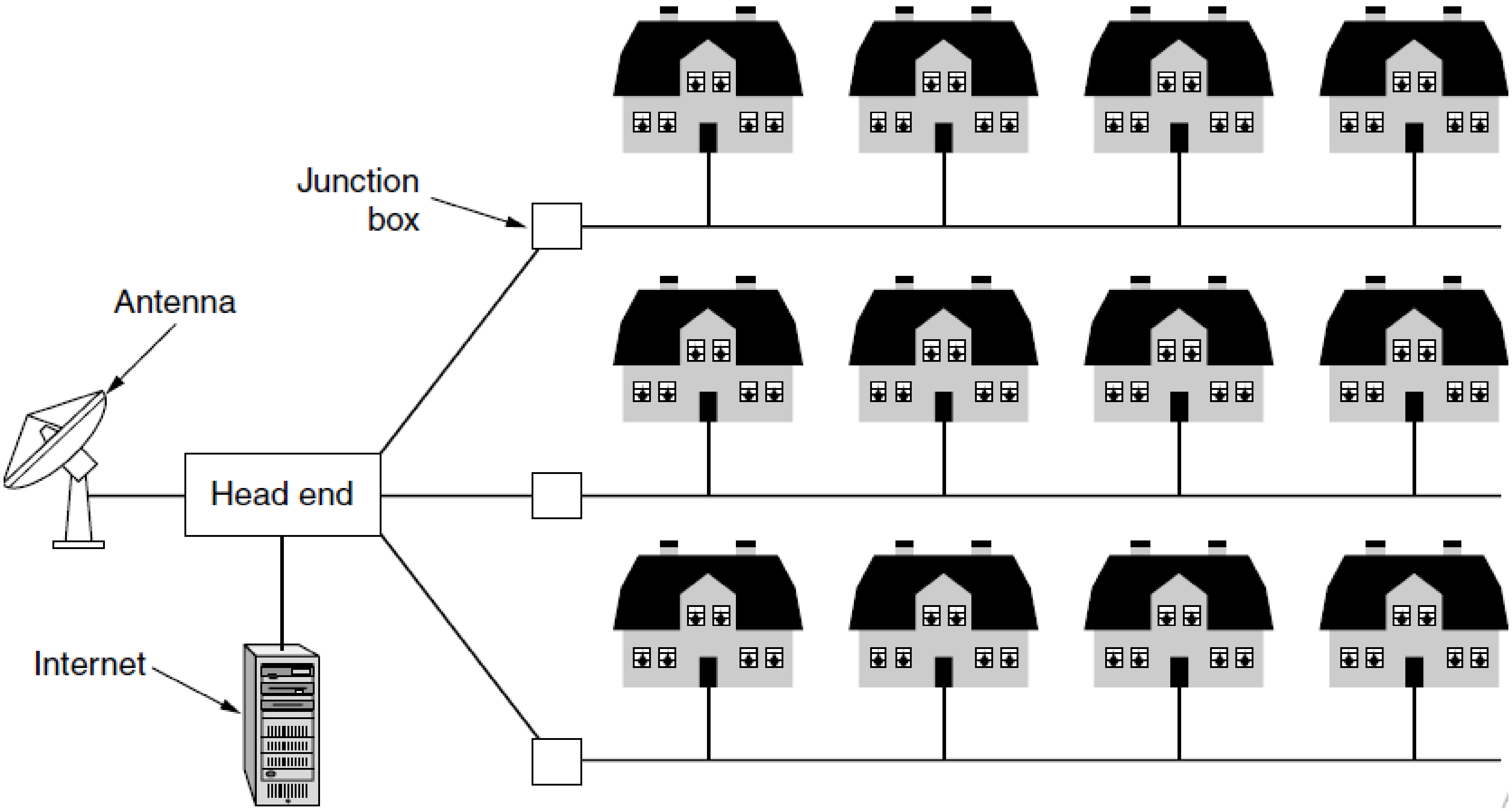
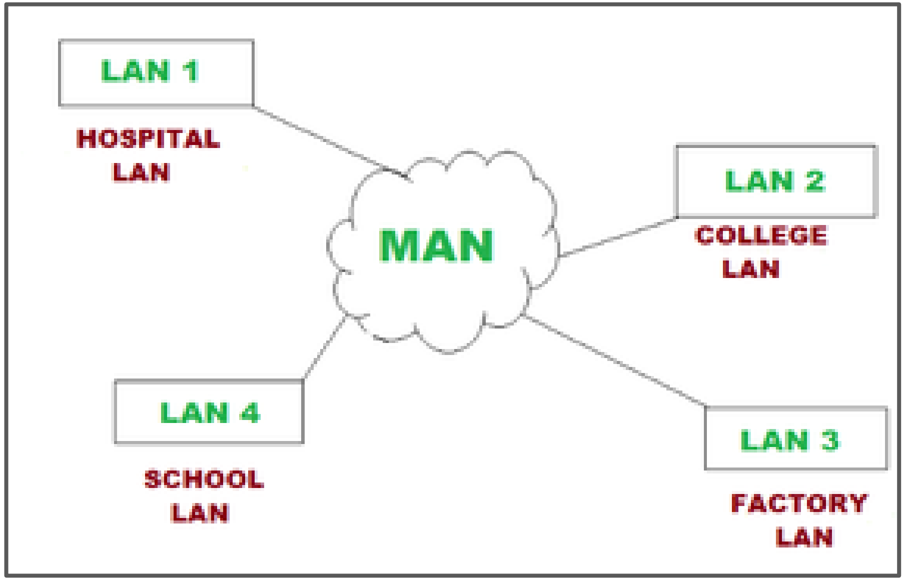


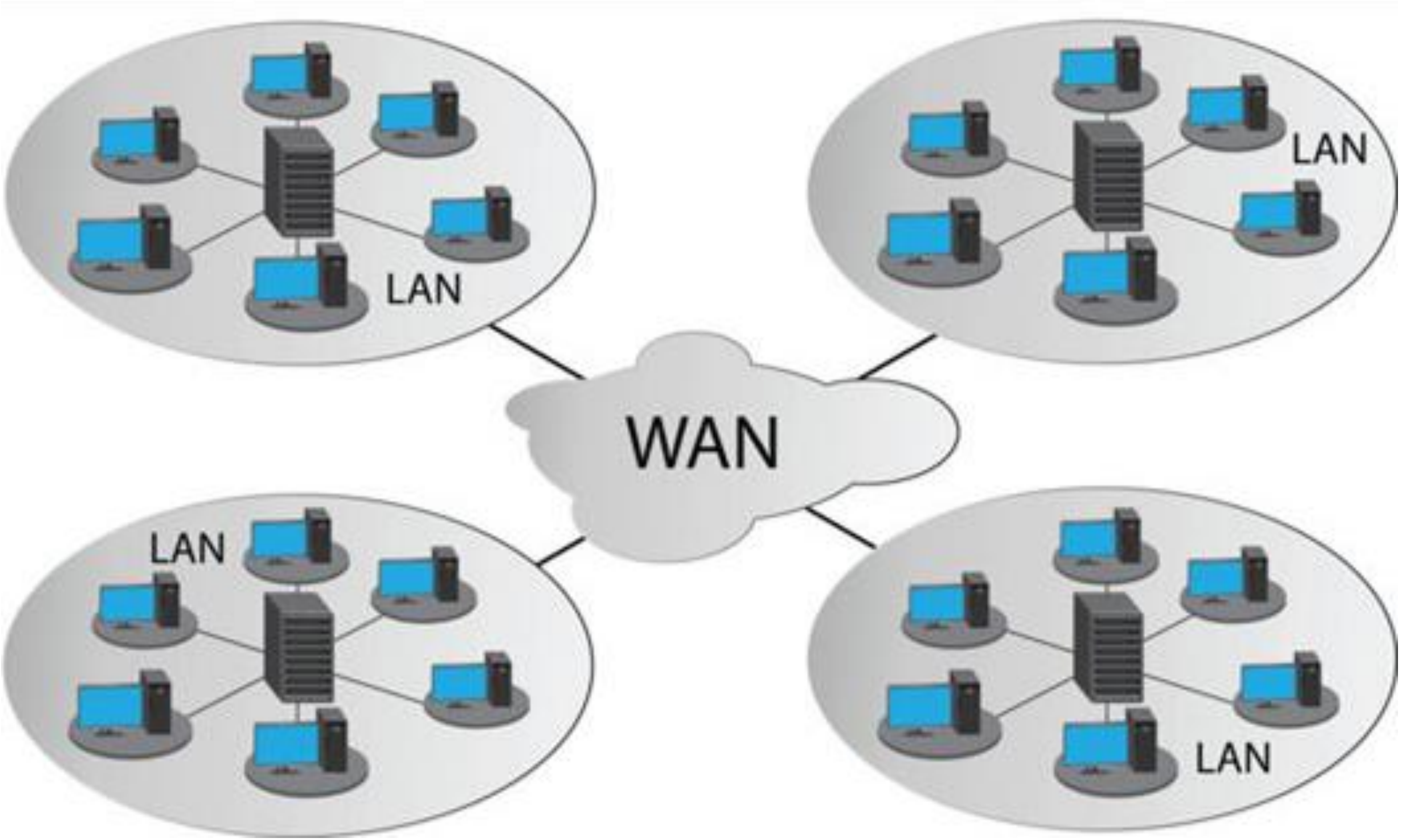
Figure 1-9. A metropolitan area network based on cable TV.

Q:: How does the MAN network work?

- MAN's primary goal is to establish a communication link between two independent LAN nodes in order to connect geographically dispersed LANs.
- To accomplish this, the Metropolitan Area Network typically uses **optical fiber** as a transmission medium, and the network is built with the help of routers and switches.
- Eg:
    - **Cable TV network**
    - **Telephone networks**



WAN (Wide Area Network)



- WAN is a type of computer network that spans a large geographical area, typically **connecting multiple Local Area Networks (LANs) or Metropolitan Area Networks (MANs)** across **cities, states, countries, or even continents**.
- We will begin our discussion with wired WANs, using the example of a company with branch offices in different cities.
- The WAN in Fig. 1-10 is a network that connects offices in Perth, Melbourne, and Brisbane. Each of these offices contains computers intended for running user (i.e., application) programs.
- We will follow traditional usage and call these machines hosts. The rest of the network that connects these hosts is then called the communication subnet, or just subnet for short.
- The job of the subnet is to carry messages from host to host, just as the telephone system carries words (really just sounds) from speaker to listener.

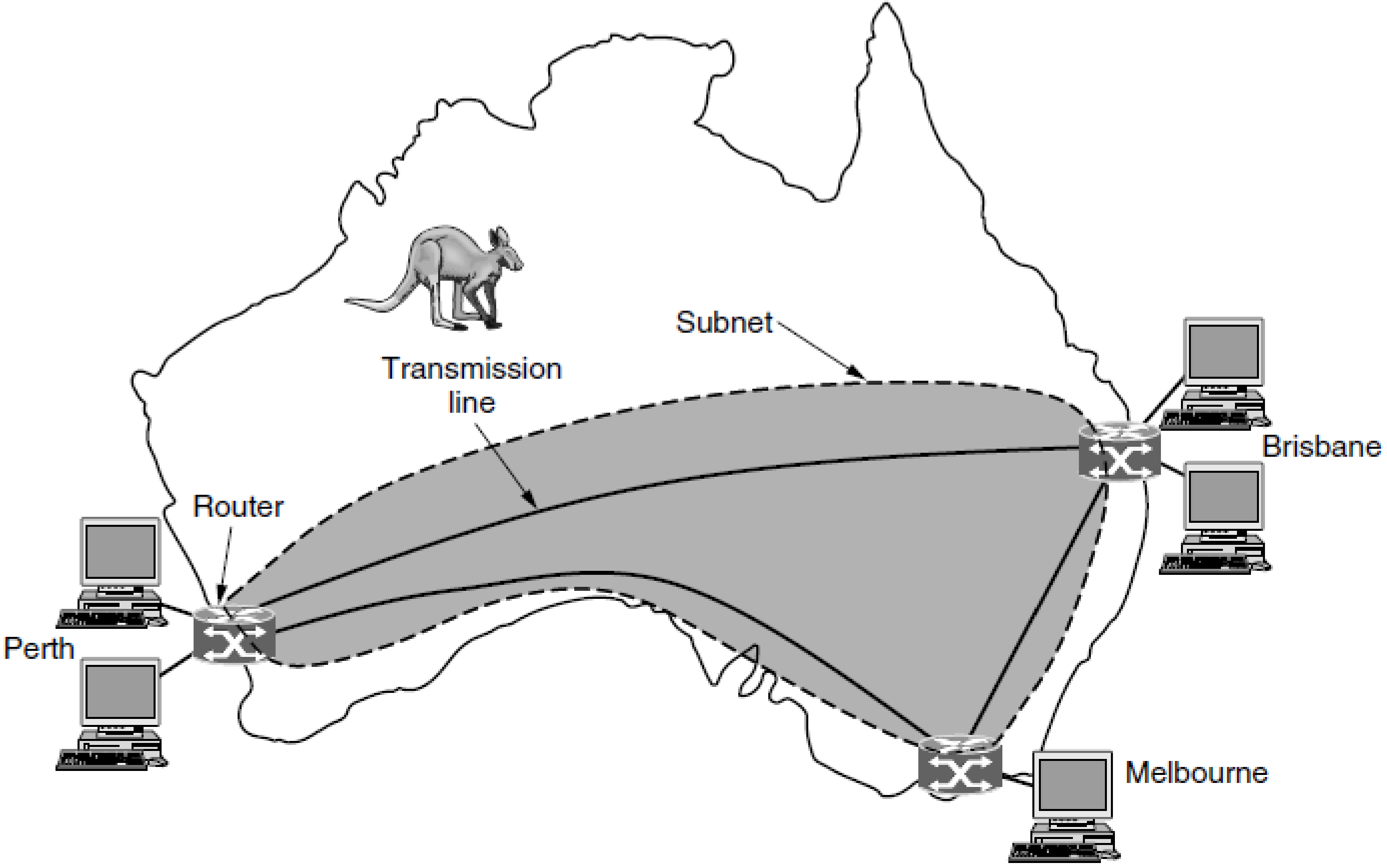
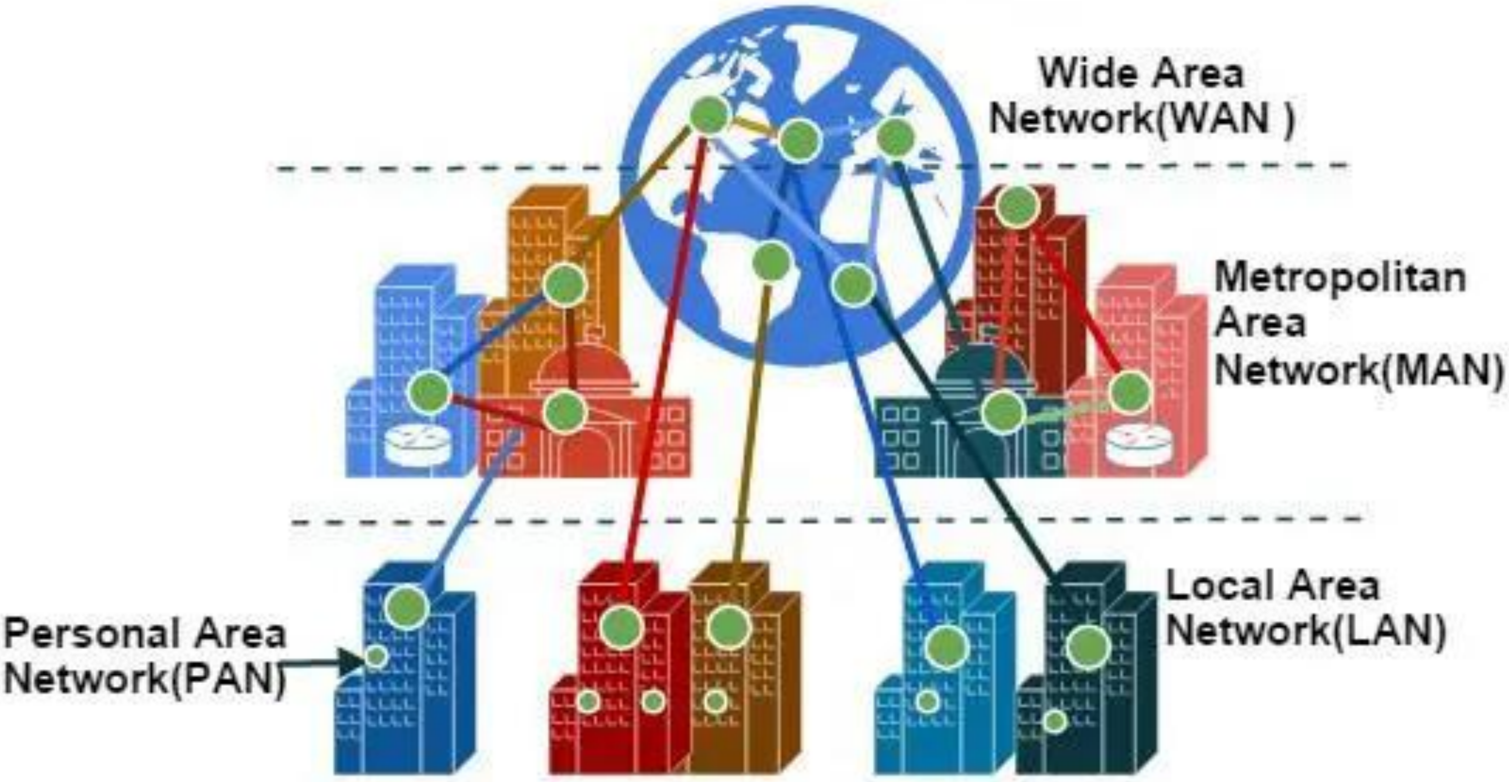


Figure 1-10. WAN that connects three branch offices in Australia.

- In most WANs, the subnet consists of two distinct components:
  - **Transmission Lines**
  - **Switching elements.**
- **Transmission lines** move bits between machines.They can be made of copper wire, optical fiber, or even radio links.
- **Switching elements**, or just switches, are specialized computers that connect two or more transmission lines.
- When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.
- These switching computers have been called by various names in the past; the name **router** is now most commonly used.

Types of Computer Networks

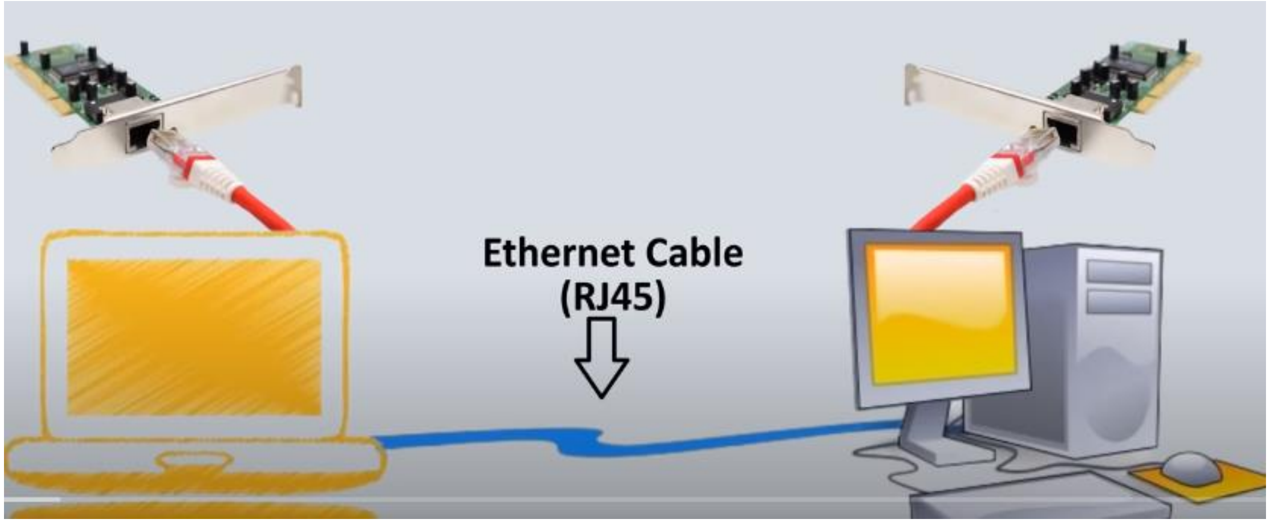


Reference Models

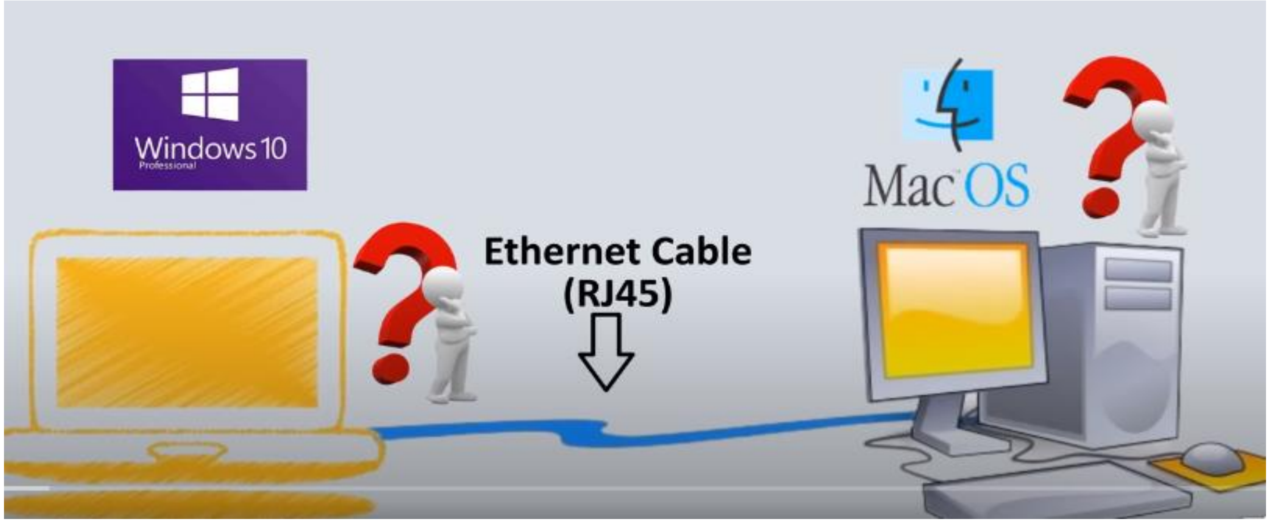
1. **The OSI Reference Model**
2. **The TCP/IP Reference Model**

Why Reference Models?

[1]



[2]

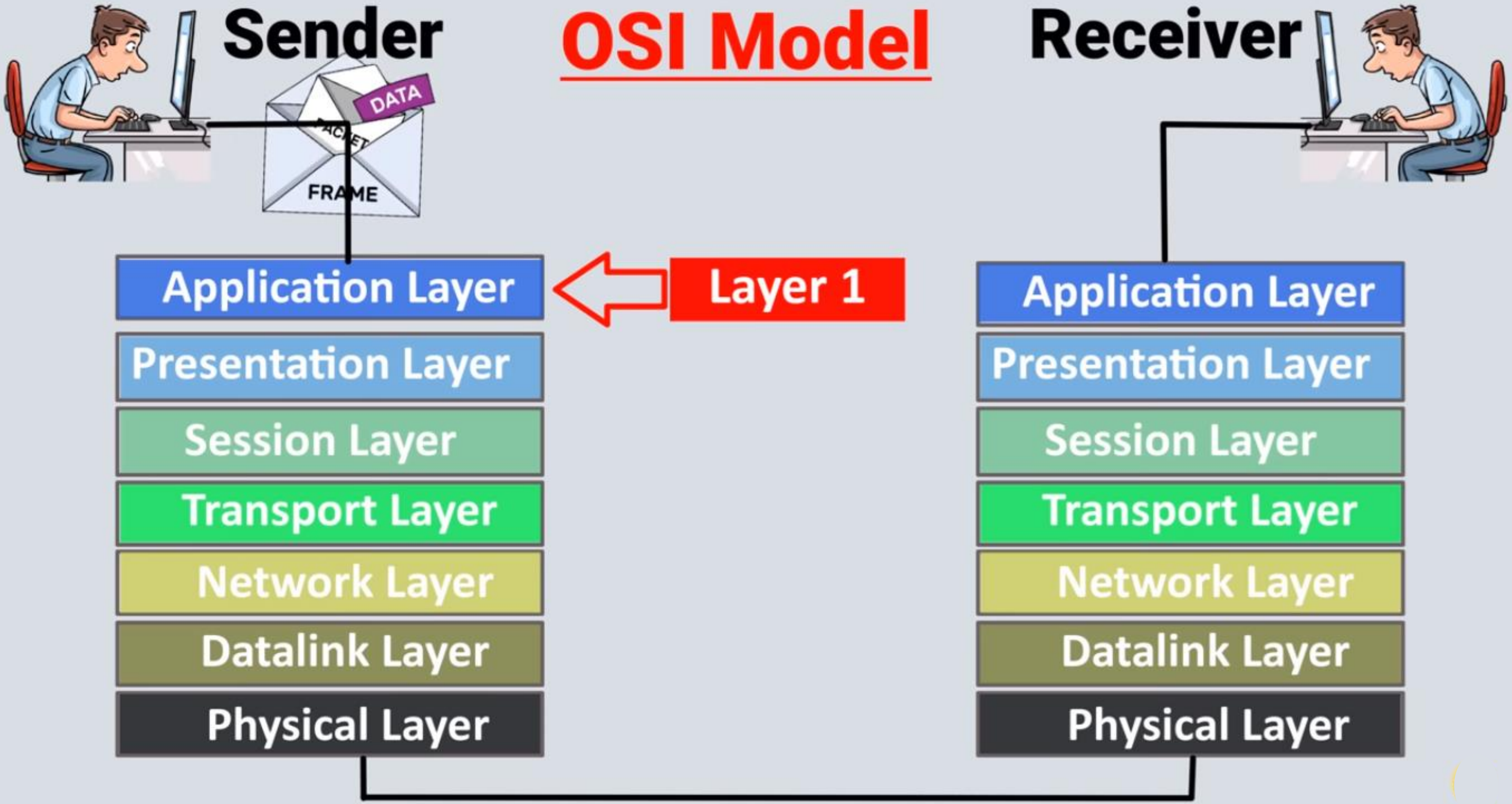


- ★ The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are both **conceptual frameworks** used to **understand and describe how data communication occurs over a network.**
- ★ They both break down the communication process into **layers**, but there are some key differences between the two models.
- ★ Both models serve as important tools for understanding network communication, and their concepts are used in the design and implementation of modern networks and protocols.
- ★ The TCP/IP model's practical implementation and widespread use have made it the dominant reference model in today's networking landscape.

OSI Reference Model

- OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization for Standardization**', in the year **1984**.
- The OSI (Open Systems Interconnection) reference model is **a conceptual framework** used to understand and standardize how different networking protocols and technologies interact and communicate with each other.
- The purpose of OSI reference model is to gude technology vendors(Microsoft,CISCO) and developers , so their H/W and S/W can interoperate and define common framework.
- 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.

OSI Model



Sender

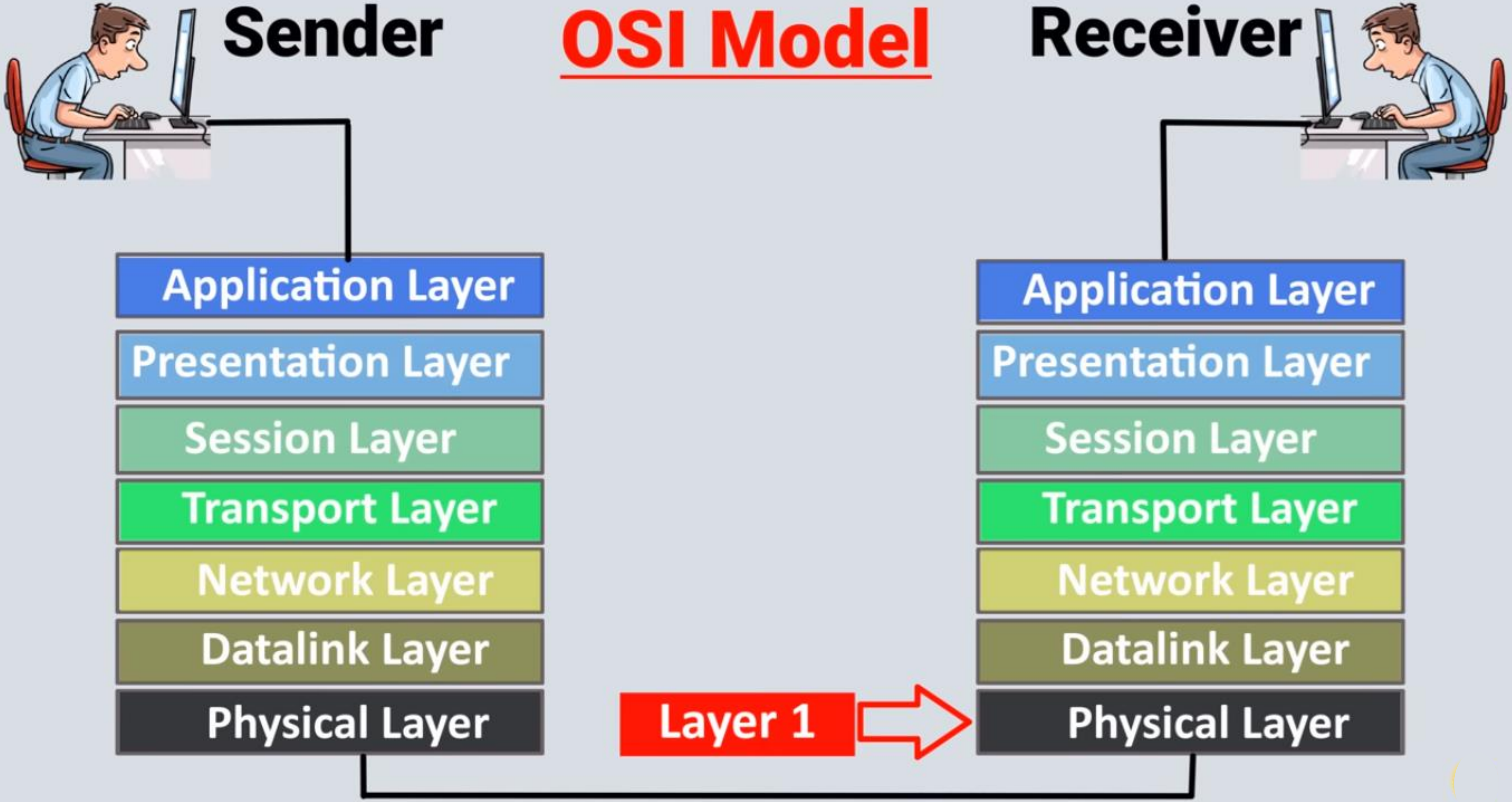
Receiver

Layer 1

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Datalink Layer
Physical Layer

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Datalink Layer
Physical Layer

OSI Model



Sender

Receiver

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Datalink Layer

Physical Layer

Layer 1

Application Layer

Presentation Layer

Session Layer

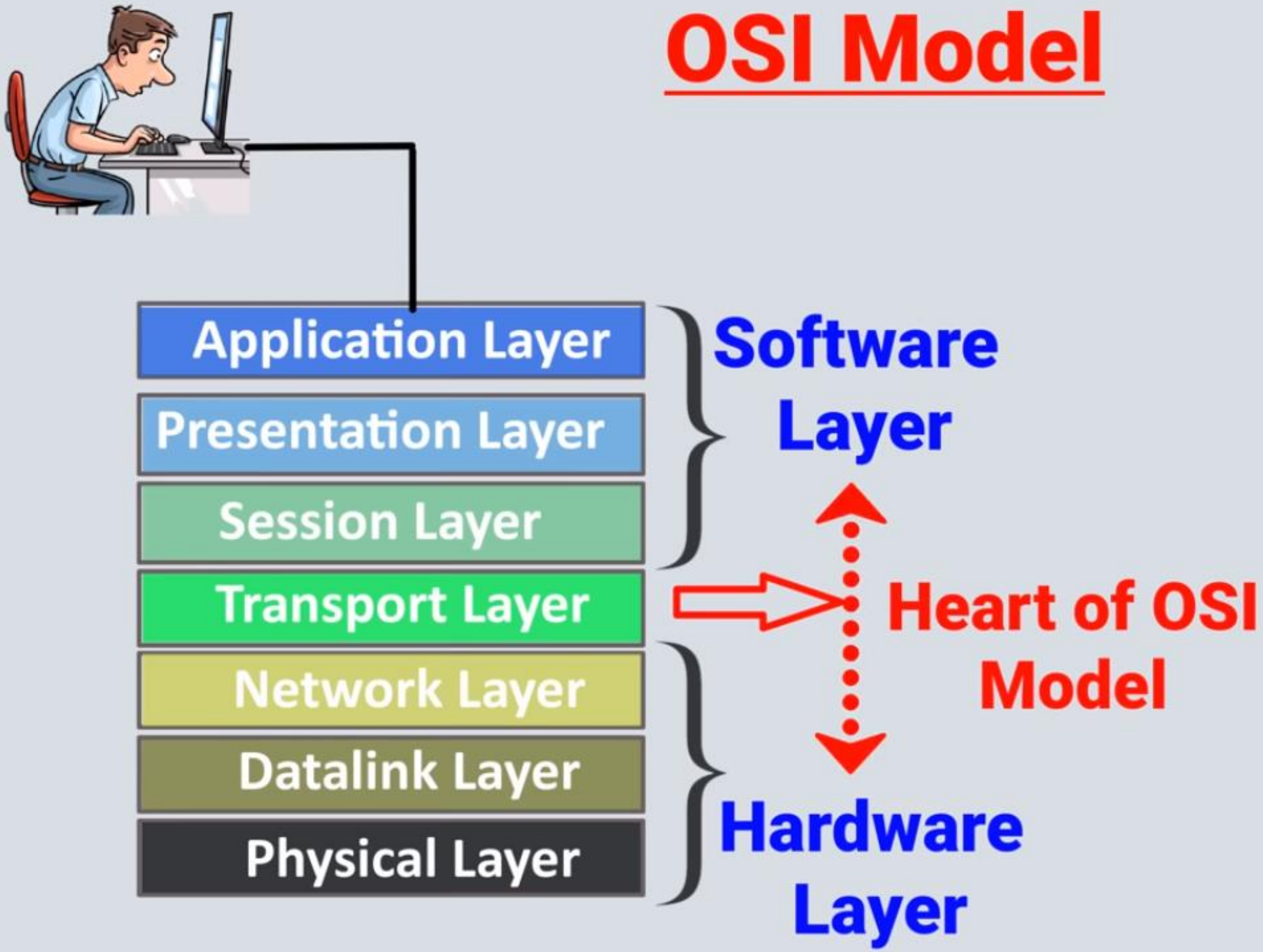
Transport Layer

Network Layer

Datalink Layer

Physical Layer

OSI Model



Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Datalink Layer

Physical Layer

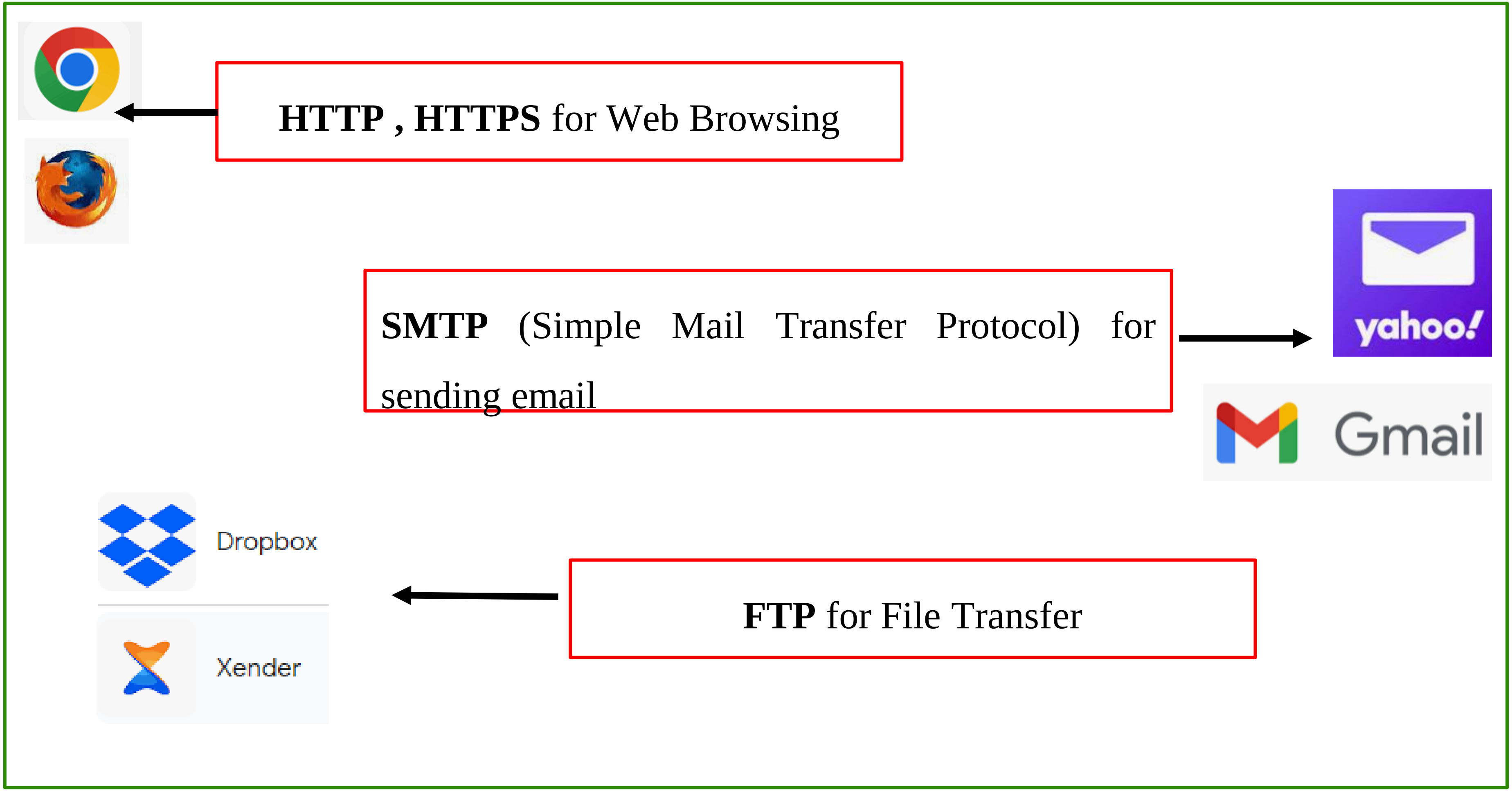
Software Layer

Heart of OSI Model

Hardware Layer

Application Layer

- ★ At the very top of the OSI Reference Model stack of layers.
- ★ It provides **interface to end user**.The application Layer is also called **Desktop Layer**
- ★ Its **primary focus** is to enable communication between software applications running on different devices across a network.
- ★ All applications and Softwares we use in daily life like **Google chrome, Firefox,Drop box , Yahoo**..etc, that all work with the help of Application layer protocols.
- ★ Some examples of Application layer protocols include **HTTP** (Hypertext Transfer Protocol) for web browsing, **SMTP** (Simple Mail Transfer Protocol) for sending email, **FTP** (File Transfer Protocol) for file transfers, and **DNS** (Domain Name System) for translating domain names to IP addresses.

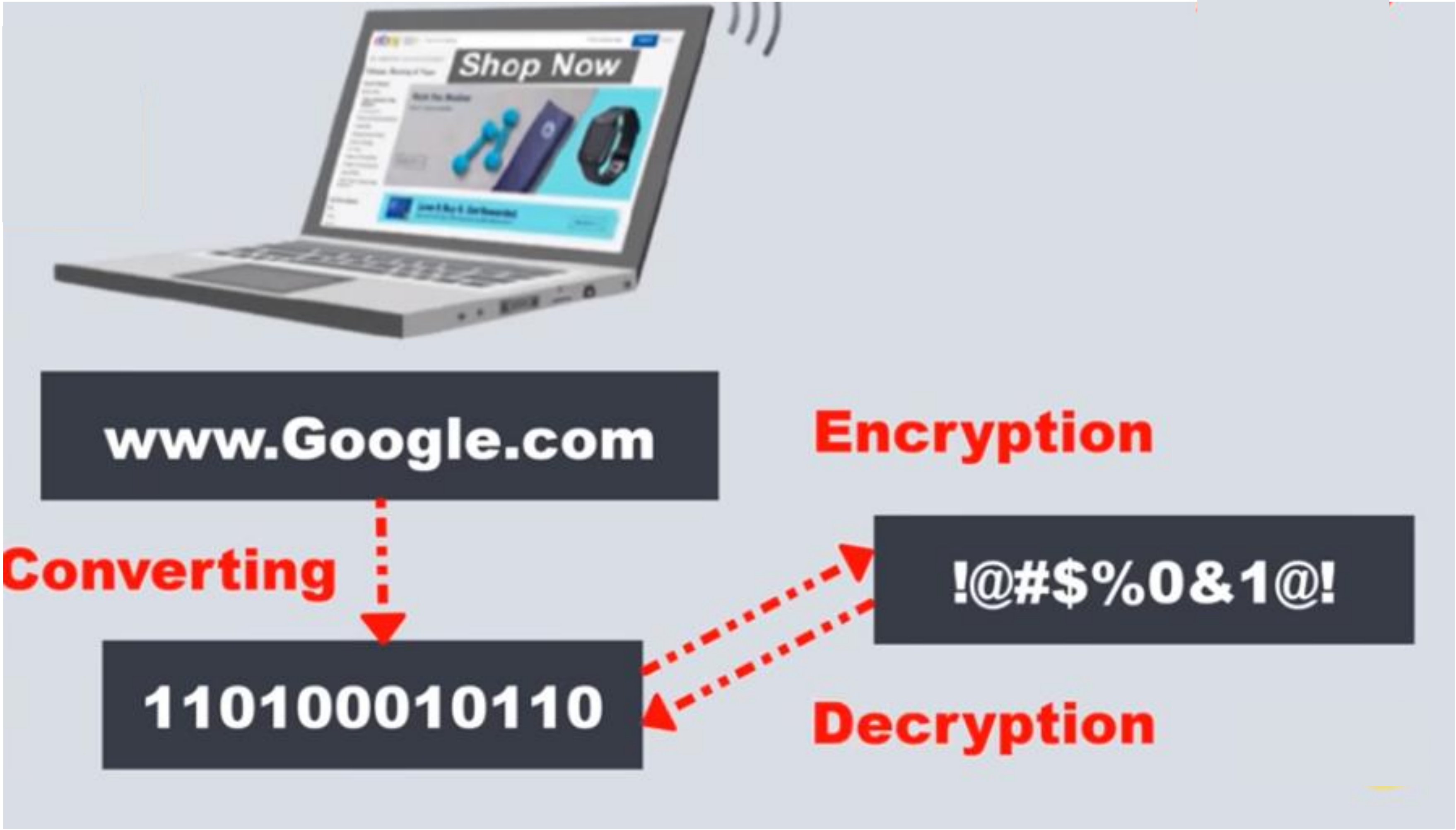


HTTP , HTTPS for Web Browsing

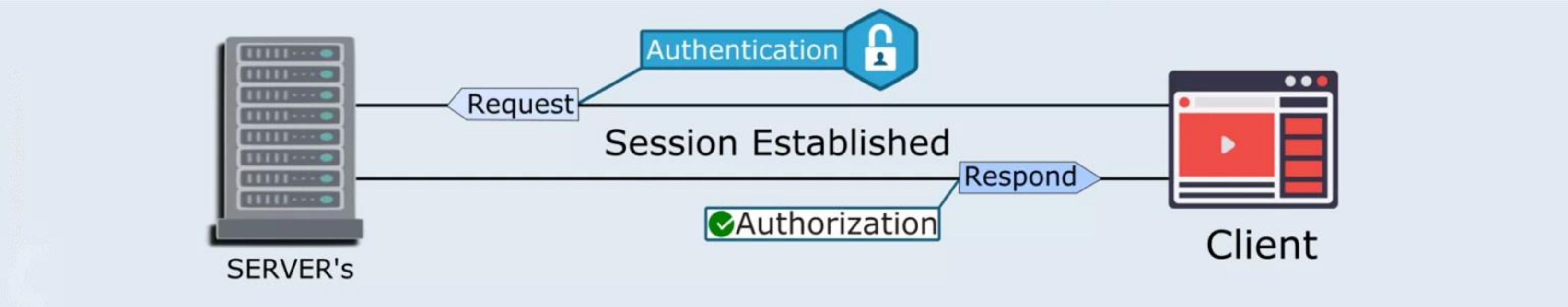
SMTP (Simple Mail Transfer Protocol) for sending email

FTP for File Transfer

Presentation Layer

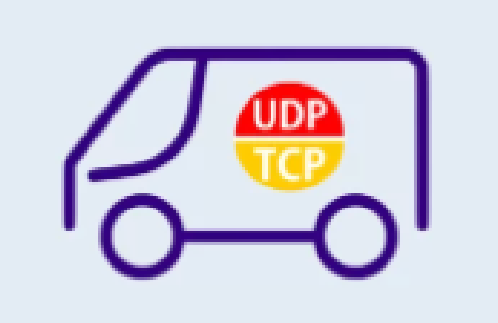

Shop Now
www.Google.com
Encryption
Converting
!@#$%0&1@!
11010001011O
Decryption

- 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.
    - i.e Converts Application layer data into Machine understandable binary format (1’s and 0’s).
- **The Functions of the Presentation Layer are**
    - **Translation**: The Presentation Layer translates data from the application layer's format into a common format that can be understood by both the sender and receiver. This translation is necessary when different systems use different data formats.
    - **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. This ensures that data remains confidential and protected from unauthorized access.
    - **Compression:** Reduces the number of bits that need to be transmitted on the network.



Session Layer

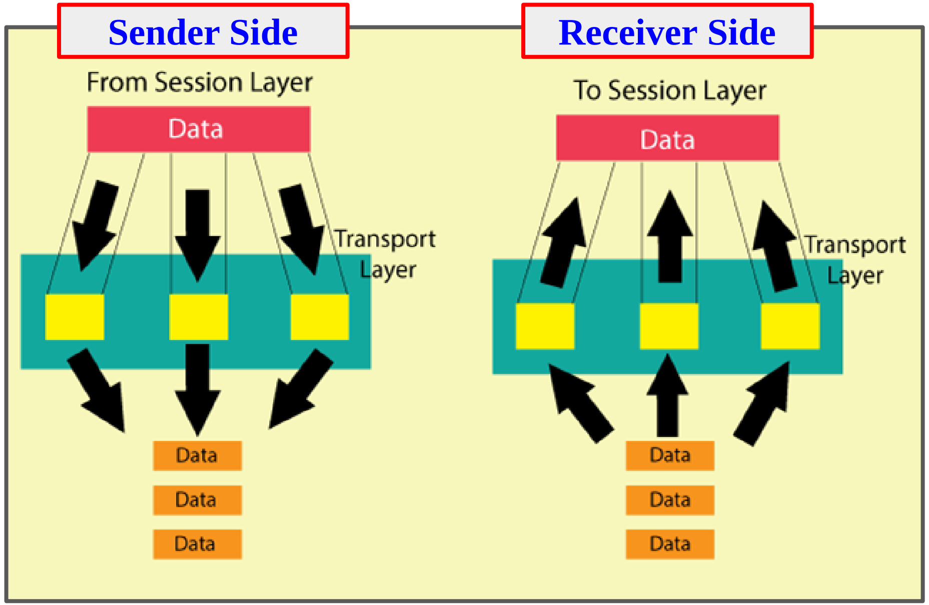
- ➔ Session Layer is responsible for establishing, maintaining, and terminating sessions or connections between two communicating devices on a network. Its primary goal is to provide synchronization and coordination between the two endpoints to enable reliable data exchange.
- ➔ Key functions of the Session Layer include
  - ◆ **Session Establishment:** The Session Layer is responsible for setting up and initiating communication sessions between two devices. It establishes a logical connection between the sender and receiver before data exchange begins.
  - ◆ **Session Maintenance:** Once the session is established, the Session Layer ensures its stability and integrity during the data transfer. It manages the session and monitors its status to handle any issues that may arise.
  - ◆ **Session Termination:** When the communication between the devices is complete, the Session Layer terminates the session in an organized manner, releasing any allocated resources and freeing up system memory.

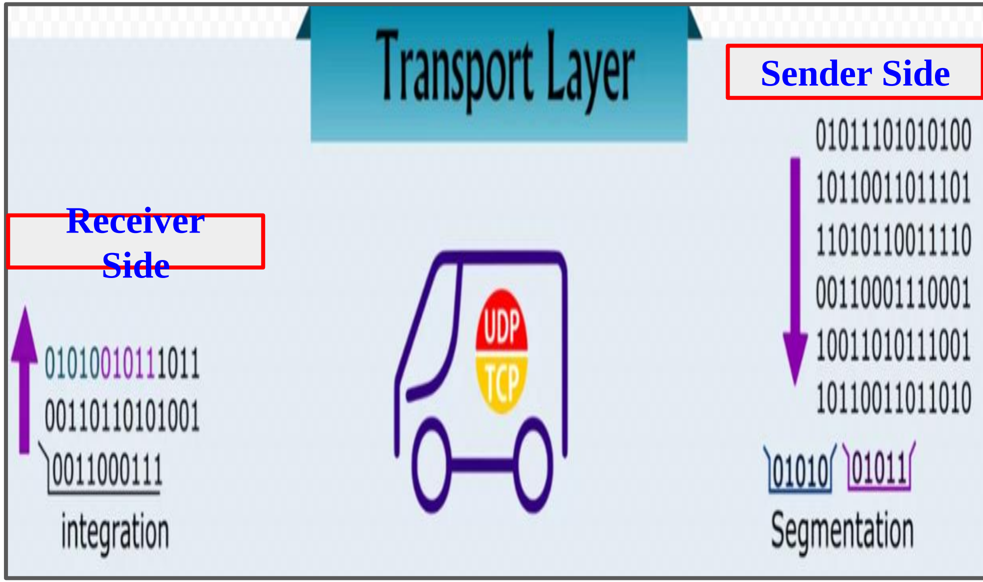


Transport Layer

- The Transport layer is responsible for the transmission of data across network connections.
- The transport layer provides services to the application layer and takes services from the network layer.
- The transport layer is called as **Heart of the OSI model.**
- 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.
- The Functions of the Transport Layer are :
  - **Segmentation and Reassembly**
  - **Flow Control**
  - **Error control**

1. Segmentation and Reassembly

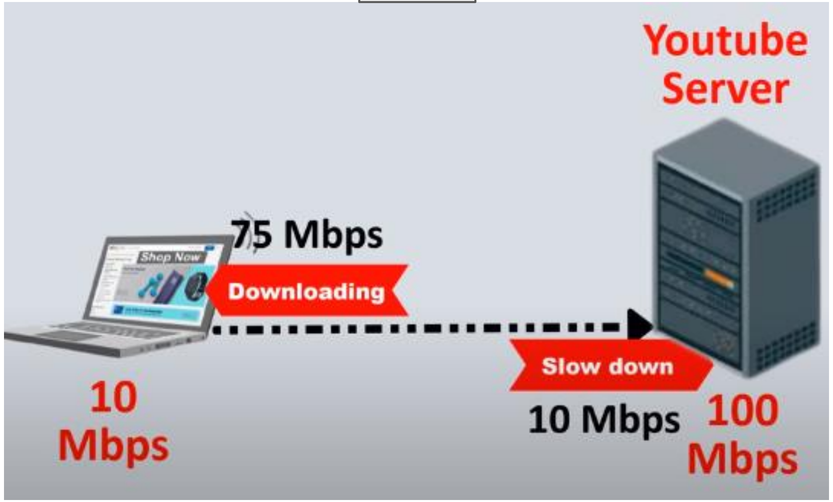




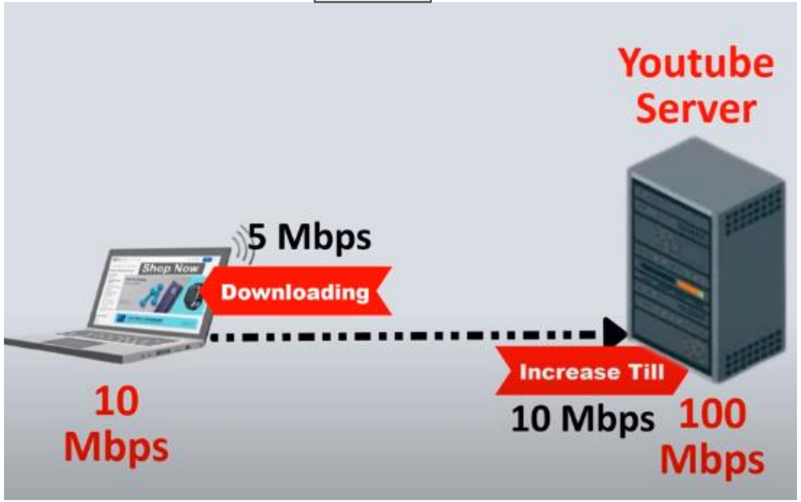
- Transport layer **breaking up messages into smaller segments**, then transmitting them over the network.
- The transport layer also **reassembles the segments into the original message** when they reach their destination.

2. Flow Control

1



2



- The Transport Layer manages the flow of data between the sender and receiver to prevent overwhelming the receiver with data.
- It uses flow control mechanisms to regulate the rate of data transmission and ensure that the receiver can handle the incoming data..

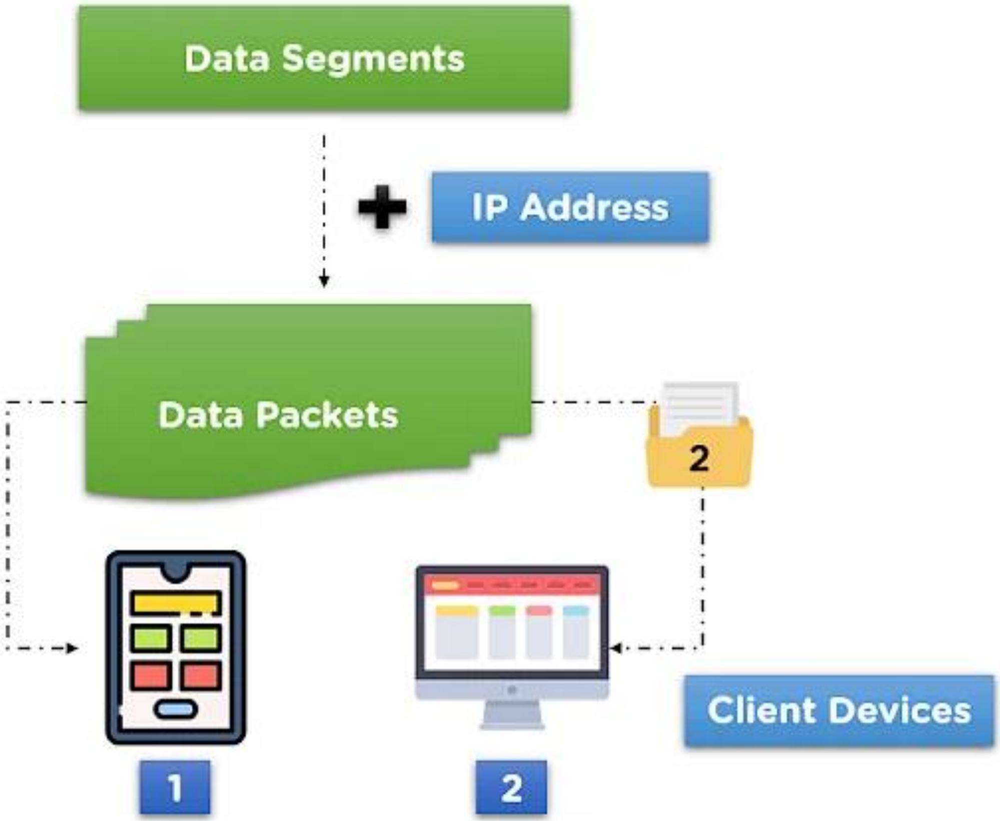
- **Error Control:** This layer is responsible for error detection and correction. It checks for errors in the received data and requests retransmission of any lost or corrupted segments to ensure the data's integrity.

Transport layer protocols

- Protocols in the transport layer of the OSI model provide **communication between applications on different hosts.**
- The two main **Transport layer protocols** are:
  - **Transmission Control Protocol [TCP]**
    - The Transmission Control Protocol (TCP) is **connection-oriented**, meaning that before exchanging data, the two applications must establish a connection between them.
    - After the connection is established, packets are sent and received reliably.
    - It provides **reliable** communication between two hosts.
  - **User Datagram Protocol [UDP]**
    - The User Datagram Protocol (UDP) is **connectionless**, meaning that data is exchanged without establishing a connection.
    - Packets are sent and received without any guarantees about their order or delivery(**Unreliable**).

Network Layer

Logical Addressing:



Data Segments

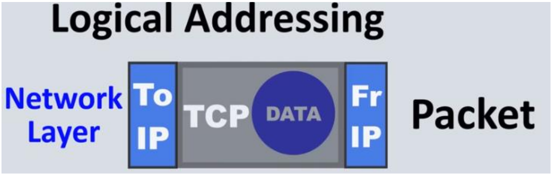
IP Address

Data Packets

Client Devices

- The Network layer operates above the data link layer (Layer 2) and below the transport layer (Layer 4) in the OSI model.
- It is responsible for delivery of data from original source to destination.

Services provided by the Network layer are:

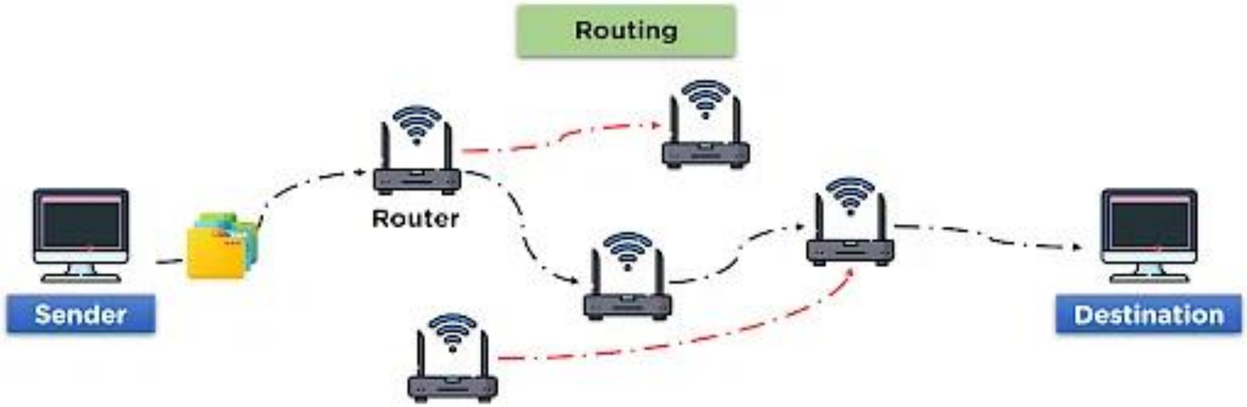


Logical Addressing:

- It is responsible for breaking down the **data segments into data packets** and is tasked with **reassembling** them on the receiver side.
- Devices at the network layer are identified using logical addresses, such as IP (Internet Protocol) addresses. The network layer adds the source and destination IP addresses to the data packets to ensure proper delivery.

Routing:

- The Network layer determines the **most efficient path** for data packets to travel from the source to the destination across multiple networks.
- It uses **routing algorithms** and protocols to make forwarding decisions based on the network topology and destination address.



Congestion:

- The network layer can detect and respond to network congestion, either by slowing down the rate of packet transmission or by using other congestion control mechanisms.

What is Congestion:

- Congestion in the network layer is a situation where **the network is overloaded with traffic**, and this can lead to a number of problems, including:
    - **Packet loss**
    - **Increased delay**

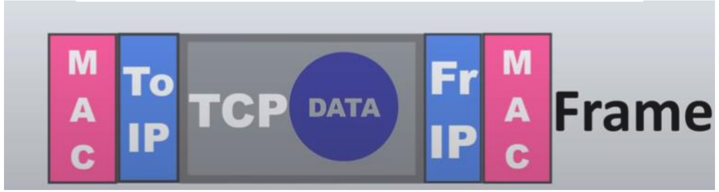
Data Link Layer

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

Services provided by Data Link Layer:

1.Framing:

Physical Addressing



★ The Data Link Layer takes the **packets** received from the Network Layer and encapsulates them into **frames** for transmission over the physical medium. At the receiving end, it extracts the data from the frames and passes it up to the Network 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(Media Access Control).**

★ MAC addresses are used for addressing and delivering data frames to the correct destination on the same network.

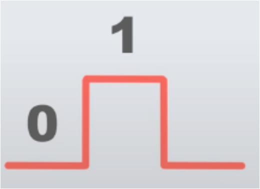
2. Error Detection and Correction: The data link layer is responsible for **error detection** at the link level. It checks for transmission errors in received frames using error-checking mechanisms like **CRC (Cyclic Redundancy Check).** If errors are detected, the layer can request **retransmission** of the corrupted frames.

3. Flow Control: The Data Link Layer manages the flow of data between devices to avoid overwhelming the receiving end. It ensures that data is sent at a rate that the receiving device can handle.

4. Access control :It ensures that only authorized devices can access the network.

Note:

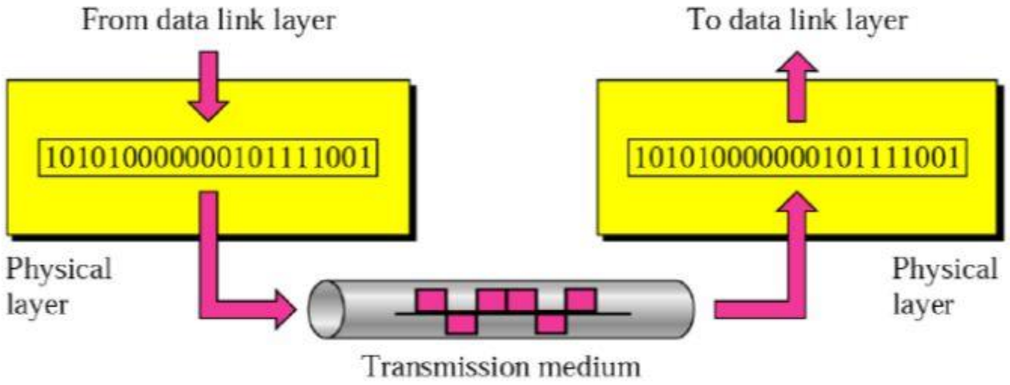
Switch & Bridge are Data Link Layer devices.



Physical Layer

01001010010100011
BitStram
Receiver
Sender

- It deals with the **physical transmission** of **data bits** over a physical medium, such as **copper cables, fiber optics, or wireless channels**.
- The primary function of the Physical Layer is to establish and maintain a physical link between network devices and transmit **raw binary data** as electrical or optical signals.
- It is also responsible for converting the **data frames** received from the Data-link layer into data **bits of 1's and 0's (raw bits)**for transmission over the network.



- The physical layer consists of **three** main components:
    - Transmission media
    - Transceivers
    - Connectors
- **Transmission media** includes **wires, cables, and optical fibers**.
- **Transceivers** convert **electrical signals into optical or radio signals**.
- **Connectors** attach transmission media to devices such as **computers,hub,repeaters,modems .**

Note:

Hub, Repeater, Modem, and Cables are Physical Layer devices.

Data Format	Layer	Function
Data	Application Layer	Applications access network services
Data	Presentation Layer	Translations ,Encryption and decryption of data
Data	Session Layer	Connection management b/w networks
Segment	Transport Layer	Segmentation,Flow control, responsible for End-to-end delivery
Packet	Network Layer	Adding IP add, Determine the path for data transfer
Frame	Data Link Layer	Framing, Error detection and correction
Raw Bits	Physical Layer	Transfer raw bits using physical media

TCP/IP Model

OSI model acts as a reference model and is not implemented on the Internet because of its late invention. **The current model being used is the TCP/IP model.**

- 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.

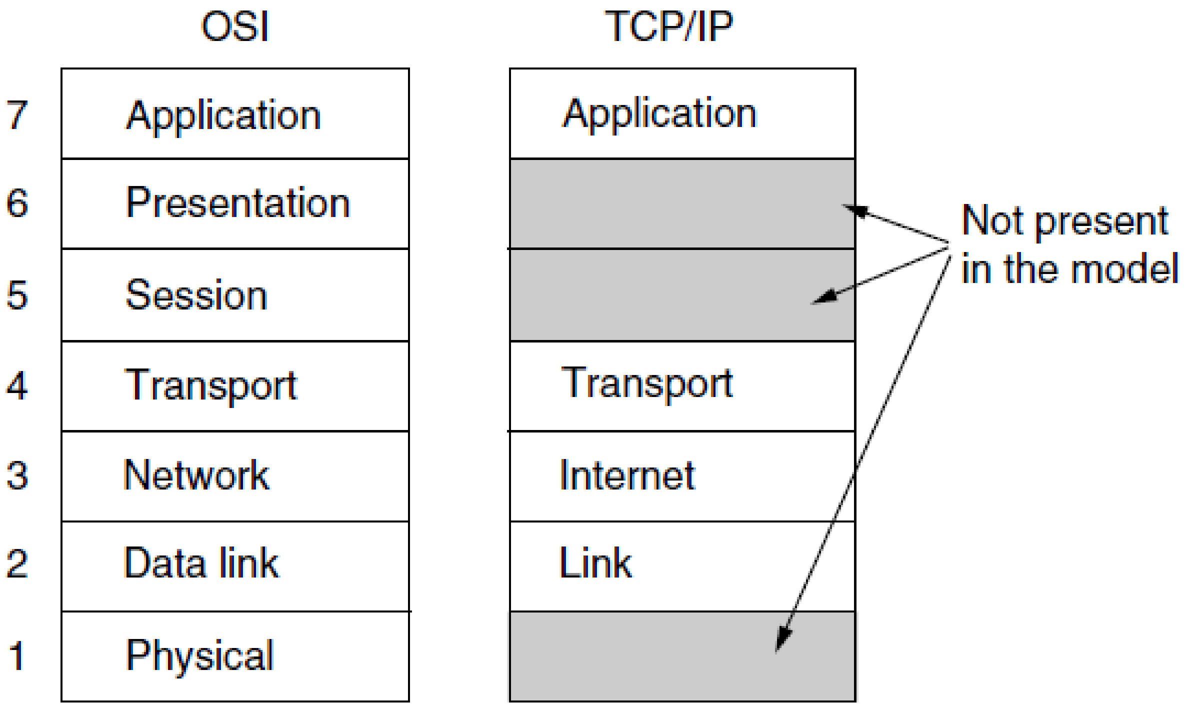


Figure 1-21. The TCP/IP reference model.

The Link Layer [Network Access Layer]

- A Network Access Layer is the lowest layer of the TCP/IP model.
- A Network Access Layer is the combination of the **Physical layer and Data Link layer** defined in the OSI reference model.
- The Link Layer is the lowest layer of the TCP/IP model and handles t**he physical transmission** of data over the network medium.
- It is responsible for defining hardware-specific details such as **MAC (Media Access Control)** addresses for devices, **error detection**.
- The functions carried out by this layer are encapsulating the **IP datagram into frames** transmitted by the network and mapping of IP addresses into physical addresses.
- The **protocols** used by this layer are **ethernet, token ring, FDDI, X.25, frame relay.**

The Internet Layer

- An Internet layer is the second layer of the TCP/IP model.
- An Internet layer is also known as **the network layer.**
- The Internet layer is responsible for **Logical Addressing, Routing, and Congestion Control** data packets across different networks.

The main protocols residing at this layer are as follows:

1. **IP** (Internet Protocol)
2. **ICMP** (Internet Control Message Protocol)
3. **ARP** (Address Resolution Protocol)

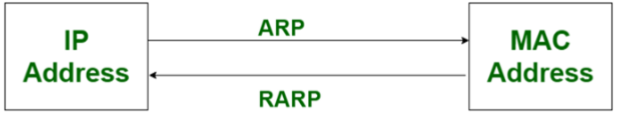
1. IP (Internet Protocol) :

- ★ 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.

1. ICMP (Internet Control Message Protocol):

- ★ It is encapsulated within IP Packets and is responsible for providing hosts with information about **network conditions or to report errors.**

1. ARP (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.

The Transport Layer

1. The Transport Layer is responsible for managing **end-to-end communication** and **ensures reliable data delivery** between applications running on different devices.
2. It handles the **segmentation and reassembly** of data, as well as **flow control and error recovery.**
3. It The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error.
4. It ensures that data is delivered in the correct order, without loss or duplication. The most commonly used protocols at this layer are the
   1. **Transmission Control Protocol (TCP)**, which is connection-oriented and guarantees reliable delivery.
   2. **User Datagram Protocol (UDP)**, which offers a connectionless and faster but less reliable delivery option.

The Application Layer

- ★ The TCP/IP model does not have session or presentation layers.
- ★ The Application layer is responsible for supporting end-user applications and their protocols.

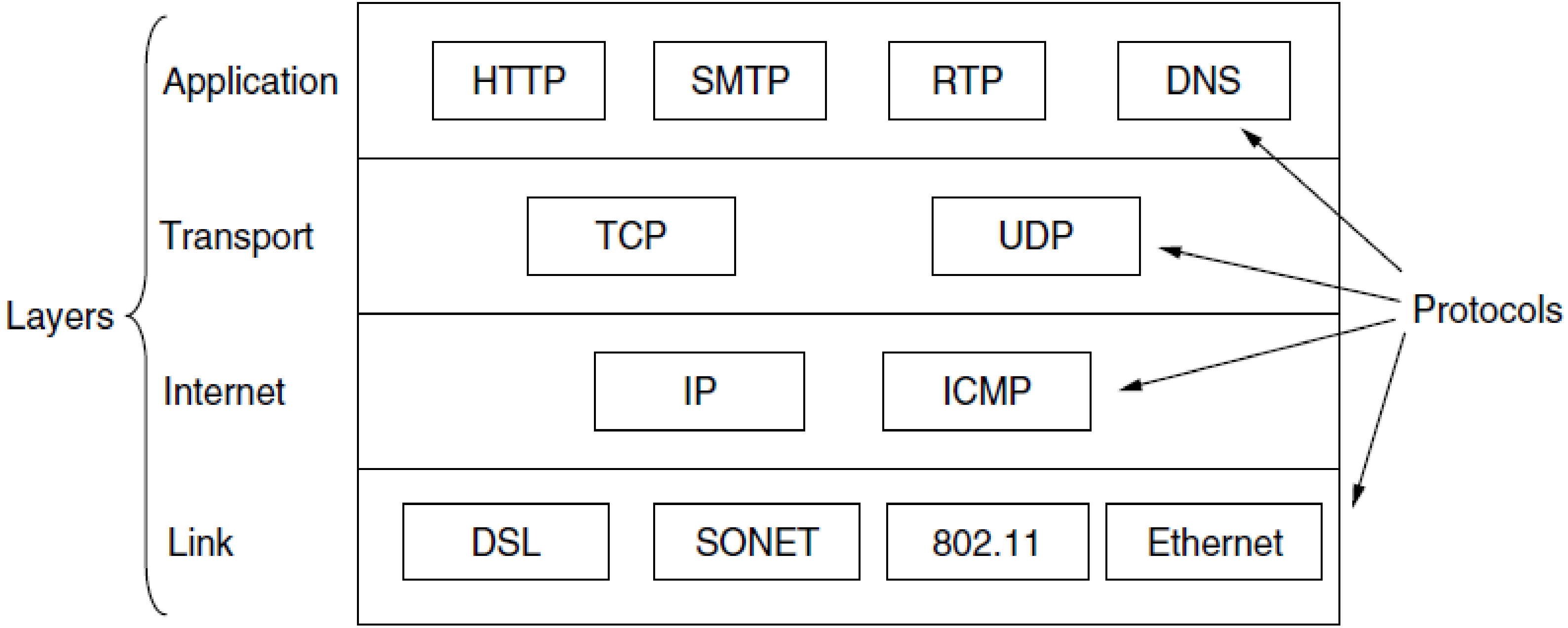
It contains all the higher-level protocols.

- ★ **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.

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. i.e. HTTP takes care of Web Browsers and Websites.
- **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.
- **SNMP:** Simple Network Management Protocol is used for **managing and monitoring network devices and systems**. It is commonly used in network management systems to collect information, configure devices, and monitor network performance.

- ★ **DNS:** The DNS (Domain Name System) protocol is an application-layer protocol used to translate human-readable domain names, such as **"www.google.com,"** into their corresponding IP addresses.
- ★ **RTP:** The RTP (Real-time Transport Protocol) for delivering real-time media such as voice or movies over networks.



Layers

Application: HTTP, SMTP, RTP, DNS

Transport: TCP, UDP

Internet: IP, ICMP

Link: DSL, SONET, 802.11, Ethernet

Protocols

Figure 1-22. The TCP/IP model with some protocols we will study.

OSI vs TCP/IP Reference Model

Assignment Topic