

# UNIT-7 : Data communication computer Network

**Contains:** Introduction, Importance of Networking,

- ❑ Data Transmission Media, Data Transmission across Media, Data Transmission and Data Networking ,
  - ❑ Computer Network, Network Types : LAN, MAN, WAN Network Topology,
- ❑ Communication Protocol, What is communication protocol? ISO model and its seven layers,
  - ❑ Network Devices, NIC, Repeater, Bridge, Hub, Switch, Router and Gateway,
- ❑ Wireless Networking , Introduction and uses of wireless networking. Bluetooth, wireless LAN and Wireless WAN.

# Introduction to Data Communication

- **Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.**
- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).
- A computer network is a system of interconnected computers and peripheral devices. For example, it may connect computers, printers, scanners and cameras.
- Communications is about the transfer of information from a sender, across a distance, to a receiver.
- Communication is an act of transmitting messages.
- **Computer networking** enables employees to share ideas more easily and work more efficiently.
- It increases their productivity and generates more income for the company.
- More importantly, **computer networking** improves the way companies offer their services to the world.

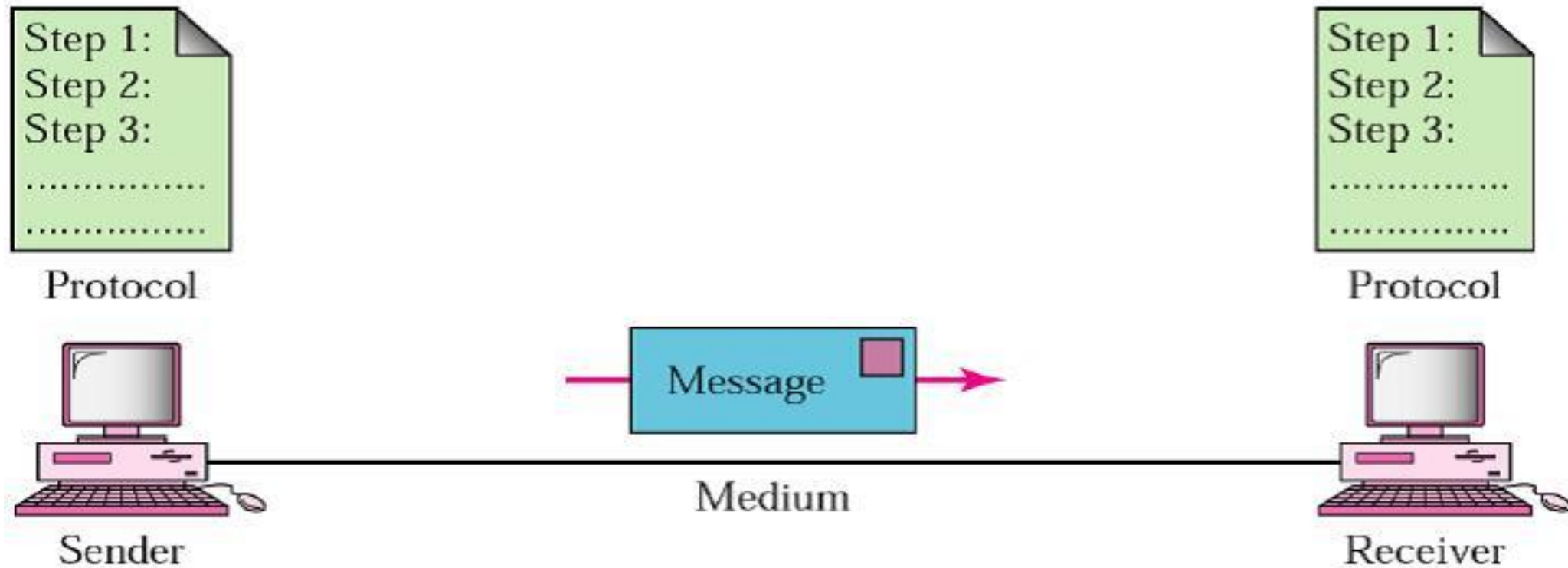
# Data Communication Fundamental Characteristics

- *The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.*

- 1. Delivery** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
- 2. Accuracy.** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable
- 3. Timeliness.** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
- 4. Jitter** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets

# Components of Data Communication

- A data communications system has five components

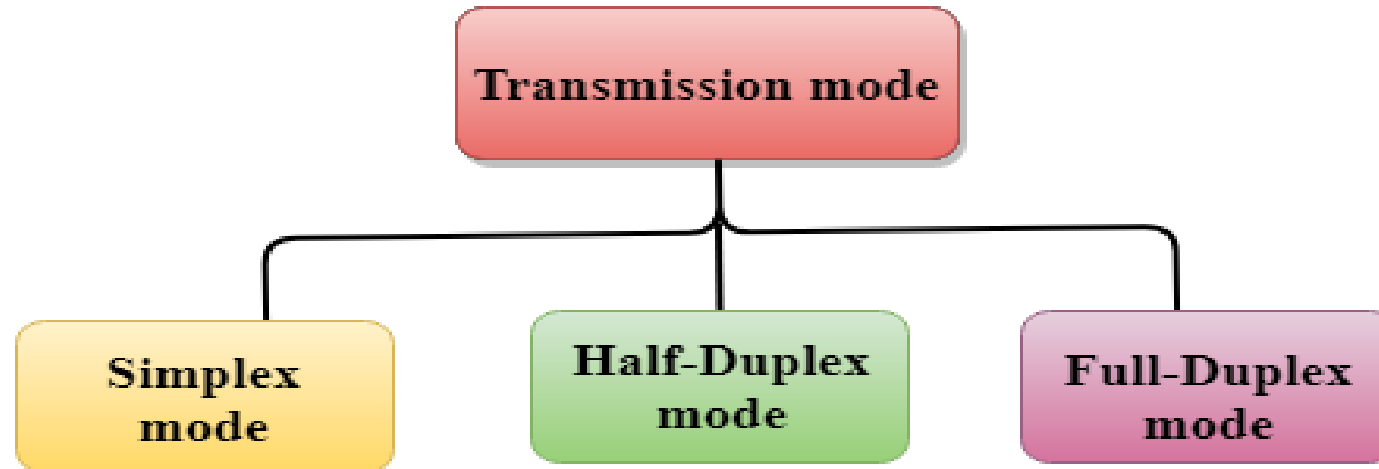


# Components of Data Communication Cont..

- 1. Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- 2. Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
- 3. Receiver:** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- 4. Transmission medium:** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber optic cable, and radio waves.
- 5. Protocol:** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

# Mode of Data Communication

- Communication between two devices can be simplex, half-duplex, or full-duplex



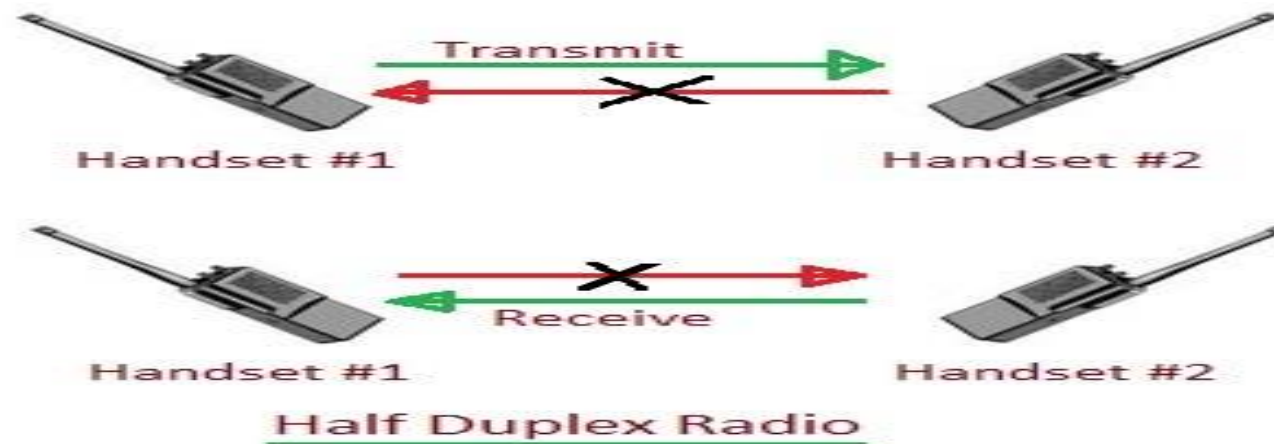
## Simplex:

- In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.
- Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

# Mode of Data Communication Cont..

- **Half-Duplex:**

- In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- Walkie talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction



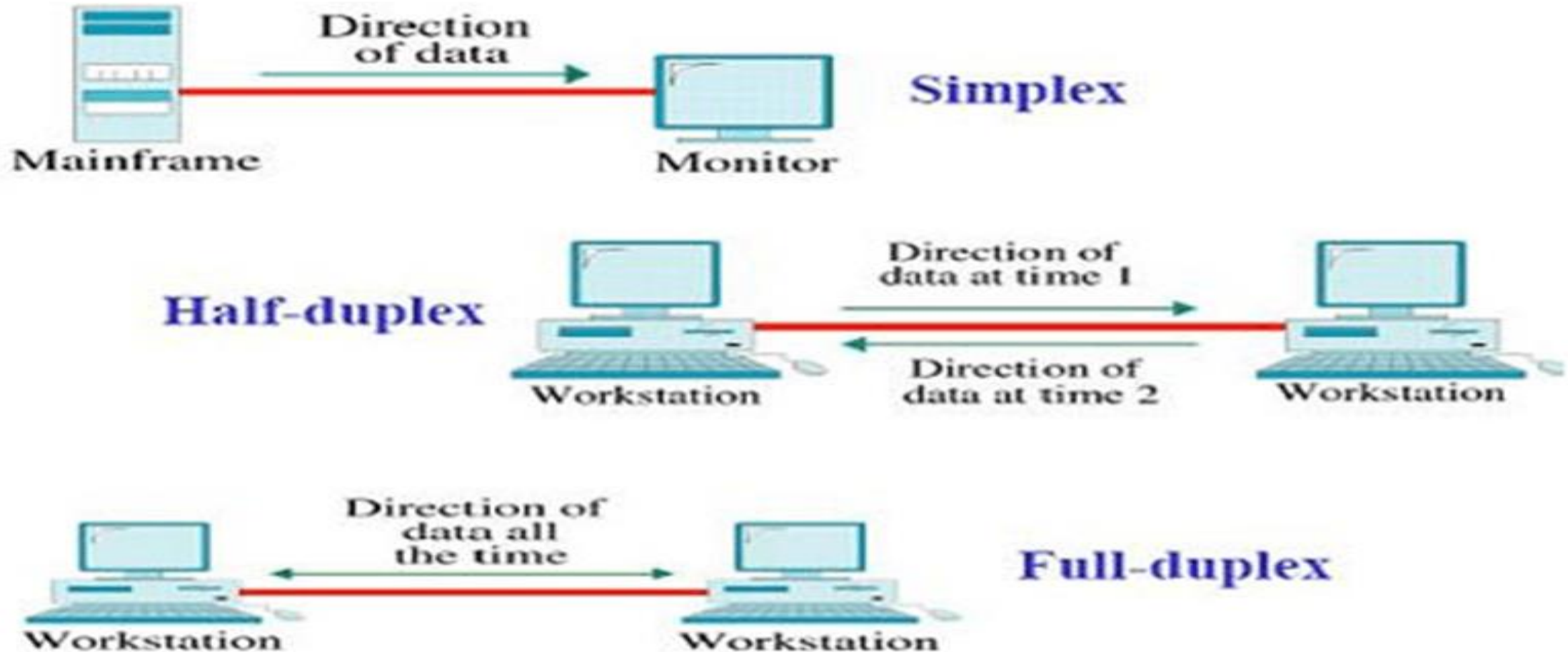
# Mode of Data Communication Cont..

## Full-Duplex:

- In full-duplex both stations can transmit and receive simultaneously.
- In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction.
- One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.
- The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

# Mode of Data Communication Cont..

## Transmission Mode



# Computer Network

- A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

## Network Criteria

- A network must be able to meet a certain number of criteria.
- The most important of these are performance, reliability, and security

# Computer Network Cont..

## 1. 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, the capabilities of the connected hardware, and the efficiency of the software

## 2. Reliability:

Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness ( the quality or condition of being strong and in good condition) in a catastrophe.(often unexpected breakdown in a machine)

**3. Security:** Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

# Types of Connections

## 1. Point-to-Point

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.

A **point-to-point connection** refers to a communications **connection** between two nodes or endpoints.

An **example** is a telephone call, in which one telephone is **connected** with one other, and what is said by one caller can only be heard by the other.

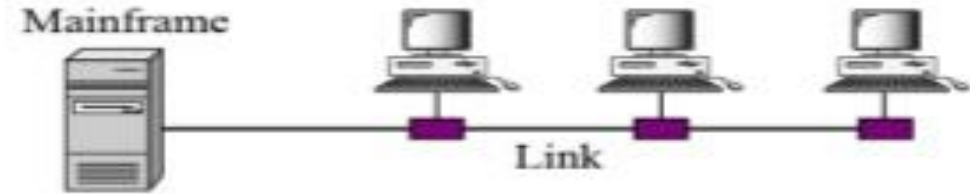
## 2. Multipoint

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.

In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



a. Point-to-point



b. Multipoint

## Point-to-point

- A dedicated line between two devices
- The entire capacity of the link is reserved for transmission between these two devices

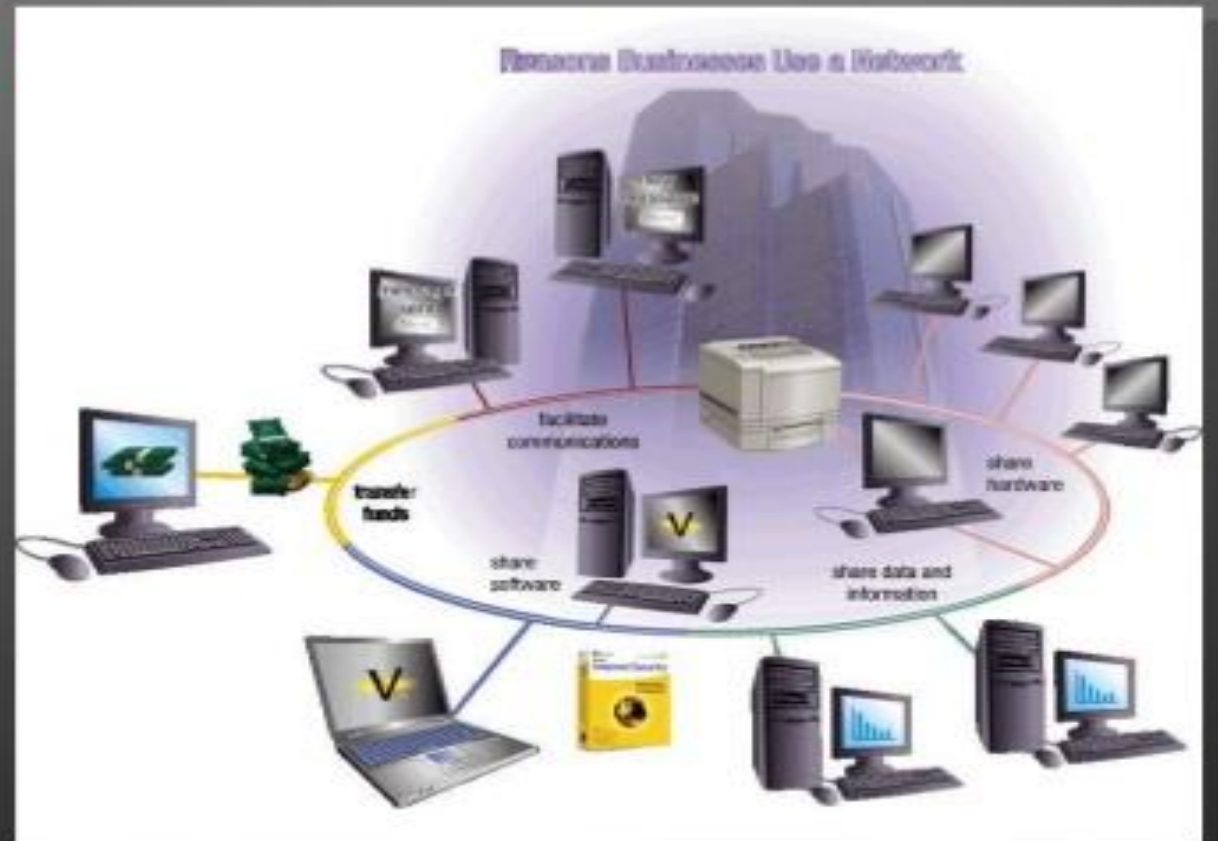
## Multipoint connection (multidrop connection)

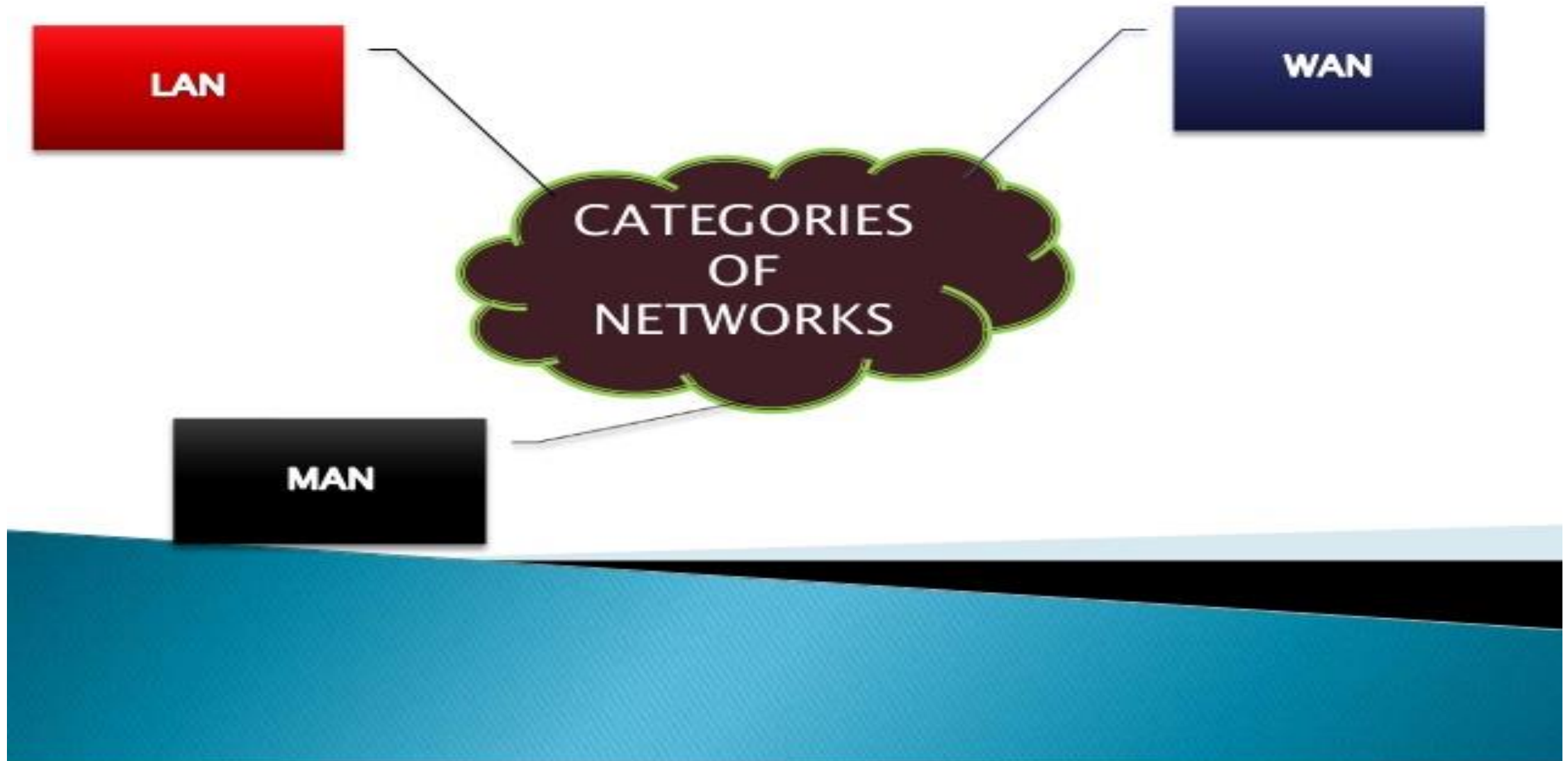
- More than two devices share a single link
- The capacity of the channel is shared, either spatially or temporally

# NETWORKS

## What is a Computer Network?

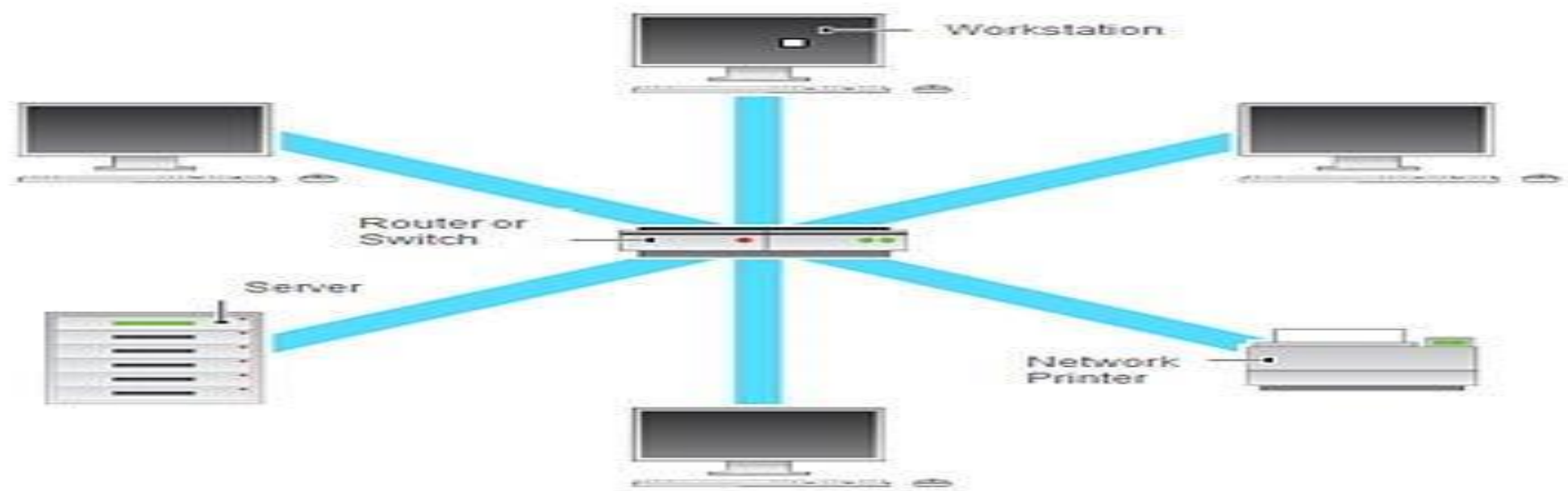
- Collection of **autonomous computers interconnected** by a **single technology** is called computer network.
- Two computers are set to be interconnected if **they are able to exchange information**.
- **Connection** can be through a **copper wire, fiber optics, microwaves, infrared or satellite**.





# Local Area Network (LAN)

- A Local Area Network (LAN) is a private network that connects computers and devices within a limited area like a residence, an office, a building or a campus. On a small scale, LANs are used to connect personal computers to printers.
- However, LANs can also extend to a few kilometers when used by companies, where a large number of computers share a variety of resources like hardware (e.g. printers, scanners, audiovisual devices etc), software (e.g. application programs) and data.



# Local Area Network (LAN) Cont..

## Advantages of LAN

- **Resource Sharing:** LAN provides resource sharing such as computer resources like printers, scanners, modems, DVD-ROM drives, and hard disks can be shared within the connected devices. This reduces cost and hardware purchases.
- **Software Applications Sharing:** In a Local Area Network, it is easy to use the same software in a number of computers connected to a network instead of purchasing the separately licensed software for each client a network.
- **Easy and Cheap Communication:** Data and messages can easily be shared with the other computer connected to the network.
- **Centralized Data:** The data of all network users can be stored on a hard disk of the central/server computer. This help users to use any computer in a network to access the required data.
- **Data Security:** Since data is stored on the server computer, it will be easy to manage data at only one place and the data will be more secure too.
- **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In school labs and internet Cafes, single internet connection is used to provide internet to all connected computers.

# Local Area Network (LAN) Cont..

## Disadvantages of LAN

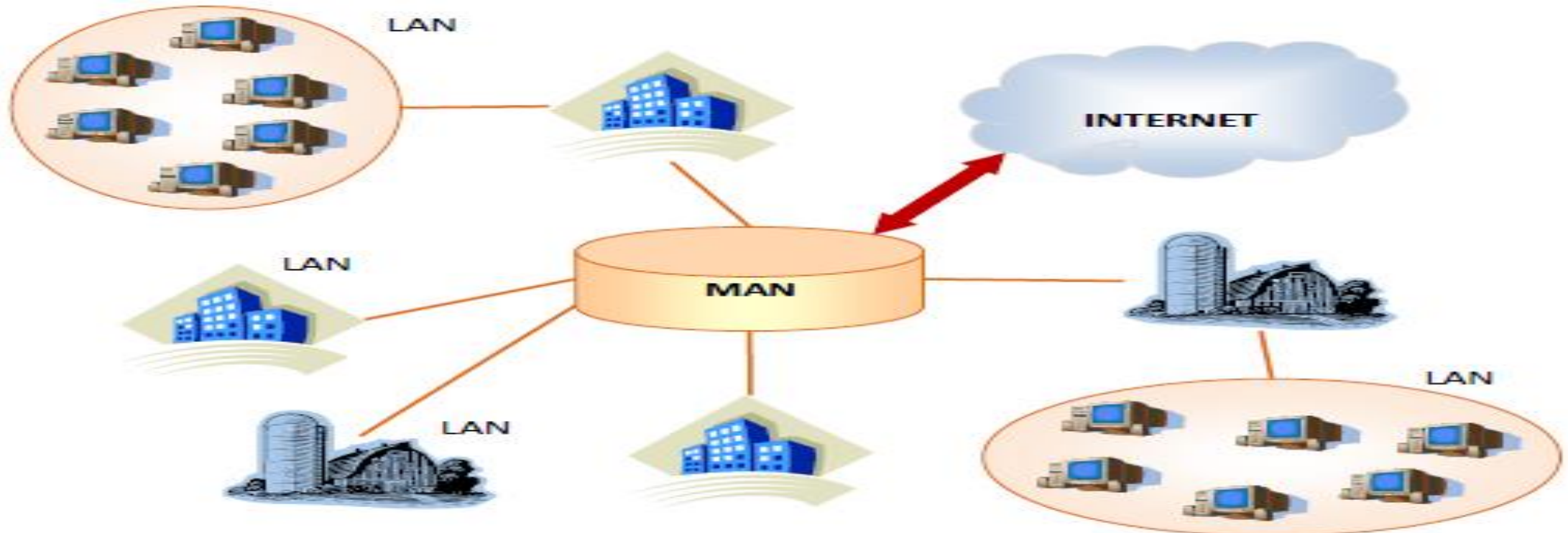
- **High Setup Cost:** The initial setup costs of installing Local Area Networks is high because there is special software required to make a server. Also, communication devices like an Ethernet cable, switches, hubs, routers, cables are costly.
- **Privacy Violations:** The LAN administrator can see and check personal data files of each and every LAN user. Moreover, he can view the computer and internet history of the LAN user.
- **Data Security Threat:** Unauthorised users can access important data of an office or campus if a server hard disk is not properly secured by the LAN administrator.
- **LAN Maintenance Job:** *Local Area Network requires a LAN Administrator* because there are problems such as software installations, program faults or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is required to maintain these issues.
- **Covers Limited Area:** LANs are restricted in size they cover a small area like a single office, single building or a group of nearby buildings.

# Metropolitan Area Network (MAN)

- A metropolitan area network (MAN) is a network with a size greater than LAN but smaller than a WAN. It normally comprises networked interconnections within a city that also offers a connection to the Internet.
- **The distinguishing features of MAN are**
- Network size generally ranges from 5 to 50 km. It may be as small as a group of buildings in a campus to as large as covering the whole city.
- Data rates are moderate to high.
- In general, a MAN is either owned by a user group or by a network provider who sells service to users, rather than a single organization as in LAN.
- It facilitates sharing of regional resources.
- They provide uplinks for connecting LANs to WANs and Internet

# Metropolitan Area Network (MAN) Cont..

- **Example of MAN**
- Cable TV network
- Telephone networks providing high-speed DSL lines
- IEEE 802.16 or WiMAX, that provides high-speed broadband access with Internet connectivity to customer premises.



# Metropolitan Area Network (MAN) Cont..

- **Advantages of a metropolitan area network (MAN)**

- **Less expensive:**

- It is less expensive to attach MAN with WAN. MAN gives the good efficiency of data. In MAN data is easily managed in a centralized way.

- **Sending local emails:**

- On MAN you can send local emails fast and free.

- **High speed than WAN:**

- MAN uses fiber optics so the speed of data can easily reach upon 1000 Mbps. Files and databases can be transferred fast.

- **Sharing of the internet:**

- In some installation of MANs, users can share their internet connection. So multiple users can get the same high-speed internet.

- **Conversion from LAN to MAN is easy:**

- MAN is a faster way to connect two fast LANs together. This is due to the fast configuration of links.

- **High Security:**

- MAN has a high-security level than WAN.

# Metropolitan Area Network (MAN) Cont..

## Disadvantages of metropolitan area network (MAN)

- **Difficult to manage:**
- If MAN becomes bigger then it becomes difficult to manage it. This is due to a security problem and other extra configuration.
- **Internet speed difference:**
- MAN cannot work on traditional phone copper wires. If MAN is installed on copper wires then there will be very low speed. So it required the high cost to set up fiber optics for the first time.
- **Hackers attack:**
- In MAN there are high chances of attacking hackers on the network compared to LAN. So data may be leaked. Data can be secured but it needs high trained staff and security tools.
- **Technical people required to set up:**
- To setup MAN it requires technical people that can correctly setup MAN. The technical people are network administrators and troubleshooters.
- **More wires required:**
- In MAN additional cables are required to connect two LAN which is another problem.

# Metropolitan Area Network (MAN) Cont..

- **Examples of metropolitan area network (MAN)**
- Some of the examples of MAN are:-
- Digital cable television
- Used in government agencies
- University campuses
- Cable broadband
- Used to connect several branches of the local school
- In hospital (for communication between doctors, research offices, labs)
- A network of fire stations
- In airports
- Networking between community colleges within the country
- Used in public libraries

# WAN: WIDE AREA NETWORK

- ▶ **Network** that provides long distance transmission of data, voice, image and video information over large geographical areas that may comprise a country, a continent.
- ▶ **Range:** Beyond 100 km.

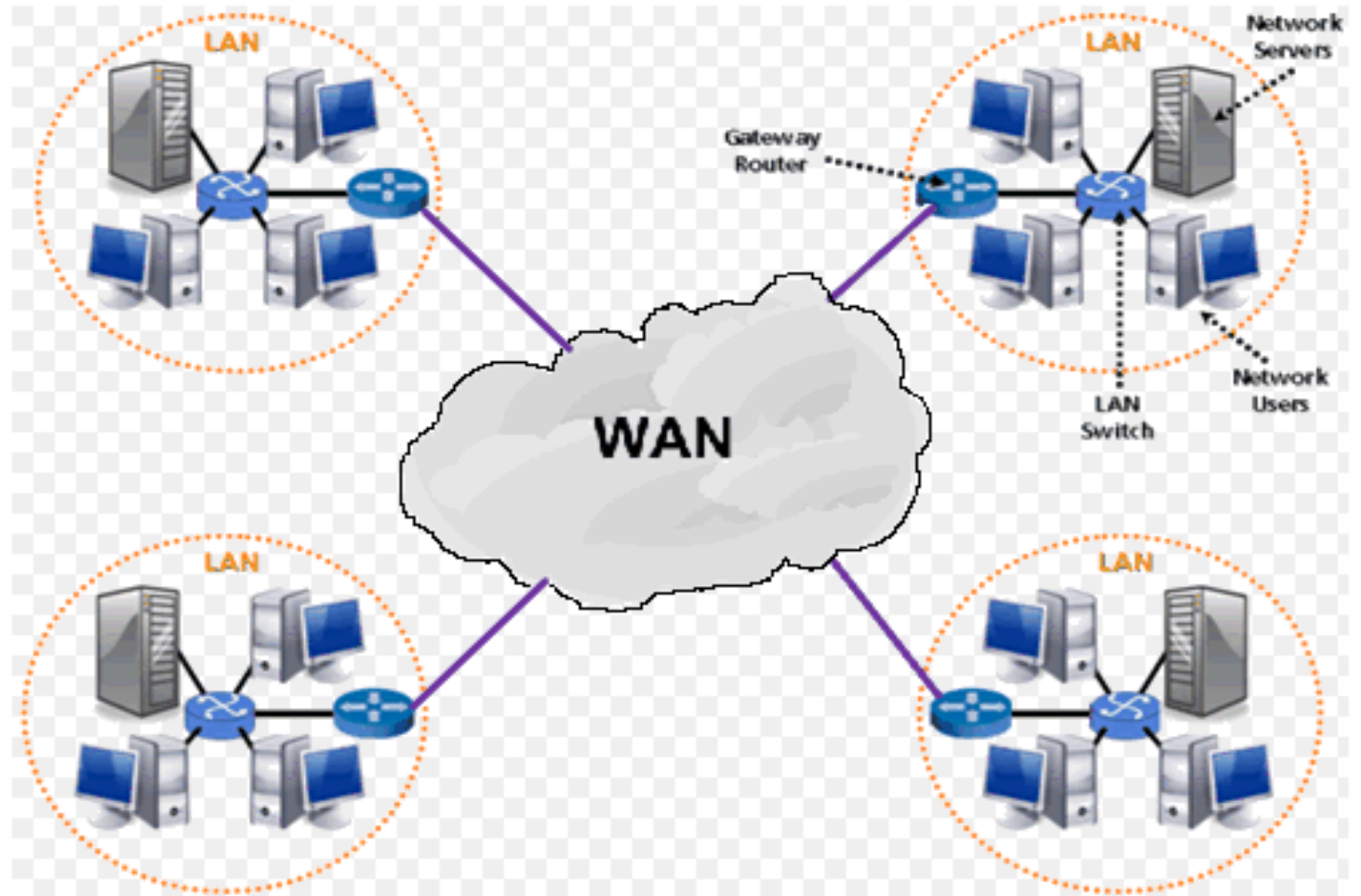


# Wide Area Network (WAN)

- A wide area network (WAN) is a computer network that covers a large geographical area comprising a region, a country, a continent or even the whole world.
- WAN includes the technologies to transmit data, image, audio and video information over long distances and among different LANs and MANs.
- **The distinguishing features of WAN are**
- WANs have a large capacity, connecting a large number of computers over a large area, and are inherently scalable.
- They facilitate the sharing of regional resources.
- They provide uplinks for connecting LANs and MANs to the Internet.
- Communication links are provided by public carriers like telephone networks, network providers, cable systems, satellites etc.
- Typically, they have low data transfer rate and high propagation delay, i.e. they have low communication speed.
- They generally have a higher bit error rate.

# Wide Area Network (WAN) Cont..

- **Example of WAN**
- The Internet
- 4G Mobile Broadband Systems
- A network of bank cash dispensers



# Wide Area Network (WAN) Cont..

## Advantages of a wide area network (WAN)

- **Covers large geographical area:**
- Wan covers a large geographical area of 1000 km or more. If your office is in different cities or countries, then you can connect your office branches through wan. ISP (Internet service provider) can give you leased lines by which you can connect different branch offices together.
- **Centralized data:**
- Your company doesn't need to buy email, files, and backup servers; they can all reside on the head office. All office branches can share the data through the head office server. You can get back up, support, and other useful data from the head office, and all data are synchronized with all other office branches.
- **Get updated files and data:**
- Software companies work over the live server to exchange updated files. So all the coders and office staff get the updated version of files within seconds.
- **A lot of application to exchange messages:**
- With IOT (Internet of things) and new LAN technologies, messages are being transmitted fast. A lot of web applications are available like Facebook messenger, WhatsApp, Skype by which you can communicate with friends via text, voice, and video chat.

# Wide Area Network (WAN) Cont..

## Advantages of a wide area network (WAN)

- **Sharing of software and resources:**
- Like LAN we can share software applications and other resources like a hard drive, RAM with other users on the internet. In web hosting, we share computer resources among many websites.
- **Global business:**
- Now everyone with computer skills can do business on the internet and expand his business globally. There are many types of business like a shopping cart, sale, and purchase of stocks etc.
- **High bandwidth:**
- If you get leased lines for your company then it gives high bandwidth than normal broadband connection. You can get a high data transfer rate that can increase your company productivity.
- **Distribute workload and decrease travel charges:**
- Another benefit of wide area network is that you can distribute your work to other locations. For example, you have an office in the U.S then you can hire people from any other country and communicate with them easily over WAN. It also reduces your travel charges as you can monitor the activities of your team online.

# Wide Area Network (WAN) Cont..

## Disadvantages of a wide area network (WAN)

- **Security problems:**
- WAN has more security problem as compare to MAN and LAN. WAN has many technologies combined with each other which can create a security gap.
- **Needs firewall and antivirus software:**
- As data transferred on the internet can be accessed and changed by hackers so firewall needs to be enabled in the computer. Some people can also inject a virus into the computer so antivirus software needs to be installed. Other security software also needs to be installed on different points in WAN.
- **The setup cost is high:**
- Setting up WAN for the first time in office costs higher money. It may involve purchasing routers, switches, and extra security software.
- **Troubleshooting problems:**
- As WAN covers a lot of areas so fixing the problem in it is difficult. Most of WAN wires go into the sea and wires get broken sometimes. It involves a lot of resources to fix lines under the sea. In ISP (Internet service provider) head office many of internet lines, routers are mixed up in rooms and fixing issues on the internet requires a full-time staff.
- **Server down and disconnection issue:**
- In some areas, ISP faces problems due to electricity supply or bad lines structure. Customers often face connectivity issues or slow Internet speed issues. The solution to this is to purchase a dedicated line from ISP.

# Wide Area Network (WAN) Cont..

## Examples of wide area network (WAN)

- Some examples of WAN are below:
- Internet
- U.S defense department
- Most big banks
- Airline companies
- Stock brokerages
- Railway reservations counter
- Large telecommunications companies like Airtel store IT department
- Satellite systems
- Cable companies
- Network providers

<b>BASIS OF COMPARISON</b>	<b>LAN</b>	<b>MAN</b>	<b>WAN</b>
<b>Expands to</b>	<b>Local Area Network</b>	<b>Metropolitan Area Network</b>	<b>Wide Area Network</b>
<b>Meaning</b>	<b>A network that connects a group of computers in a small geographical area.</b>	<b>It covers relatively large region such as cities, towns.</b>	<b>It spans large locality and connects countries together. Example Internet.</b>
<b>Ownership of Network</b>	<b>Private</b>	<b>Private or Public</b>	<b>Private or Public</b>
<b>Design and maintenance</b>	<b>Easy</b>	<b>Difficult</b>	<b>Difficult</b>
<b>Propagation Delay</b>	<b>Short</b>	<b>Moderate</b>	<b>Long</b>
<b>Speed</b>	<b>High</b>	<b>Moderate</b>	<b>Low</b>
<b>Fault Tolerance</b>	<b>More Tolerant</b>	<b>Less Tolerant</b>	<b>Less Tolerant</b>
<b>Congestion</b>	<b>Less</b>	<b>More</b>	<b>More</b>
<b>Used for</b>	<b>College, School, Hospital.</b>	<b>Small towns, City.</b>	<b>Country/Continent.</b>
<b>Allows</b>	<b>Single pair of devices to communicate.</b>	<b>Multiple computers can simultaneously interact.</b>	<b>A huge group of computers communicate at the same time.</b>

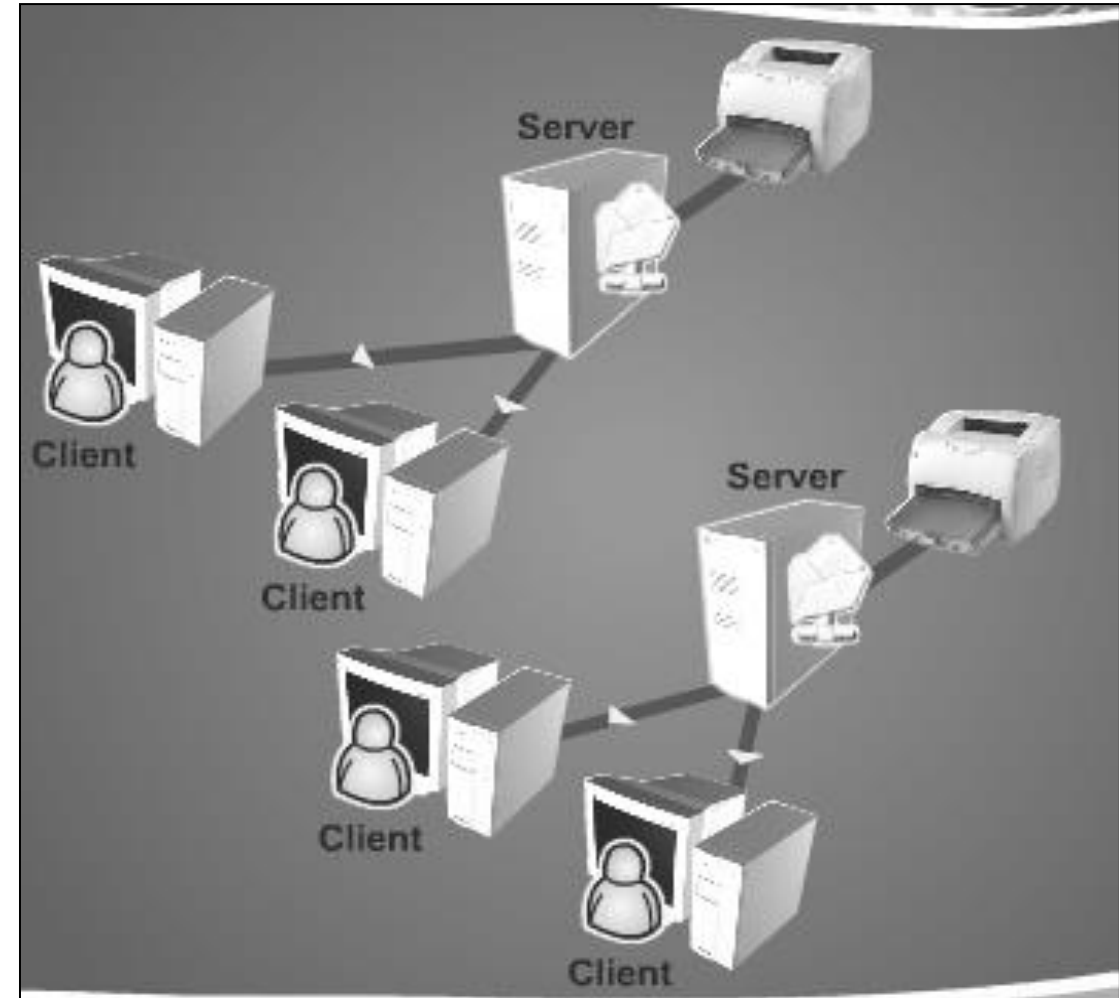
# Network architecture

- Overall design of a computer network that describes how a computer network is configured and what strategies are being used.
- Mainly focuses on the functions of the networks.
- Also known as network model or network design.

# Network architecture Cont..

## CLIENT/SERVER NETWORK

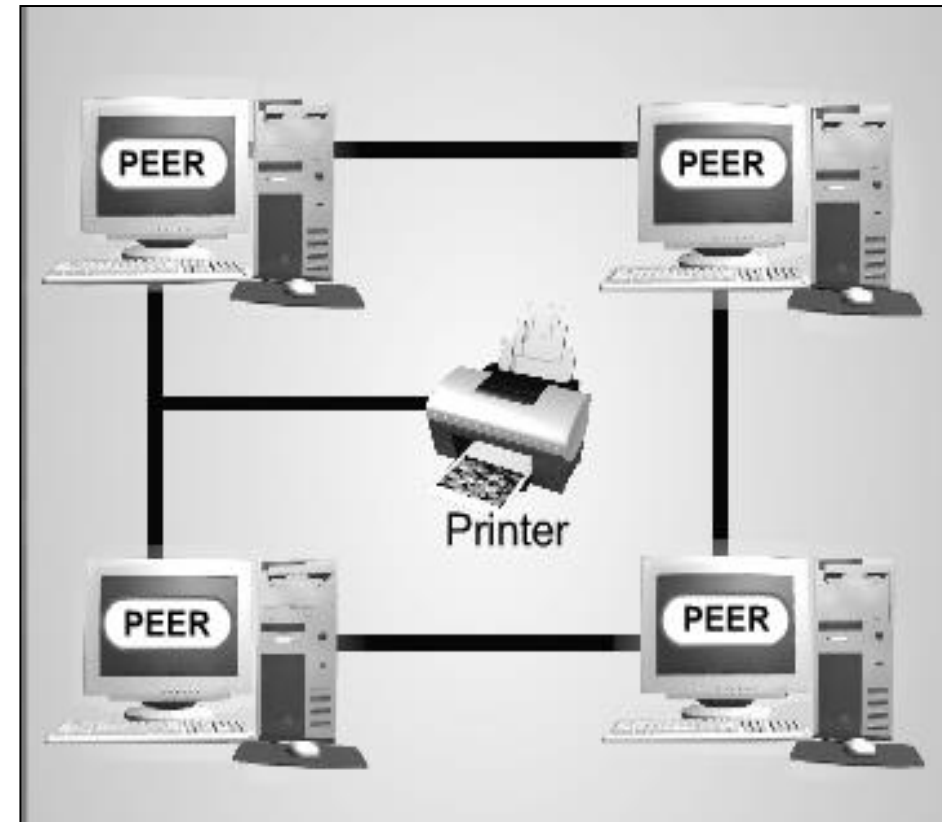
- A client/server network is a network in which the shared files and applications are stored in the server but network users (clients) can still store files on their individual PCs.
- A server is a computer that shares information and resources with other computers on a network.
- A client is a computer which requests services or files from a server computer.



# Network architecture Cont..

## Peer-to-peer or P2P

- It is a network with all the nodes acting as both servers and clients.
- A PC can access files located on another PC and can also provide files to other PCs.
- All computers in the peer-to-peer network has equal responsibilities and capabilities to use the resources available on the network.
- With peer-to-peer network, no server is needed; each computer in the network is called a peer.



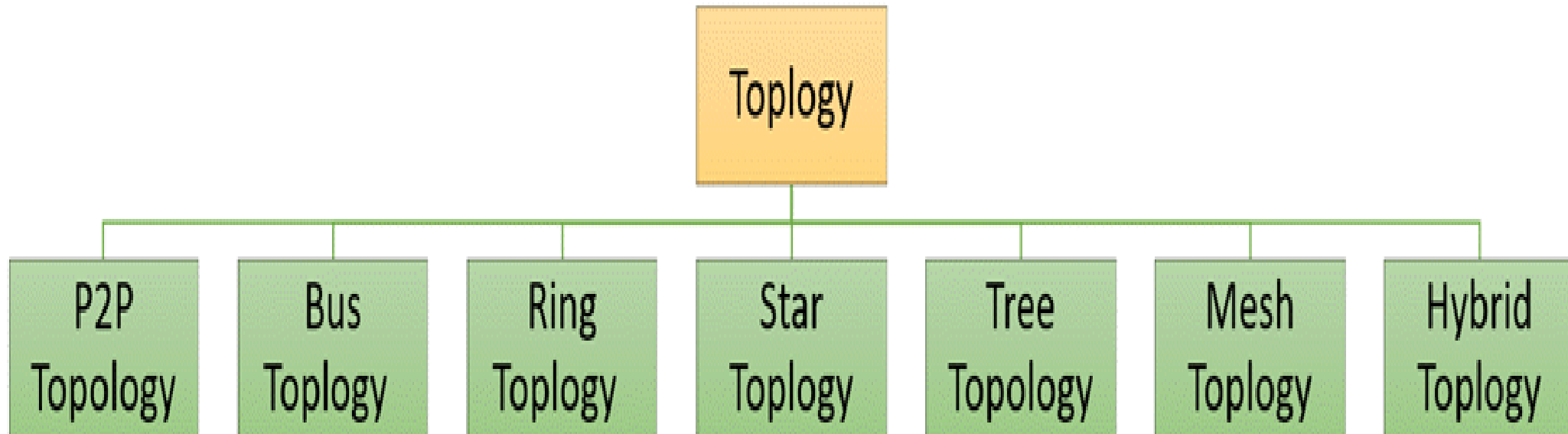
<b>Client/Server</b>	<b>Peer-To-Peer</b>
Server has the control ability while clients don't	All computers have equal ability
Higher cabling cost	Cheaper cabling cost
It is used in small and large networks	Normally used in small networks with less than 10 computers
Easy to manage	Hard to manage
Install software only in the server while the clients share the software	Install software to every computer
One powerful computer acting as server	No server is needed

# Network Topology

- **Network topology** is the arrangement of the elements (links, nodes, etc.) of a communication network.
- Network topology can be used to define or describe the arrangement of various types of telecommunication networks, including command and control radio networks
- Conversely, mapping the data flow between the components determines the logical **topology** of the **network**.

# Network Topology Cont..

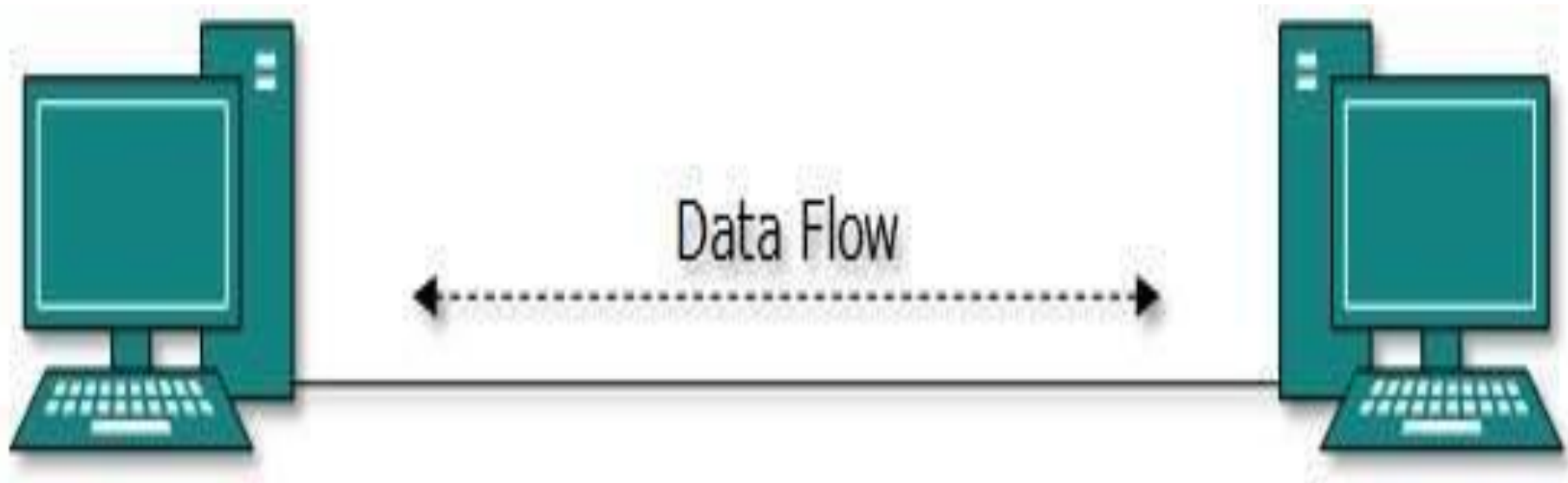
- Network topologies describe the methods in which all the elements of a network are mapped.
- A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network.



# Network Topology Cont..

## 1. Point to Point

- Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa.



# Point to Point Topology Cont..

## **Advantages:**

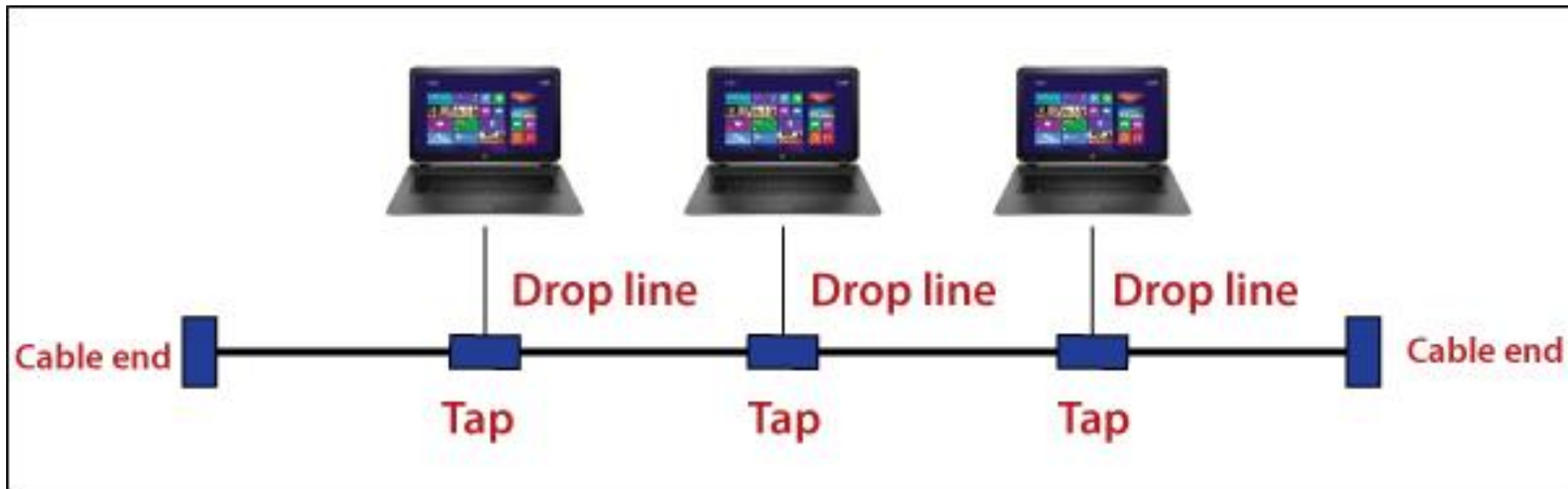
- This is faster and highly reliable than other types of connections since there is a direct connection.
- No need for a network operating system
- Does not need an expensive server as individual workstations are used to access the files
- No need for any dedicated network technicians because each user sets their permissions

## **Disadvantages:**

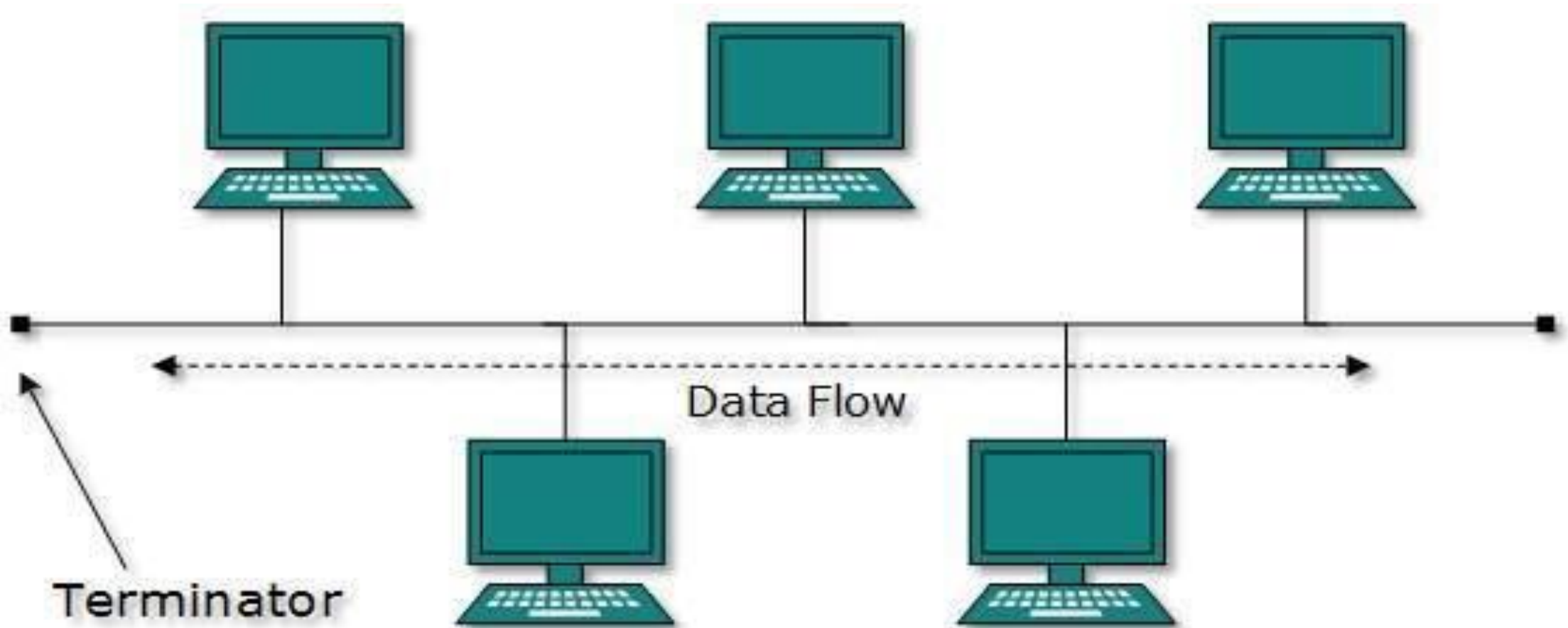
- The biggest drawback is that it only be used for small areas where computers are in close proximity.
- You can't back up files and folders centrally
- There is no security besides the permissions. Users often do not require to log onto their workstations.

# BUS Topology

- A bus topology is multipoint. One long cable act as a backbone to link all the devices in a network. Nodes are connected to the bus cable by drop lines and taps.
- As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps.



## Bus Topology Cont..



# Bus Topology Cont..

- **Advantages of Bus Topology :**

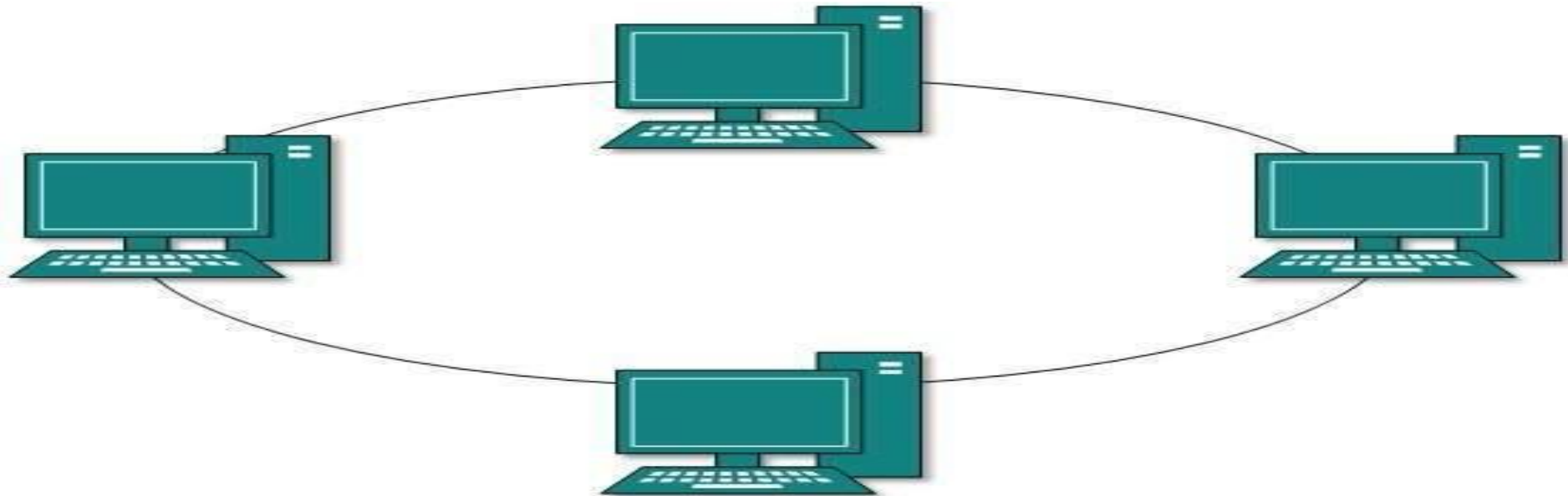
- It is the easiest network topology for connecting peripherals or computers in a linear fashion.
- It works very efficient well when there is a small network.
- Length of cable required is less than a star topology.
- It is easy to connect or remove devices in this network without affecting any other device.
- Very cost-effective as compared to other network topology i.e. mesh and star
- It is easy to understand topology.
- Easy to expand by joining the two cables together.

- **Disadvantages of Bus Topology :**

- Bus topology is not great for large networks.
- Identification of problem becomes difficult if whole network goes down.
- Troubleshooting of individual device issues is very hard.
- Need of terminators are required at both ends of main cable.
- Additional devices slow network down.
- If a main cable is damaged, whole network fails or splits into two.
- Packet loss is high.
- This network topology is very slow as compared to other topologies.

# Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

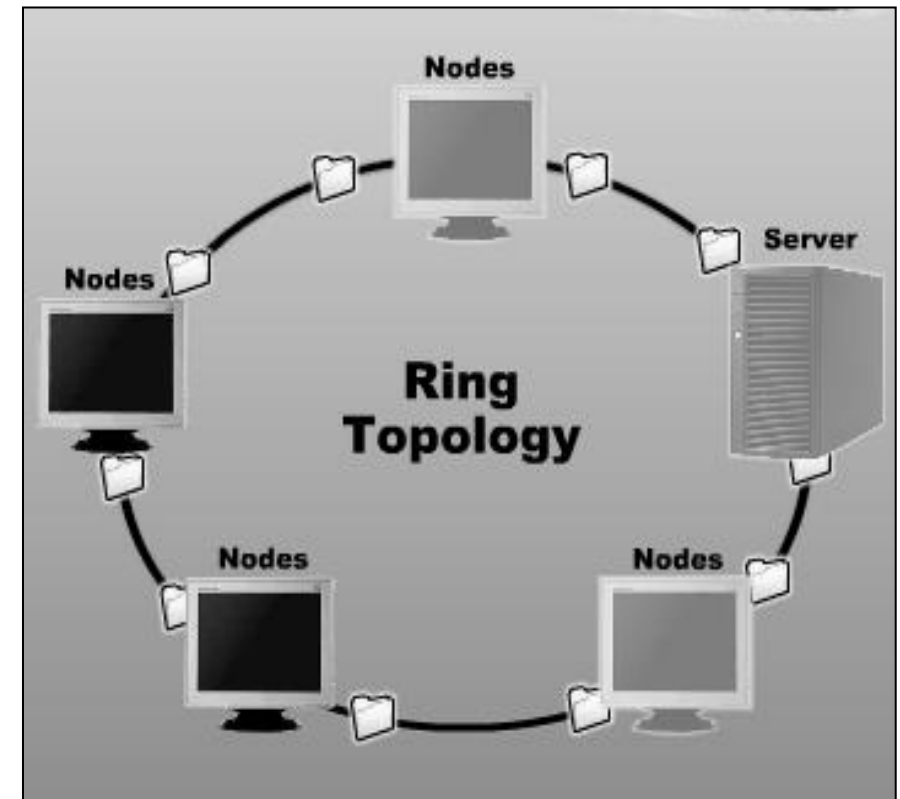


# Ring Topology Cont..

**A ring topology consists of all computers and other devices that are connected in a loop. Ring topology is also known as a ring network.**

## DESCRIPTION OF RING TOPOLOGY

- Can be found in LAN.
- Each node directly connect to two neighboring nodes.
- A server may exist in a ring network, but it will not connect to all the nodes in the network.
- The server, like other nodes, will only communicate to its two neighboring nodes



# Ring Topology Cont..

- **Advantages of Ring Topology:**

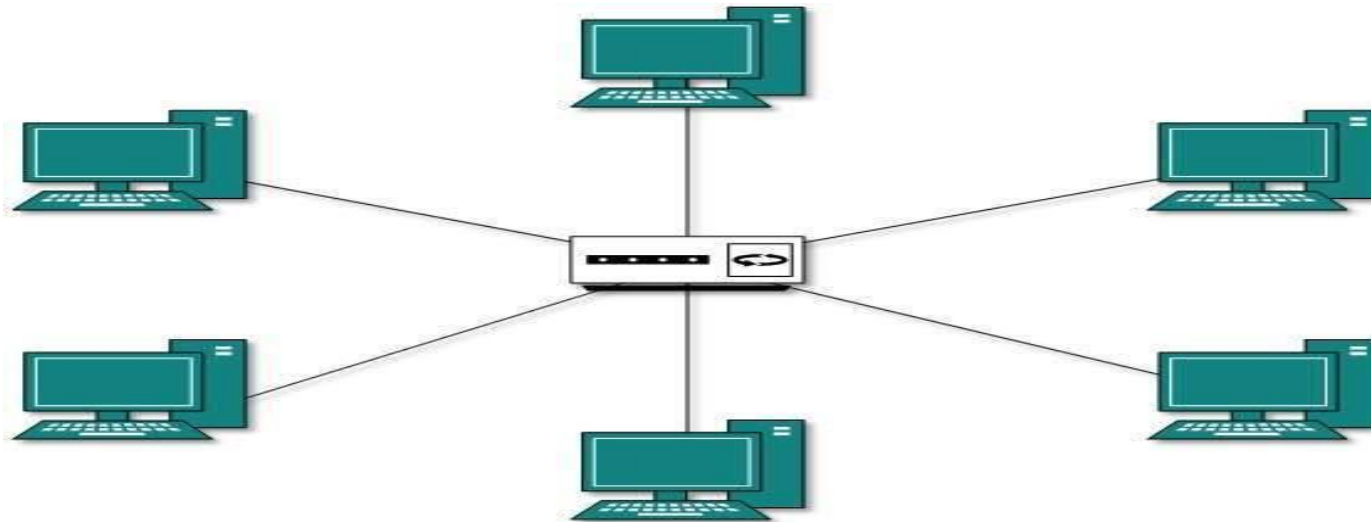
- Flow of data is in circular direction which minimizes the chance of packet collision.
- The uni-directional ring topology provides very high speed.
- It has better performance than bus topology, even when the nodes are increased.
- Ring network can handle high volume of nodes in a network (Robust).
- It can handle heavy traffic as compared to bus topology due to Token passing principal.
- Ring topology provides good communication over a long distance.
- The maintenance of ring network is much easier compared to the bus network.
- There is no need of network server to control the flow of data.
- Troubleshooting in ring network is much easier because cable faults can be easily located.
- Ring network is less costly compared to the other topologies I.e. (mesh, hybrid, and tree topology).

- **Disadvantage of Ring Topology:**

- A single break in the cable can cause disturbance in the entire network
- In Uni-directional Ring, a data packet (token) must pass through all the nodes.
- Addition and removal of any node in a network is difficult and can cause issue in network activity.
- Ring network is much slower than Ethernet network under normal load conditions.

# Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices.
- The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

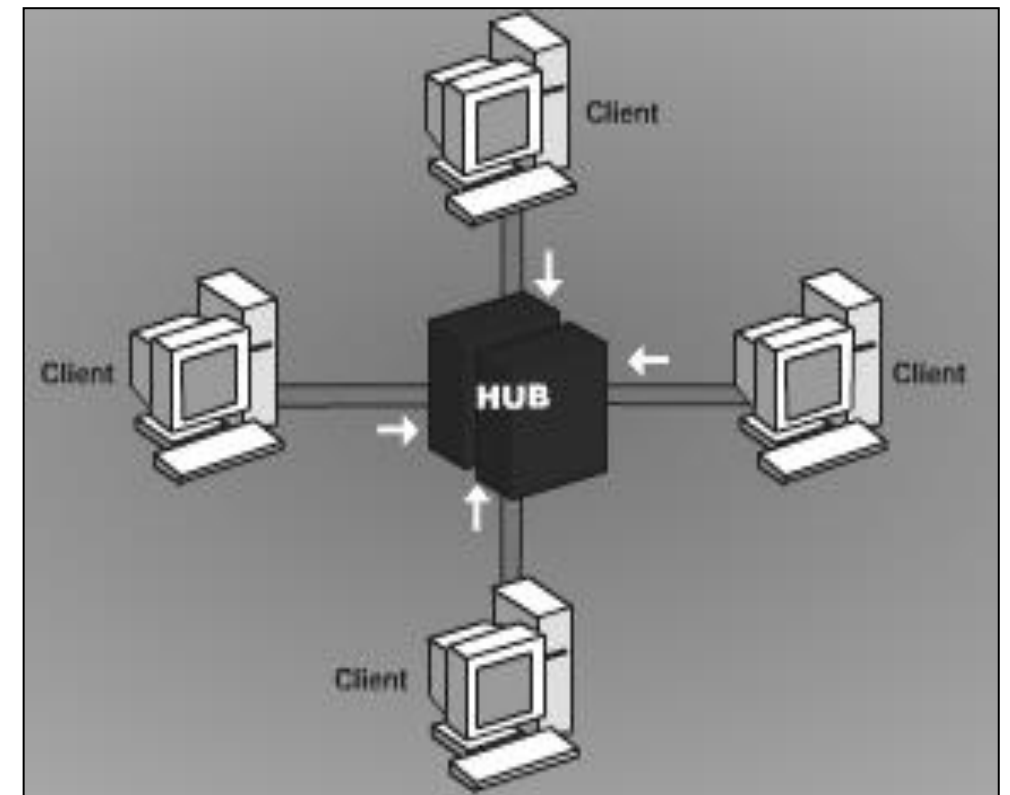


# Star Topology Cont..

A star topology consists of a central host which acts as the center, and all nodes connect to the host. A star topology is also known as star network.

## DESCRIPTION OF STAR TOPOLOGY

- A star network is found in a Local Area Network setting.
- A star network must have a host which acts as the centre.
- The host can be a server, hub or router.
- In a star network, every node will not connect to the neighboring nodes.
- Every node must connect to the host in order to communicate.
- The host will control the flow of communication in the network.



# Star Topology Cont..

- **Advantages of Star Topology**

- It is very reliable – if one cable or device fails then all the others will still work
- It is high-performing as no data collisions can occur
- Less expensive because each device only need one I/O port and wishes to be connected with hub with one link.
- Easier to put in
- Robust in nature
- Easy fault detection because the link are often easily identified.
- No disruptions to the network when connecting or removing devices.
- Each device requires just one port i.e. to attach to the hub.
- If N devices are connected to every other in star, then the amount of cables required to attach them is N. So, it's easy to line up.

- **Disadvantages of Star Topology**

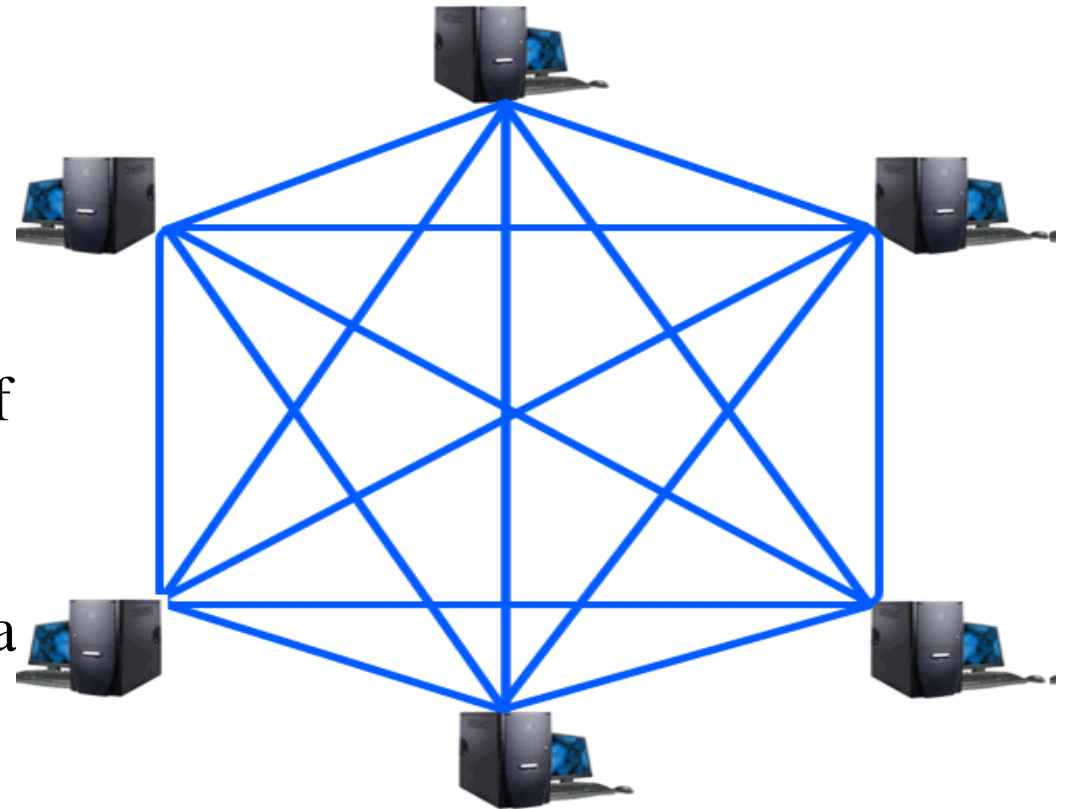
- Requires more cable than a linear bus .
- If the connecting network device (network switch) fails, nodes attached are disabled and can't participate in network communication.
- More expensive than linear bus topology due to the value of the connecting devices (network switches)
- If hub goes down everything goes down, none of the devices can work without hub.
- Hub requires more resources and regular maintenance because it's the central system of star .
- Extra hardware is required (hubs or switches) which adds to cost
- Performance is predicated on the one concentrator i.e. hub.

# Mesh Topology

Mesh Network is a network where all the nodes are connected to each other and is a complete network. In a Mesh Network every node is connected to other nodes on the network through hops.

## DESCRIPTION OF MESS TOPOLOGY

- Data is automatically configured to reach the destination by taking the shortest route.
- The reliability factor is high in any kind of Mesh Network.
- The Mesh Network is based on a very sensible concept and has lesser chances of a network breakdown.



# Mesh Topology Cont..

## **Advantages of Mesh Topology :**

- Failure during a single device won't break the network.
- There is no traffic problem as there is a dedicated point to point links for every computer.
- Fault identification is straightforward.
- This topology provides multiple paths to succeed in the destination and tons of redundancy.
- It provides high privacy and security.
- Data transmission is more consistent because failure doesn't disrupt its processes.
- Adding new devices won't disrupt data transmissions.
- This topology has robust features to beat any situation.
- A mesh doesn't have a centralized authority

# Mesh Topology Cont..

## Disadvantages of Mesh Topology :

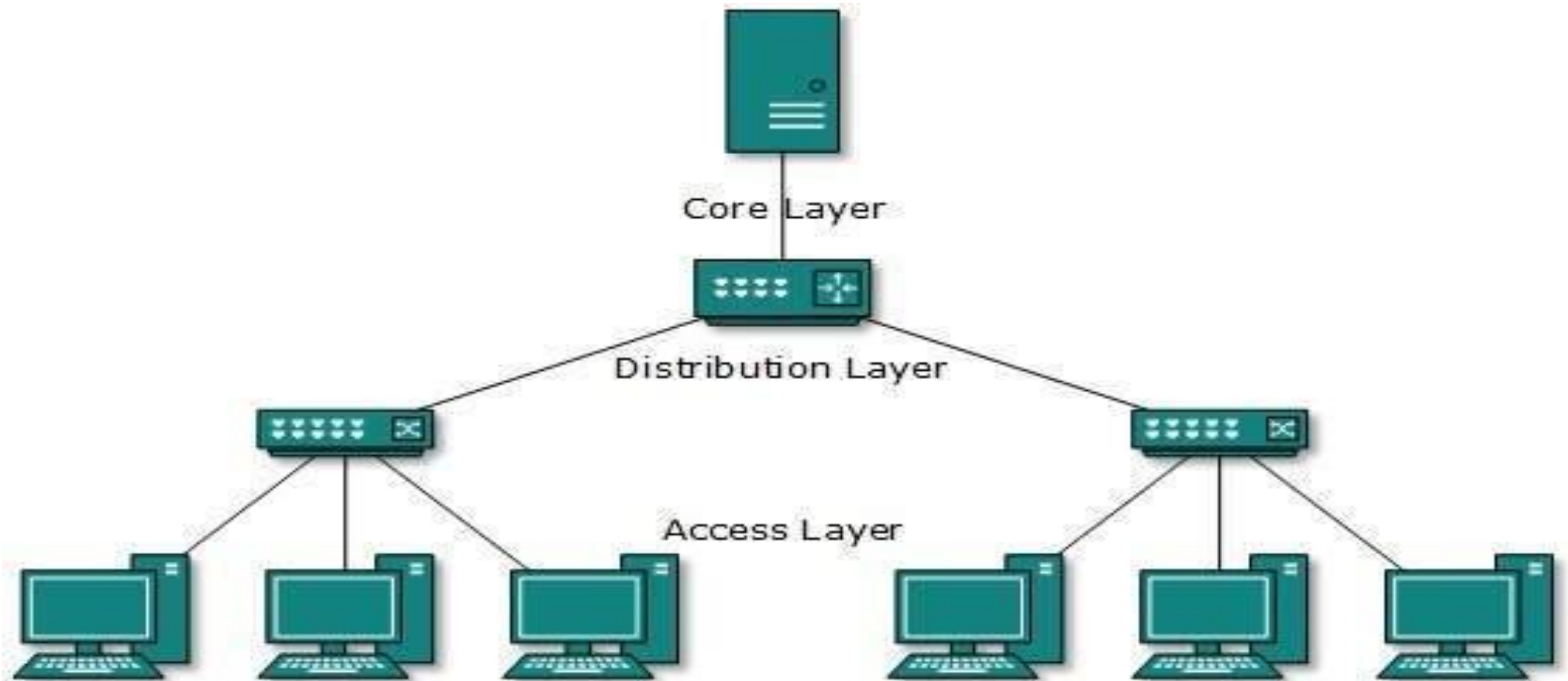
- It's costly as compared to the opposite network topologies i.e. star, bus, point to point topology.
- Installation is extremely difficult in the mesh.
- Power requirement is higher as all the nodes will need to remain active all the time and share the load.
- Complex process.
- The cost to implement mesh is above other selections.
- There is a high risk of redundant connections.
- Each node requires a further utility cost to think about.
- Maintenance needs are challenging with a mesh.

# Network Topology cont..

## 6. Tree Topology

- A **tree topology** is a special type of structure where many connected elements are arranged like the branches of a **tree**. ... Because any two nodes can have only one mutual connection, **tree** topologies create a natural parent and child hierarchy.
- In **Tree Topology**, all the computer are connected like the branches of a tree. In Computer Networking, tree topology is known as a combination of a Bus and Star network topology.
- Also known as Hierarchical Topology, this is the most common form of network topology in use presently.
- This topology imitates as extended Star topology and inherits properties of bus topology.
- The **lowermost is access-layer** where computers are attached.
- The **middle layer** is known as distribution layer, which works as mediator between upper layer and lower layer.
- The **highest layer** is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.
- A **tree topology** is a special type of structure where many connected elements are arranged like the branches of a **tree**. For **example**, **tree** topologies are frequently used to organize the computers in a corporate network, or the information in a database.

# Tree Topology Cont...



# Tree Topology Cont..

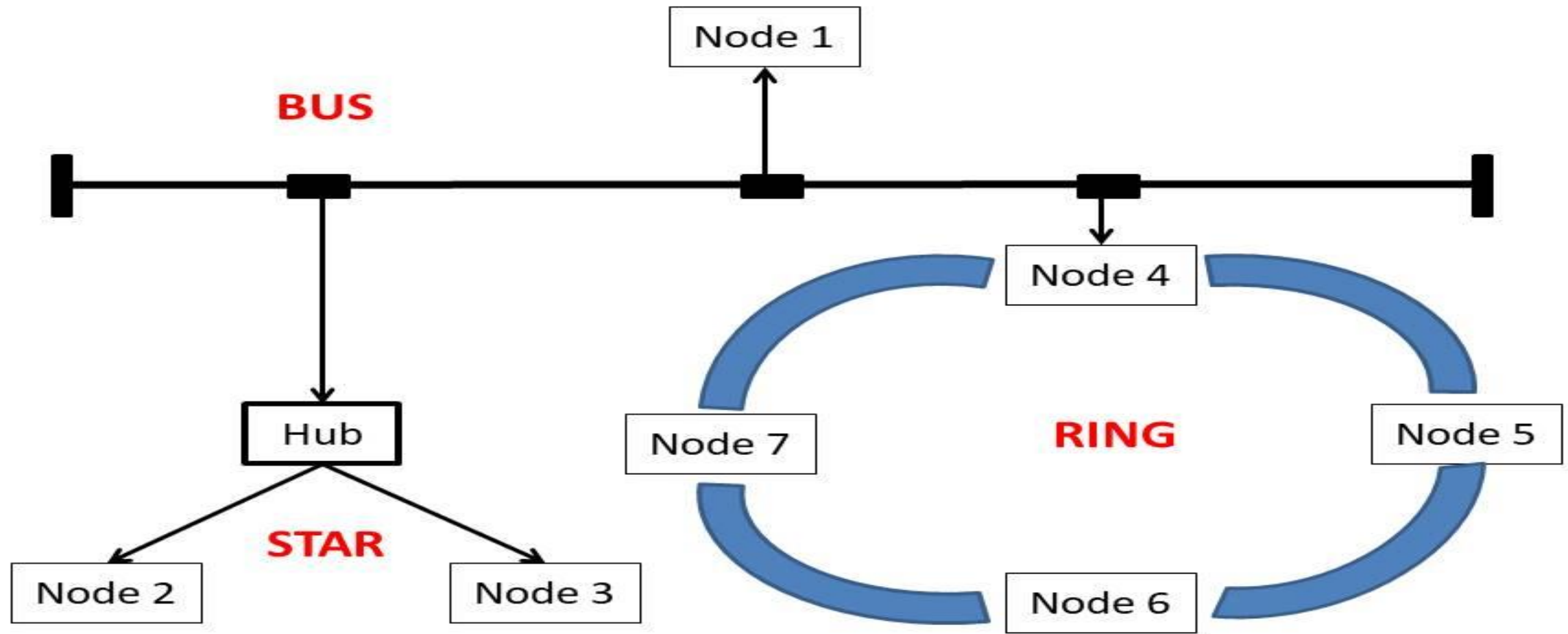
- **Advantages of Tree Topology :**
- This topology is the combination of bus and star topology.
- This topology provides a hierarchical as well as central data arrangement of the nodes.
- As the leaf nodes can add one or more nodes in the hierarchical chain, this topology provides high scalability.
- The other nodes in a network are not affected, if one of their nodes get damaged or not working.
- Tree topology provides easy maintenance and easy fault identification can be done.

# Tree Topology Cont..

- **Disadvantages of Tree Topology :**
- This network is very difficult to configure as compared to the other network topologies.
- Length of a segment is limited & the limit of the segment depends on the type of cabling used.
- Due to the presence of large number of nodes, the network performance of tree topology becomes a bit slowly.
- If the computer in first level is erroneous, next level computer will also go under problems.
- Requires large number of cables compared to star and ring topology.
- As the data needs to travel from the central cable this creates dense network traffic.
- The Backbone appears as the failure point of the entire segment of the network.
- Treatment of the topology is pretty complex.
- The establishment cost increases as well.
- If the bulk of nodes are added in this network, then the maintenance will become complicated.

# Network Topology Cont..

- **7. A hybrid topology** is a kind of network topology that is a combination of two or more network topologies, such as **star topology**, **bus topology**, and **ring topology**.
- Its usage and choice are dependent on its deployments and requirements like the performance of the desired network, and the number of computers, their location.
- However, a variety of technologies are needed for its physical implementation, and it offers a complex structure. Also, it includes an advantage as increasing flexibility; it can increase fault tolerance, and allows new basic topologies to be added or removed easily.
- The hybrid topology is more useful when you need to fulfill diversity in Computer Network.



## Hybrid Topology

# Hybrid Topology Cont..

## Advantages of Hybrid Topology:

- **Reliable:** It is more reliable as it has better fault tolerance. If a node gets damaged between the network, it is possible in this network to single out the damaged node from rest of the network. Also, in this case, without impacting the processing of the network, the needed steps can be taken.
- **Effective:** This is the biggest advantage of hybrid topology. The weakness of the several topologies connected in this topology is ignored. And, there is a consideration only about the strengths of these different topologies. For case, the high tolerance capability is offered by star topology, and good data reliability is provided by ring topology. Therefore, in hybrid star-ring topology, these two-function work quite well.
- **Scalable:** Hybrid networks are the kind of network that is designed in a way, which led to making capable them to easy integration of additional concentration points or other new hardware components. Without disturbing existing architecture, it is very easy to extend the network size with the latest addition of new elements.
- **Flexible:** One of the great benefits of hybrid topology is flexibility. This topology can be implemented for various different network environments as it is created. The hybrid network can be created by maximizing the available resources and in line with the demands of the corporation.

# Hybrid Topology Cont..

## Disadvantages of Hybrid Topology:

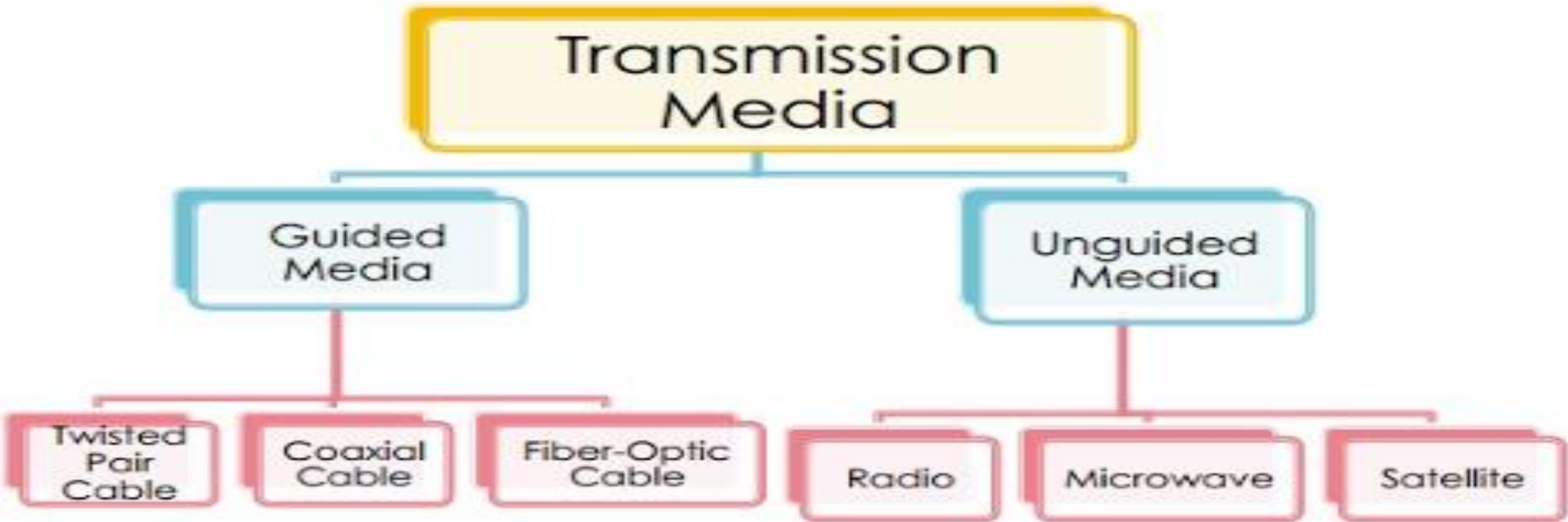
- **Complexity:** To manage the topology become challenging, as the different topologies are linked in the hybrid topology.
- It is a difficult job for designers and not easy to create this type of architecture. There is a need to be very efficient for the installation and configuration process.
- **Expensive:** Purchasing and maintaining the hybrid topology is much expensive while comparing with other topologies. The hubs are also required in this network topology that are used to connect two different networks, and they are also expensive.
- Furthermore, the hybrid topology may need advanced network devices, a lot of cables, and more as its architectures are usually larger in scale.
- One of the other disadvantages of hybrid topology; although it is able to detect faults easily, it needs a multi-station access unit to bypass faulty devices.

# APPLICATIONS OF COMPUTER NETWORK

- **File sharing.**
- **Printer sharing.**
- **Communication and collaboration.**
- **Remote access.**
- **Data protection.**
- **Centralized Support and Administration.**

# Transmission Media

- In data communication terminology, a **transmission medium** is a physical path between the transmitter and the receiver i.e it is the channel through which data is sent from one place to another.
- A transmission medium can be broadly defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable, or fiber-optic cable.
- Transmission media can be generally categorized as either **guided** or **unguided**.



# Guided Media

It is **defined** as the physical **medium** through which the signals are transmitted.

## 1. Twisted-Pair Cable

- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The signal sent by the sender on one of the wires causes interference (noise) and crosstalk creating unwanted signals.
- Twisting the pair of cable reduces interference and cross talk between signals. For example, Twisted-pair cables are used in telephone lines to provide voice and data channels

# Guided Media Cont..

## ● Twisted Pair Cont..

- A set of copper wires coupled and twisted with each other is twisted pair cables.
- They are very commonly used cables for both analog and digital signal transmission.

### **Advantages**

- Twisted pair cable is easily available and it is the cheapest in the wired medium as of now.
- It is easier to install and needs no expertise in installing the medium
- In case of breakup on a part of cable, it doesn't affect the whole network.
- It is light weight, flexible and easier to handle.
- Additional nodes can be added easily.

### **Disadvantages:**

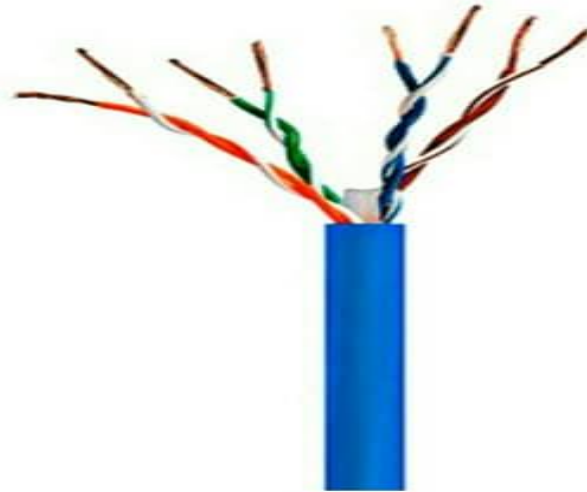
- Twisted pair is less secure. It can be tapped easily.
- It is subjected to electromagnetic interference and is affected by the interference readily.
- Since it can break easily, it needs a higher maintenance than other wired mediums

# Guided Media :

Coaxial Cable



Twisted Pair



Fiber Optic



# Guided Media Cont..

## 2. Coaxial Cable

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The cost of **guided media** is very low (inexpensive) and easily available. This is very Flexible and Lightweight. Very easy to set up and install.

### Coaxial cable

- They are the most common means of data communication over short distances.
- Cheap to install.
- Good Bandwidth.
- Great channel capacity.

# Guided Media Cont..

## Fiber Optic Cable:

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light.
- Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

# Guided Media Cont..

- The **advantages of optical fiber** include the following.
- Bandwidth is higher than copper cables
- Less power loss and allows data transmission for longer distances
- The optical cable is resistance for electromagnetic interference
- The size of the fiber cable is 4.5 times better than copper wires and
- These cables are lighter, thinner, and occupy less area compare with metal wires.
- Installation is very easy due to less weight.
- The optical fiber cable is very hard to tap because they don't produce electromagnetic energy. These cables are very secure while carrying or transmitting data.
- A fiber optic cable is very flexible, easily bends, and opposes most acidic elements that hit the copper wire.

# Guided Media Cont..

- The **disadvantages of optical fiber** include the following
- The optical fiber cables are very difficult to merge & there will be a loss of the beam within the cable while scattering.
- The Installation of these cables is cost-effective. They are not as robust as the wires. Special test equipment is often required to the optical fiber.
- Fiber optic cables are compact and highly vulnerable while fitting
- These cables are more delicate than copper wires.
- Special devices are needed to check the transmission of fiber cable.

# UNGUIDED MEDIA

- **Unguided** transmission **media** are methods that allow the transmission of data without the use of physical means to define the path it takes.

## 1. Radio Wave

- Transmission of data using radio frequencies is called **radio-wave transmission**.
- Radio stations transmit radio waves using **transmitters**, which are received by the receiver installed in our devices.
- Both transmitters and receivers use antennas to radiate or capture radio signals. These radio frequencies can also be used for **direct voice communication** within the **allocated range**.

# UNGUIDED MEDIA Cont..

## **Advantages of Radio Wave**

- These are some of the advantages of radio wave transmissions –
- Inexpensive mode of information exchange
- No land needs to be acquired for laying cables
- Installation and maintenance of devices is cheap

## **Disadvantages of Radio Wave**

- These are some of the disadvantages of radio wave transmissions –
- Insecure communication medium
- Prone to weather changes like rain, thunderstorms, etc.

# UNGUIDED MEDIA Cont..

## 2. Microwaves

- The **microwave** radiation is commonly referred to as **microwaves**. They fall between the infrared radiation and radio waves in the electromagnetic spectrum.
- **Microwave** frequencies are widely used for wireless devices such as cell phones, cordless phones, and wireless LANs (Wi-Fi) access for laptops, and Bluetooth earphones.

# UNGUIDED MEDIA Cont..

## 3. Satellites

- The communication across longer distances can be provided by combining radio frequency transmission with satellites.
- A ground station on one side of the ocean transmits signal to the satellite which in turn sends the signal to the ground station on the other side of the ocean.

### Applications of Satellite Systems

- Weather forecasting. Without the help of **satellites**, we cannot predict weather. ...
- Radio and TV broadcast **satellites**. ...
- Military **satellites**. ...
- **Satellites** for Navigation. ...
- Global telephone backbones. ...
- Connections for remote or developing areas. ...
- Global mobile communication.

# UNGUIDED MEDIA Cont..

## 4. Infrared transmission

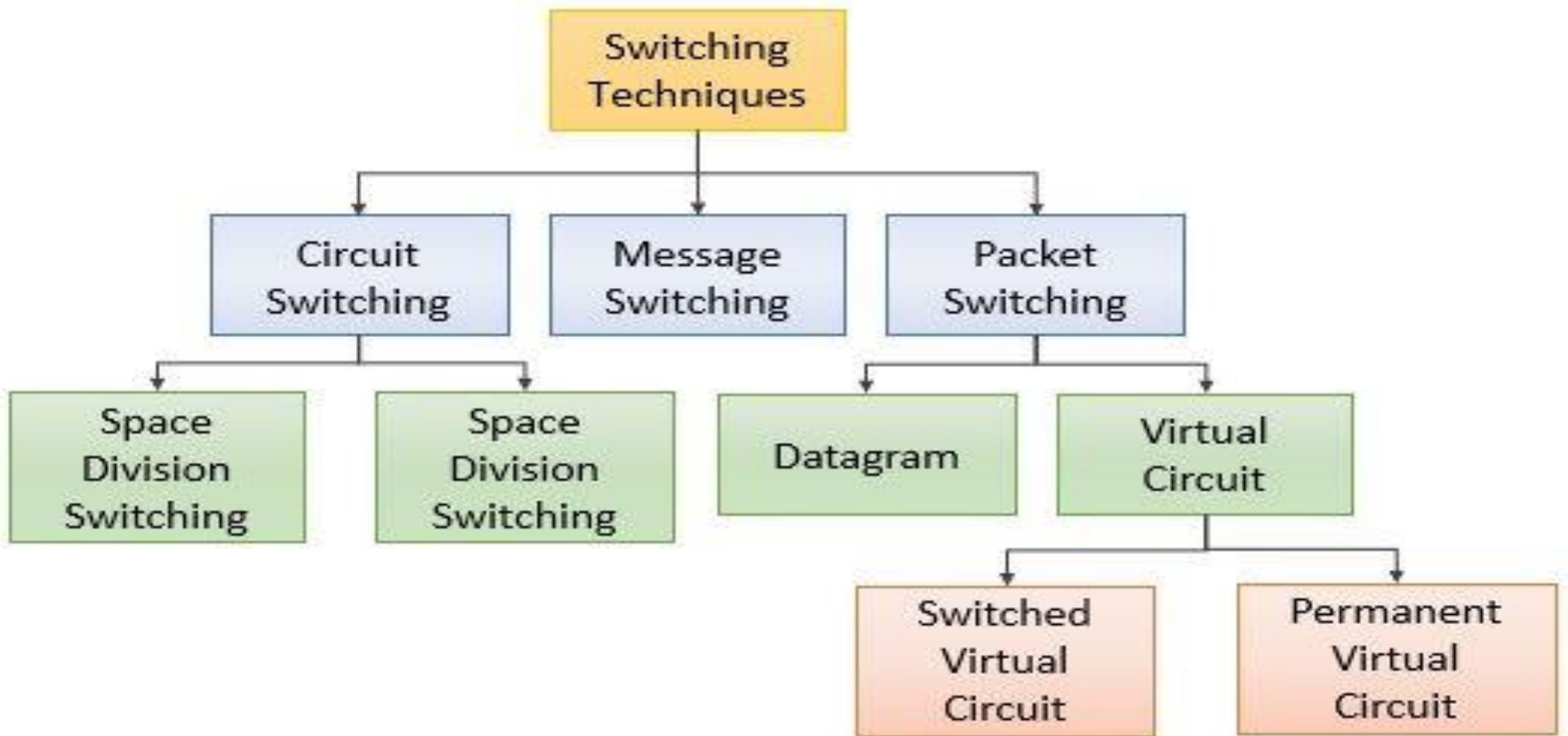
- **It** refers to energy in the region of the electromagnetic radiation **spectrum** at wavelengths longer than those of visible light, but shorter than those of radio waves.
- **Infrared** thermal-imaging cameras are **used** to detect heat loss in insulated systems, to observe changing blood flow in the skin, and to detect the overheating of electrical components. Military and civilian **applications** include target acquisition, surveillance, night vision, homing, and tracking.

# UNGUIDED MEDIA Cont..

- **Infrared transmission** refers to energy in the region of the electromagnetic radiation **spectrum** at wavelengths longer than those of visible light, but shorter than those of radio waves.
- **Infrared** thermal-imaging cameras are **used** to detect heat loss in insulated systems, to observe changing blood flow in the skin, and to detect the overheating of electrical components. Military and civilian **applications** include target acquisition, surveillance, night vision, homing, and tracking.

# Network Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as switching.
- There are three different types of switching techniques:
- **Circuit switching:** Circuit switching is a type of network configuration in which a physical path is obtained and dedicated to a single connection between two endpoints in the network for the duration of a dedicated connection.
- **Message switching:** Message Switching is a network switching strategy in which data or message is transmitted entirely from the source to the destination node, one hop at a time. Every intermediary switch in the network stores the entire message during message routing
- **Packet switching:** Packet switching is the transfer of small pieces of data across various networks. These data chunks or “packets” allow for faster, more efficient data transfer. Often, when a user sends a file across a network, it gets transferred in smaller data packets, not in one piece.

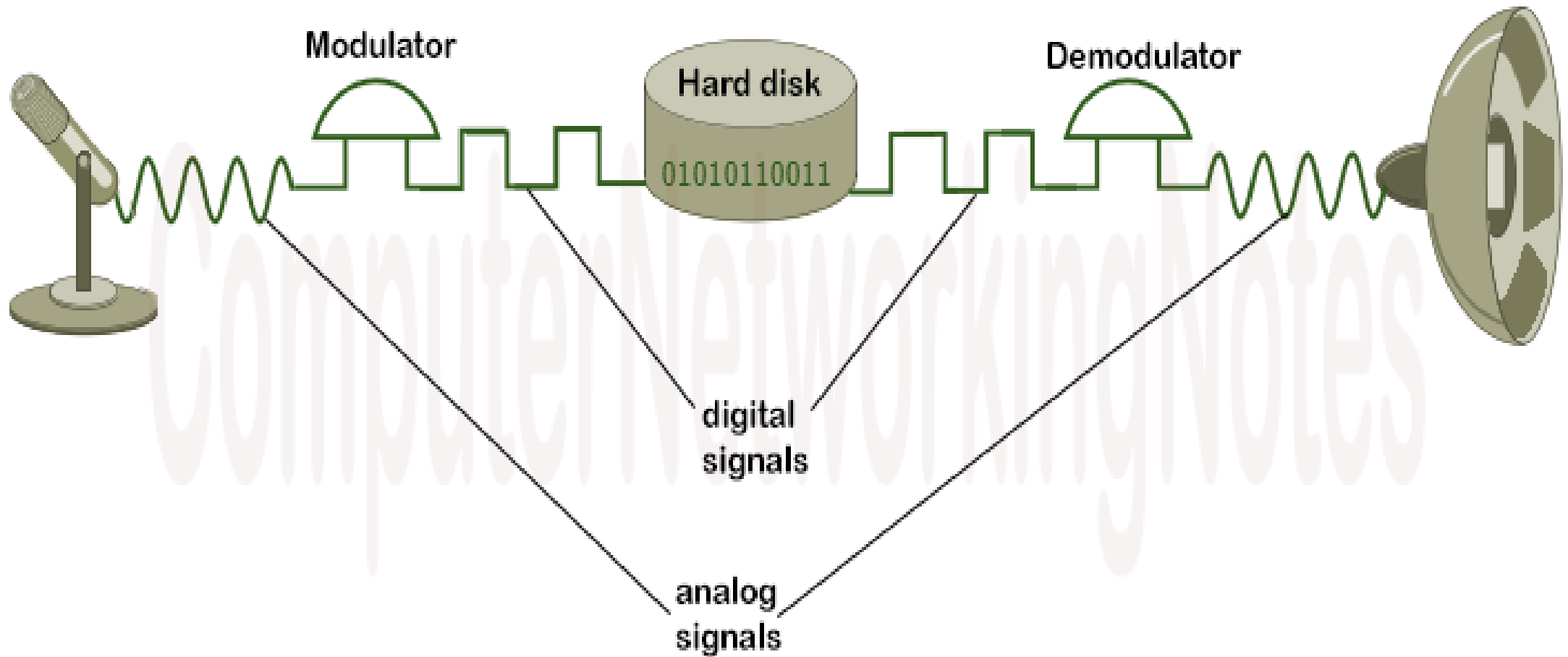


# Switching Techniques

# Data Modulation in Computer Networks

- Data modulation is a process that converts analog signals into digital signals and digital signals into analog signals. Computers store and process data in digital format. Data modulation allows computers to store and process analog signals.
- Let's take a simple example. When you record and play an audio clip, the following happens.
- You use a microphone to record the audio clip. The microphone sends your voice to the computer. Since the human voice consists of analog signals, the computer converts the received voice into digital signals before processing and storing them onto the hard disk.
- When the recorded clip is played, the computer reads digital signals from the hard disk and converts them into analog signals before sending them to the speaker.

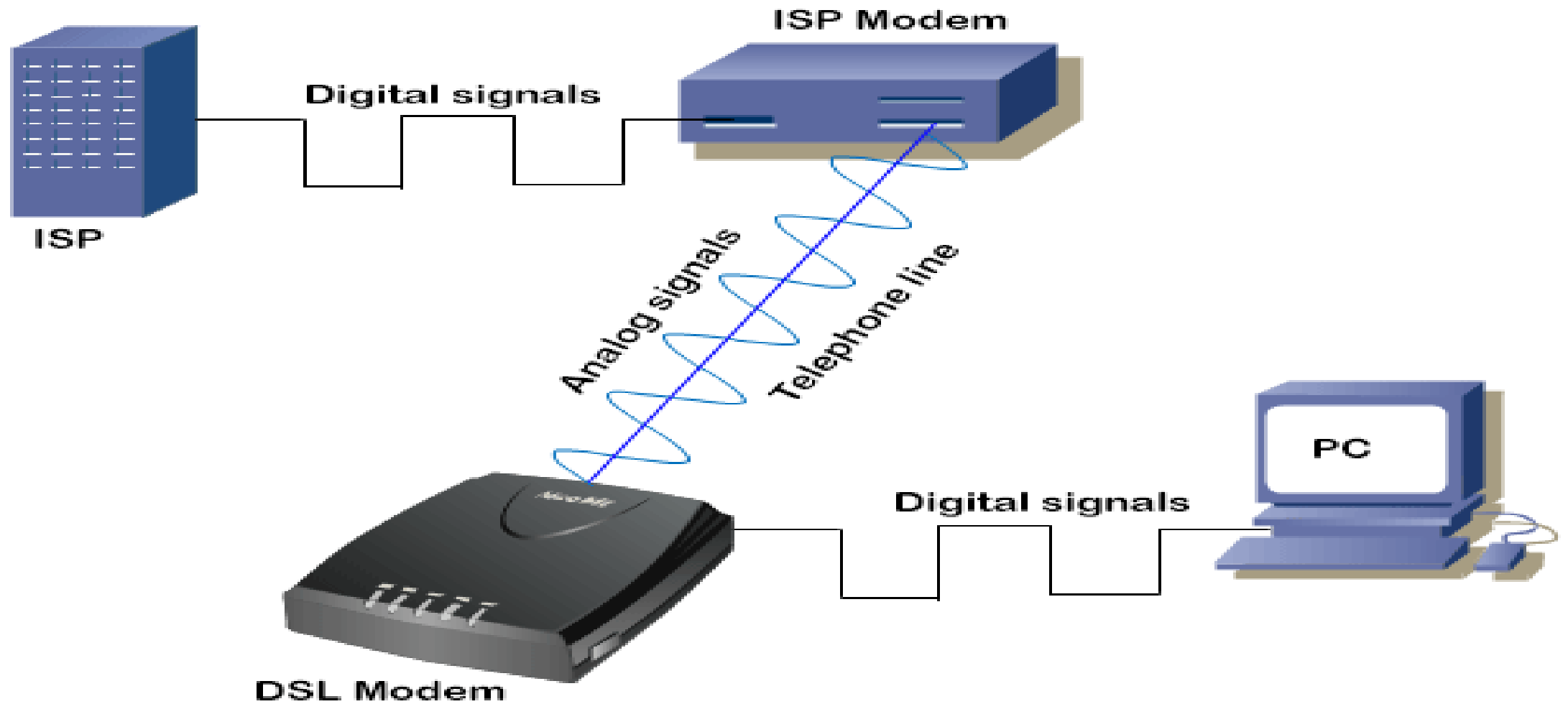
# Data Modulation in Computer Networks Cont..



# Data Modulation in Computer Networks Cont..

- Modulators and demodulators are devices or chips or components that convert analog signals into digital signals and digital signals into analog signals, respectively.
- Data modulation is not only used within the computer, but it is also used outside the computer. It allows computers to send digital signals on a media that can only carry analog signals. It converts signals in such a way that they become suitable for transport on a communication path that is not designed to carry such signals.
- For example, telephone lines are designed to carry analog signals. Through data modulation, the same telephone lines can also be used to provide the Internet facility. To provide the Internet facility through telephone lines, a device known as the **modem** is used. A modem can act as both a modulator and a demodulator.
- A modem connects a computer to the ISP network via a telephone line. It modulates digital signals into analog signals at the transmitting end, then demodulates analog signals into digital signals at the receiving end. The following image shows this process.

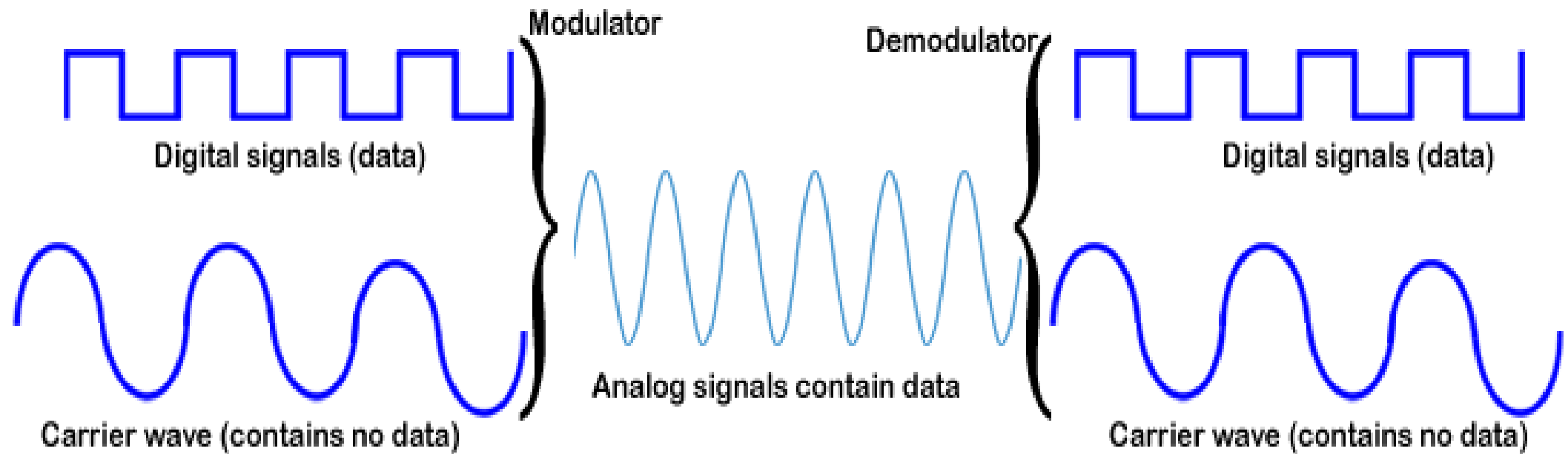
# Data Modulation in Computer Networks Cont..



# How does the data modulation work?

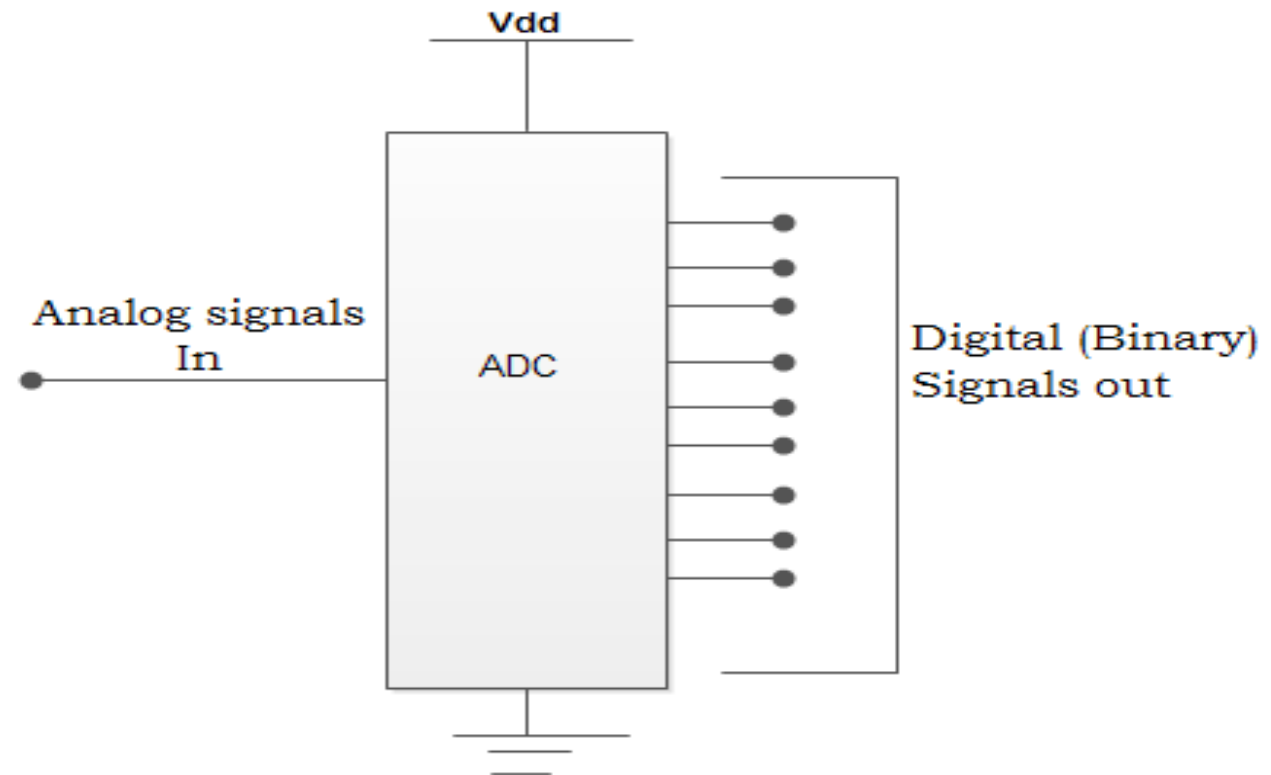
- To convert digital signals into analog signals, a simple analog wave, known as the **carrier wave**, is combined into digital signals. A carrier wave does not contain any information or data. In simple words, it's only a messenger that transfers information between two nodes.
- An analog wave has four properties; amplitude, frequency, wavelength, and phase. From these, amplitude and frequency are used to blend digital signals. To load digital signals on the analog wave, the modulator modifies either **amplitude** or **frequency** in a pre-defined way.
- After modification, the modulator loads the blended wave on the media. When the blended wave reaches its destination, the demodulator separates the data from the blended wave by using the same pre-defined way. After separation, the data is sent to its destination in the digital format and the carrier wave is discarded.
- The following image shows an example of this process.

# How does the data modulation work?



# Digitizing analog signals

- To convert analog signals into digital signals, an ADC (Analog to Digital Converter) is used. An ADC is an integrated electronic circuit. It takes input analog signals and

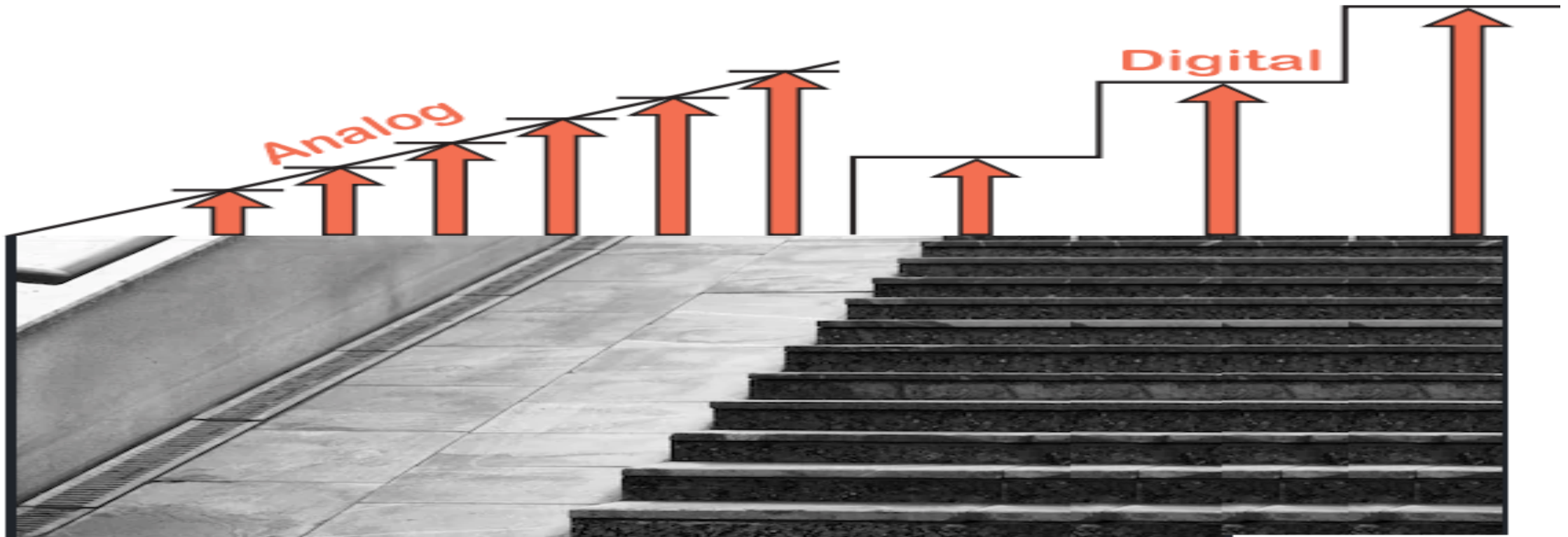


## Digitizing analog signals Cont..

- An ADC converts the output data into a series of digital values by approximating the signals with fixed precision. In each cycle of the analog signal, an ADC measures all the falling and rising of signals and converts them into digital values.
- To understand how an ADC converts analog signals into digital signals, think about a staircase and a ramp. A ramp is analog because it has an infinite number of heights. To construct a parallel staircase, a constructor uses sample heights of the ramp. The more samples the constructor takes, the more accurate the staircase will be.

# Digitizing analog signals Cont..

- The process of measuring the height and width of steps works similarly to the process of digitizing analog signals.

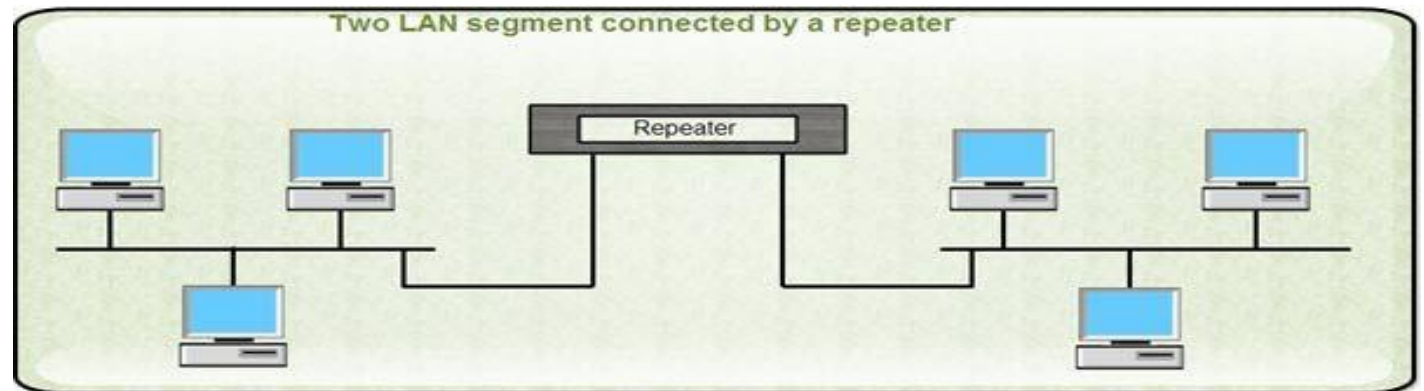


# Network device

The devices which are used for communication between different hardware's used in the computer network are known as network devices.

## 1. Repeaters

- A repeater is a device that operates only in the physical layer.
- A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern.
- A repeater does not actually connect two LANs; it connects two segments of the same LAN.
- A **repeater** is an electronic device in a communication channel that increases the power of a signal and retransmits it, allowing it to travel further.



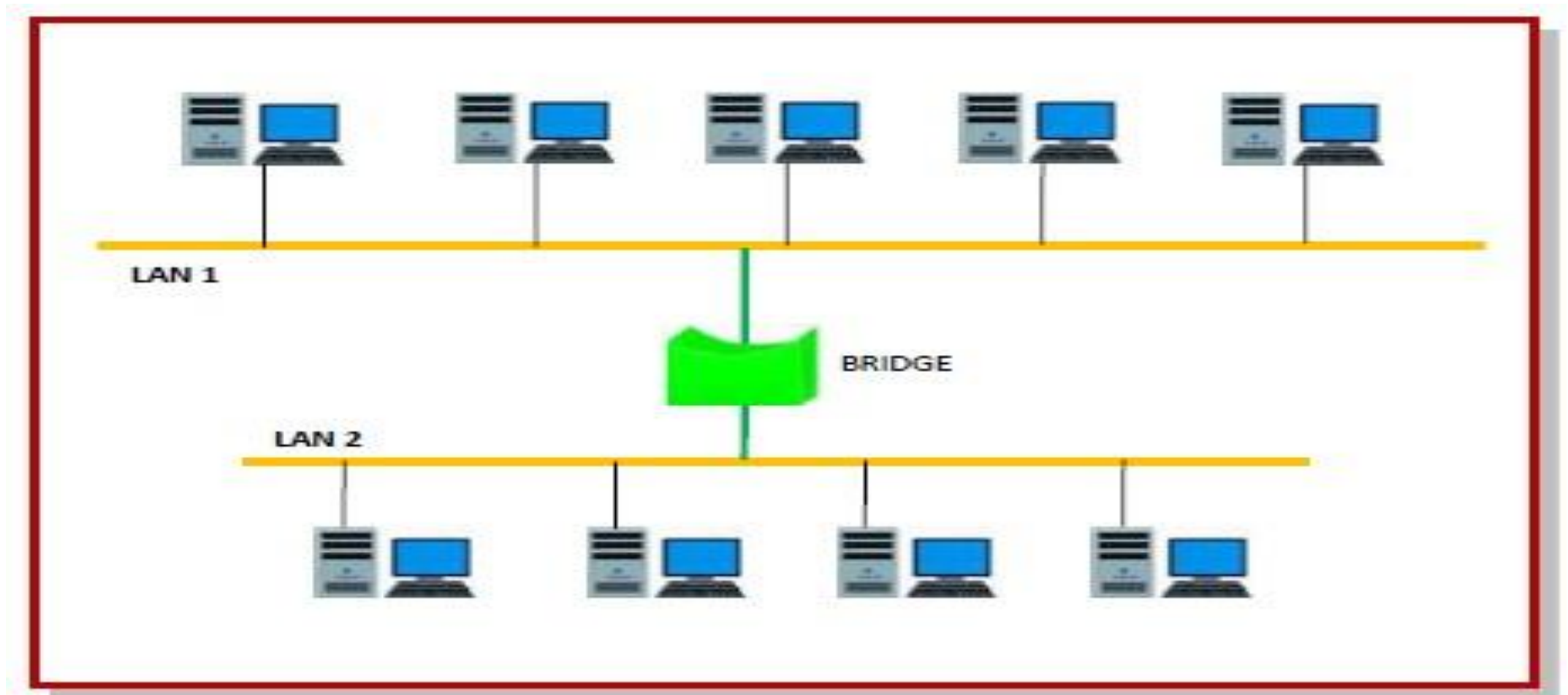
# Network device Cont..

## 2 . Bridge: Bridges or Link Layer Switches

- A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging.
- A bridge connects the different components so that they appear as parts of a single network.
- **Uses of Bridge**
  - Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.
  - By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
  - Since they operate at data link layer, they transmit data as data frames.
  - On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.

## Network device Cont..

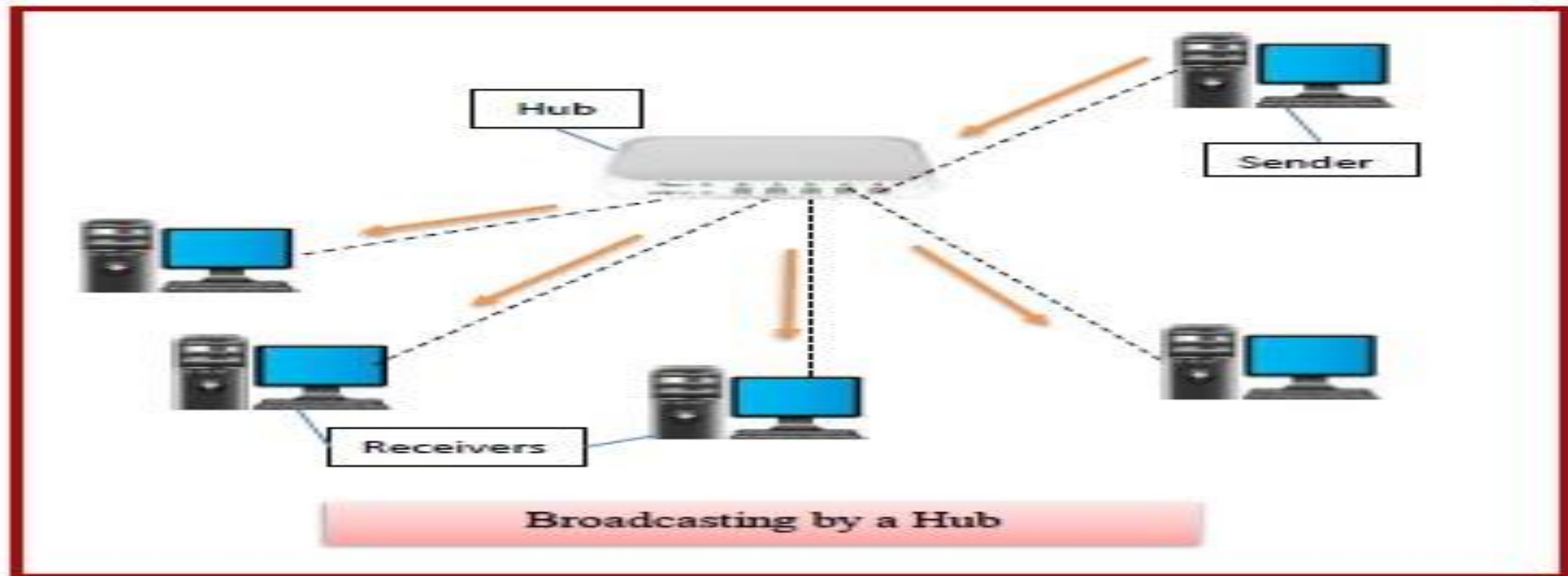
- The following diagram shows a bridges connecting two LANs –



# Network device Cont..

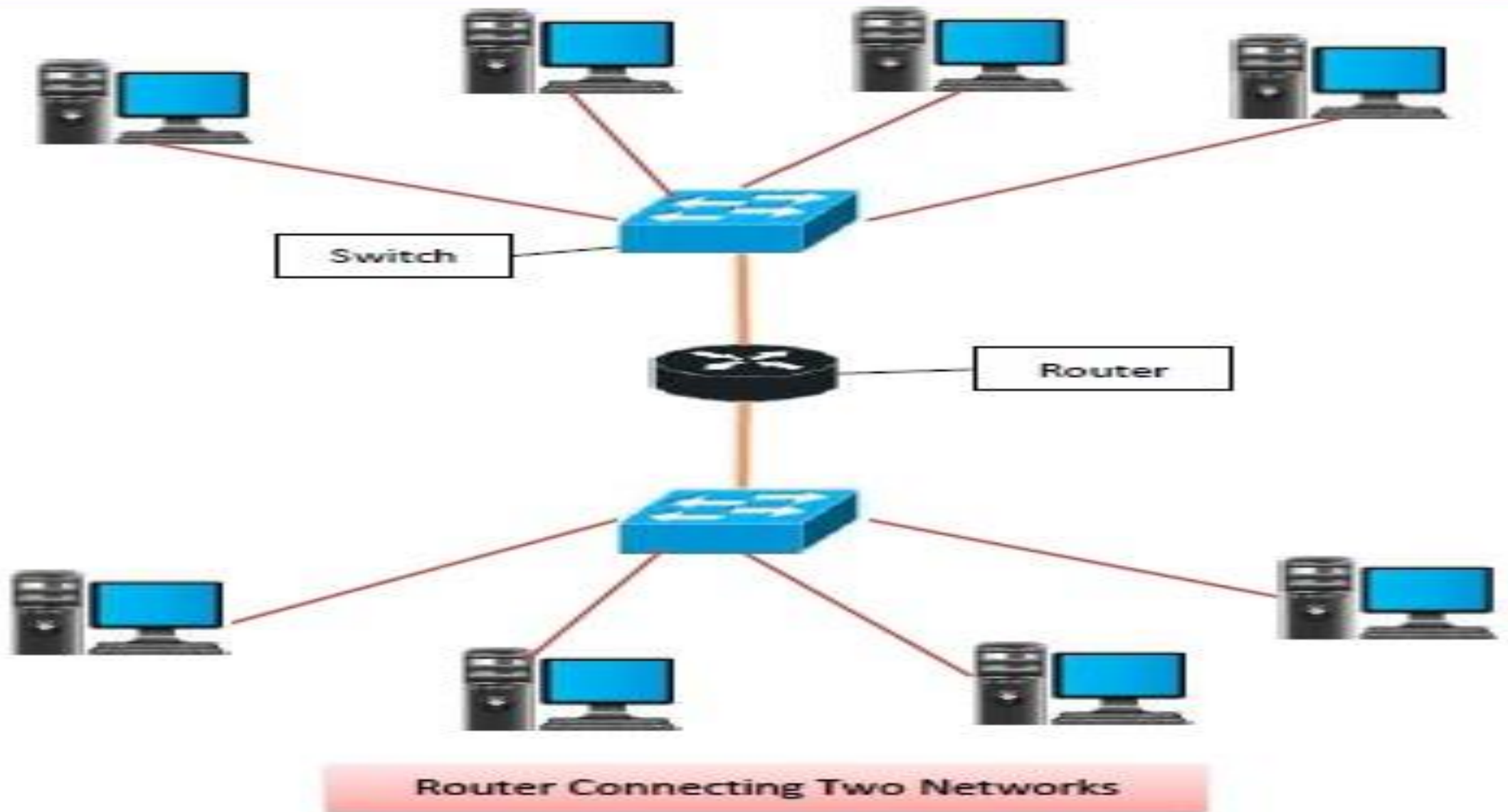
## 3. Hubs

- Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network.



## 4. Routers

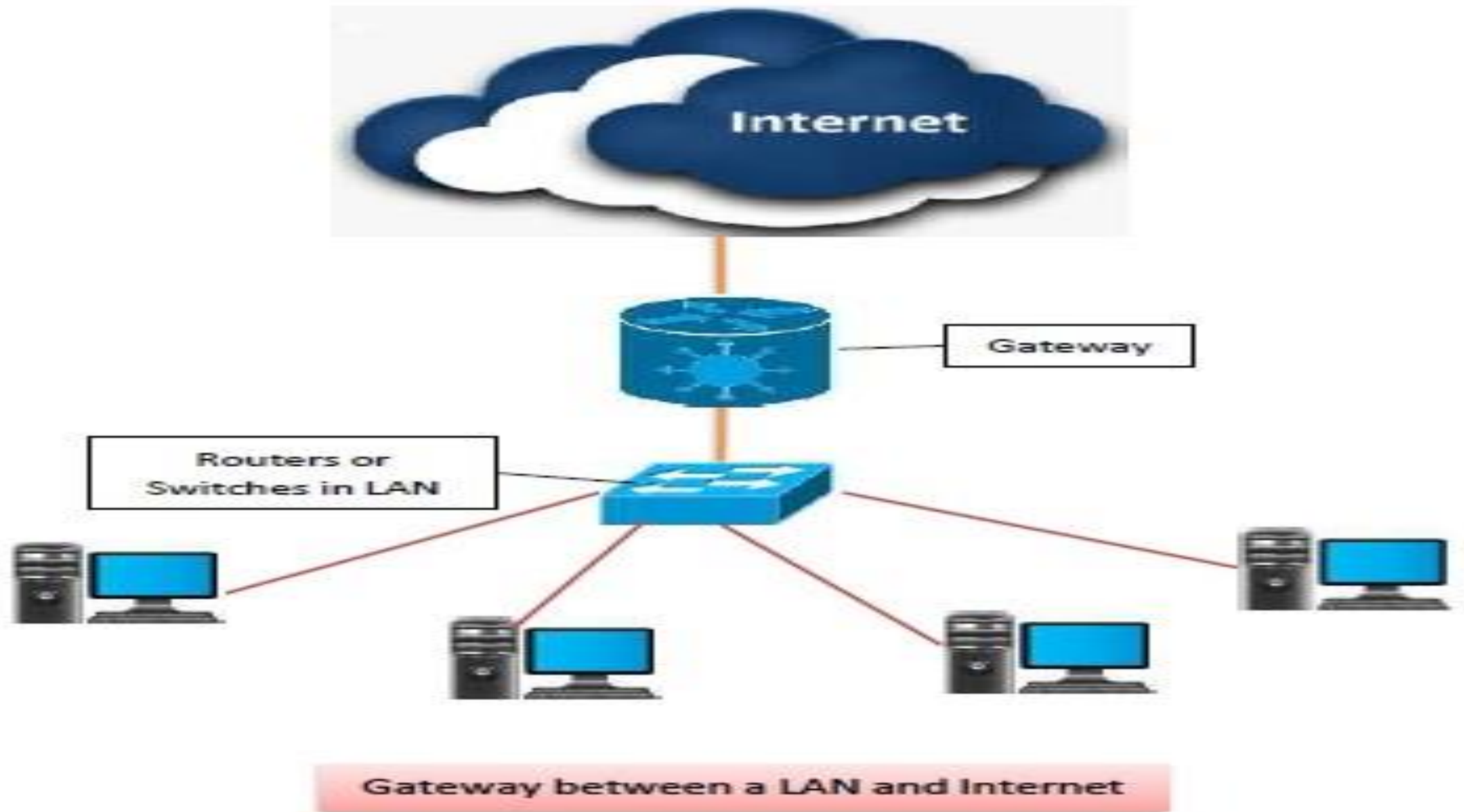
- A router is a three-layer device that routes packets based on their logical addresses (host-to host addressing).
- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route.
- Routers are networking devices operating at layer 3 or a network layer of the OSI model.
- They are responsible for receiving, analyzing, and forwarding data packets among the connected computer networks.
- When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.



# Network device Cont..

## 5. Gateway

- A gateway is a piece of networking hardware or software used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.
- A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models
- A gateway is a network node that forms a passage between two networks operating with different transmission protocols.
- The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model.
- However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model.
- It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway.
- Only the internal traffic between the nodes of a LAN does not pass through the gateway.



# Network device Cont..

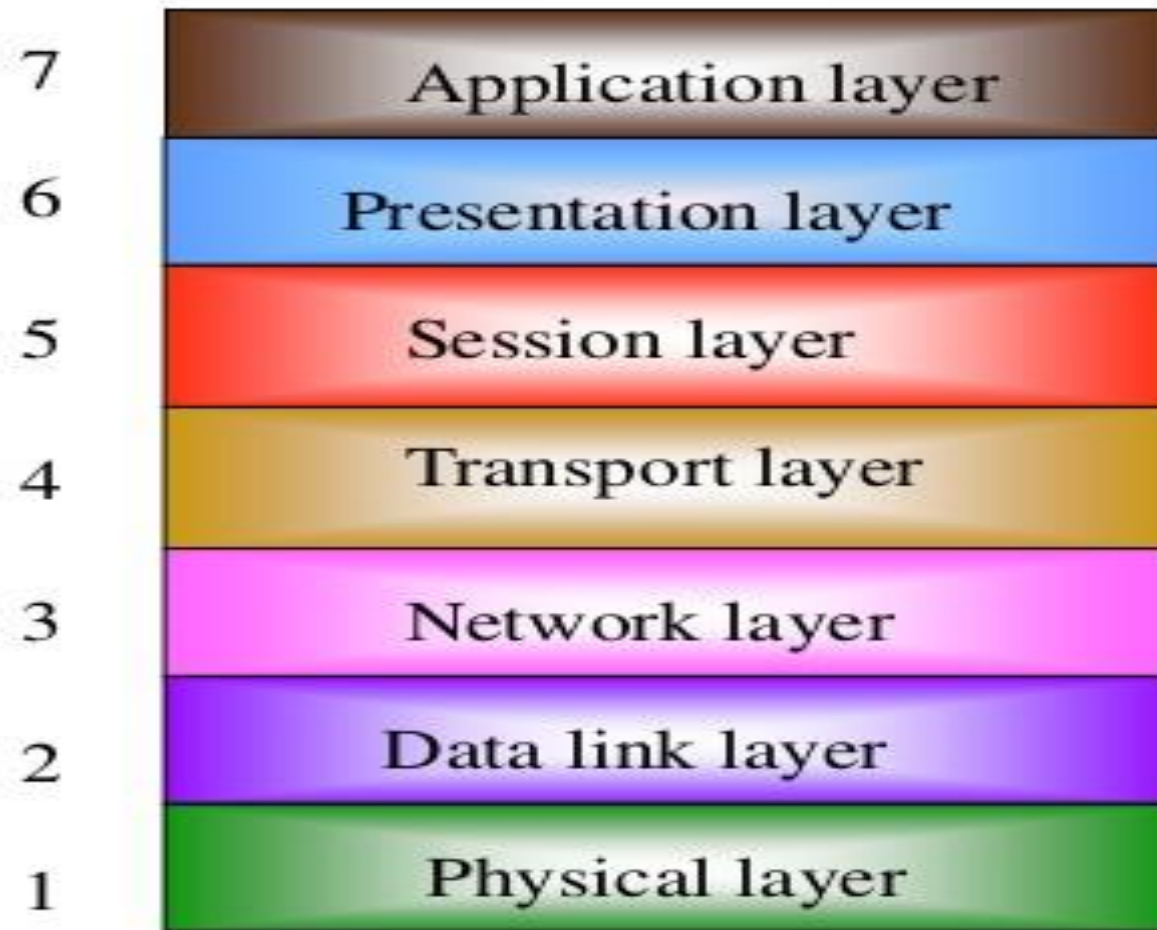
## 7. NIC

- A **network interface card (NIC)** is a hardware component, typically a circuit board or chip, which is installed on a computer so that it can connect to a network.
- 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.
- **Purpose**
- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.



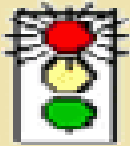

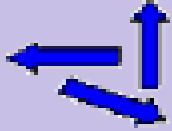


# OSI Reference Model

- **OSI** stands for Open Systems Interconnection.
- **OSI** model was developed by the International Organization for Standardization(ISO)
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.
- **The OSI model is composed of seven ordered layers:**

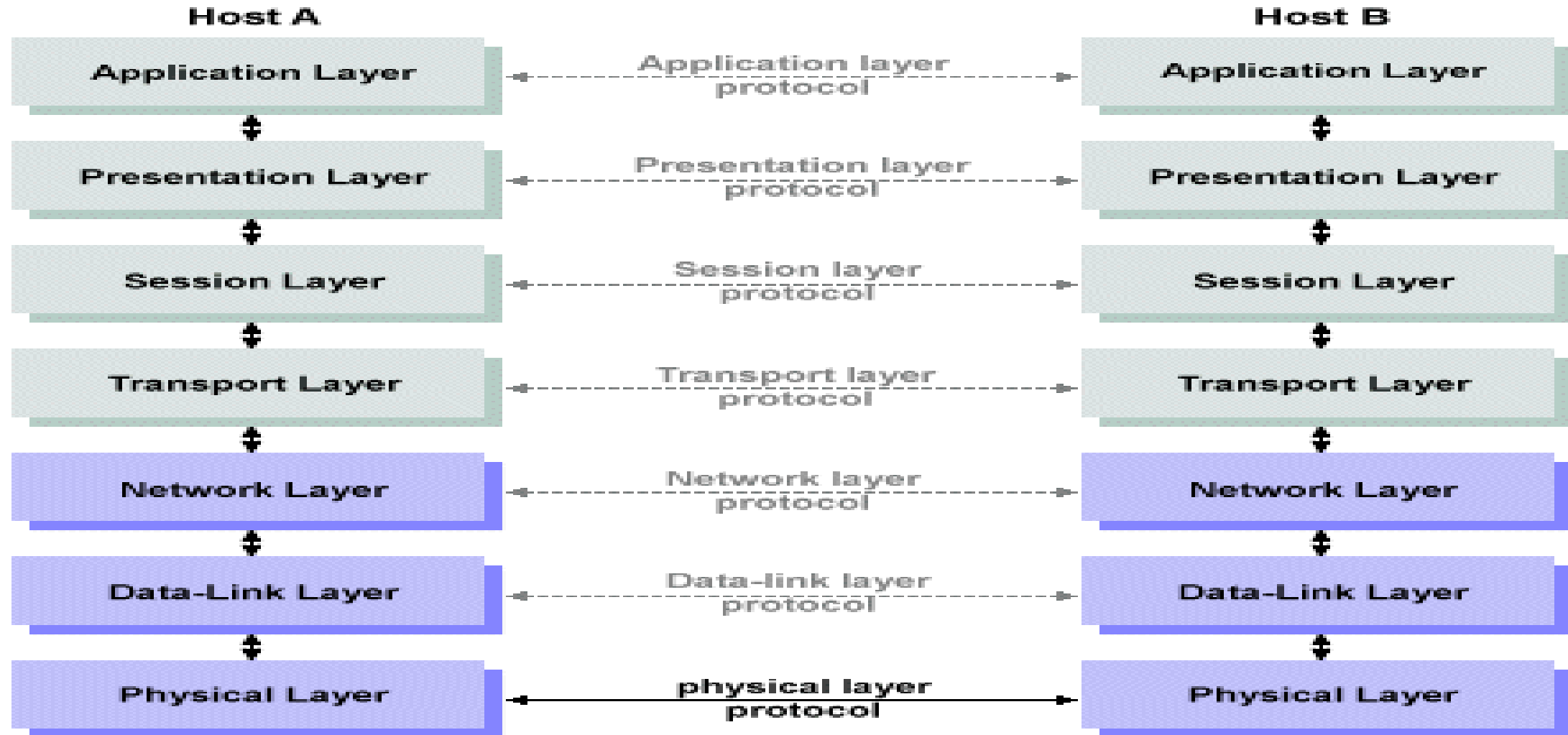
# OSI MODEL



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

OSI NETWORK MODEL				UPPER LAYERS
7		Application Layer	Network Process Applications	
6		Presentation Layer	Data Representation and Encryption	
5		Session Layer	Start & Stop Session Maintain Order	
4		Transport Layer	Ensures the delivery of entire file / message	LOWER LAYERS
3		Network Layer	Routes Data to different LANs/WANs	
2		Data Link Layer	Packet Transmission based on Stn Address	
1		Physical Layer	Media, Signal & Binary transmission	

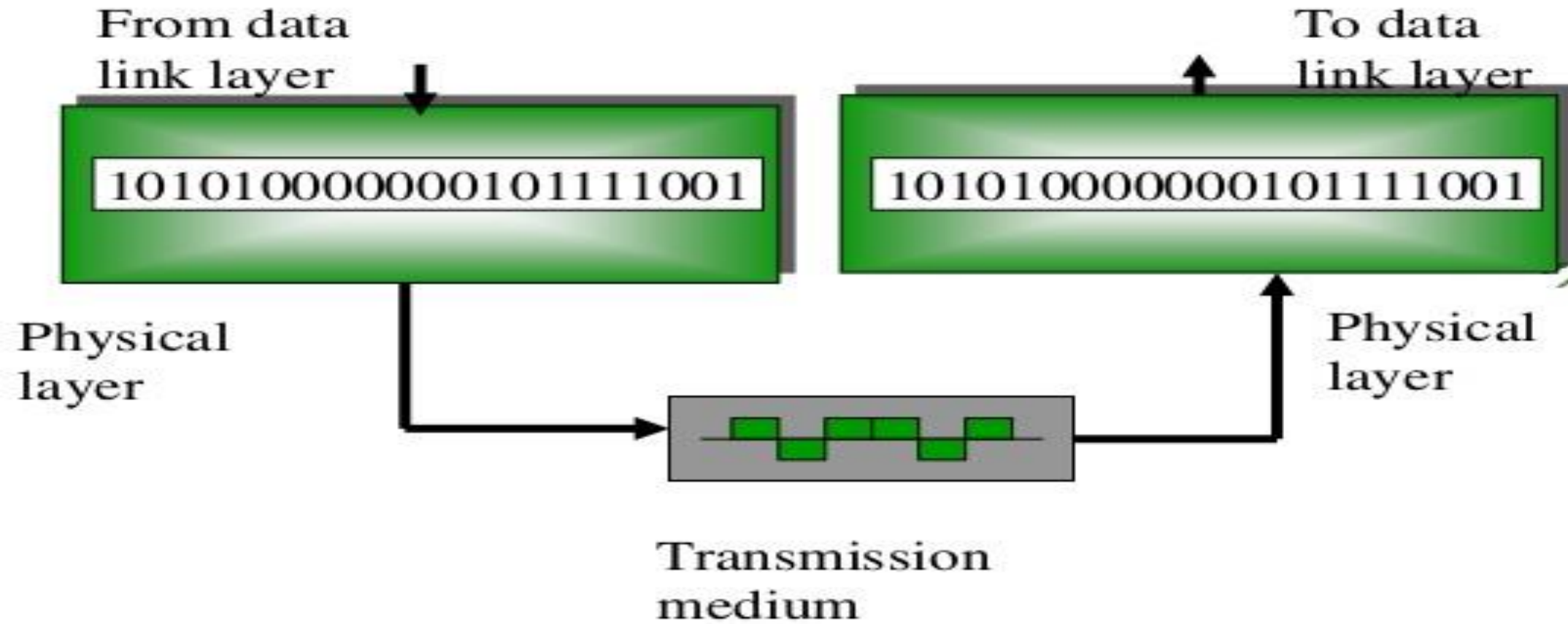
# Fig: OSI-ISO Reference Model



# 1.Physical Layer

- The physical layer coordinates the functions required to carry a bit stream over a physical medium.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.
- It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.

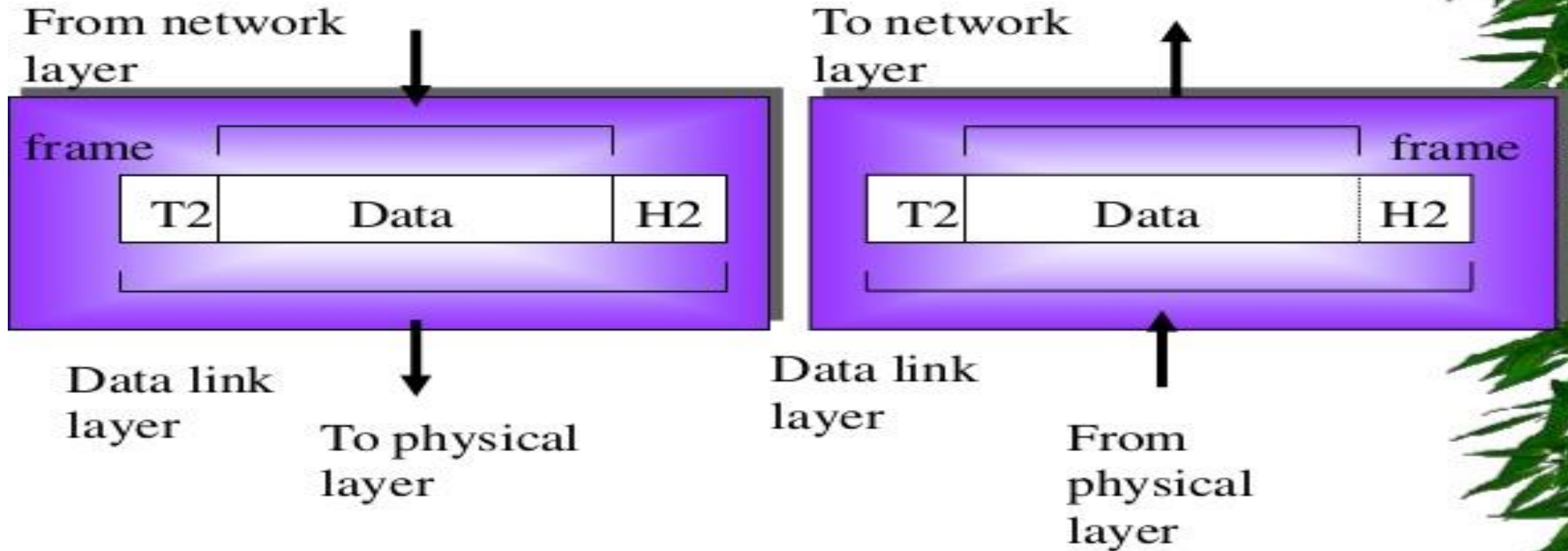
# PHYSICAL LAYER



## 2. Data Link Layer

- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).
- Other responsibilities of the data link layer include the following
  - **Framing** - The data link layer divides the stream of bits received from the network layer into manageable data units called frames
  - **Physical addressing:** The **Data Link layer** adds a header to the frame in order to define **physical address** of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network. This prevents traffic jam at the receiver side.
- At the **Data Link layer**, each device on the network has an **address** known as the Media Access Control **address**, or **MAC address**.
- **Flow control** - If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver
- **Error control** - The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame
- **Access control** - When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time

# DATA LINK LAYER



### 3. Network Layer

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
- Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.
- Other responsibilities of the network layer include the following:
  - **Logical addressing** - The physical addressing implemented by the data link layer handles the addressing problem locally.

If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

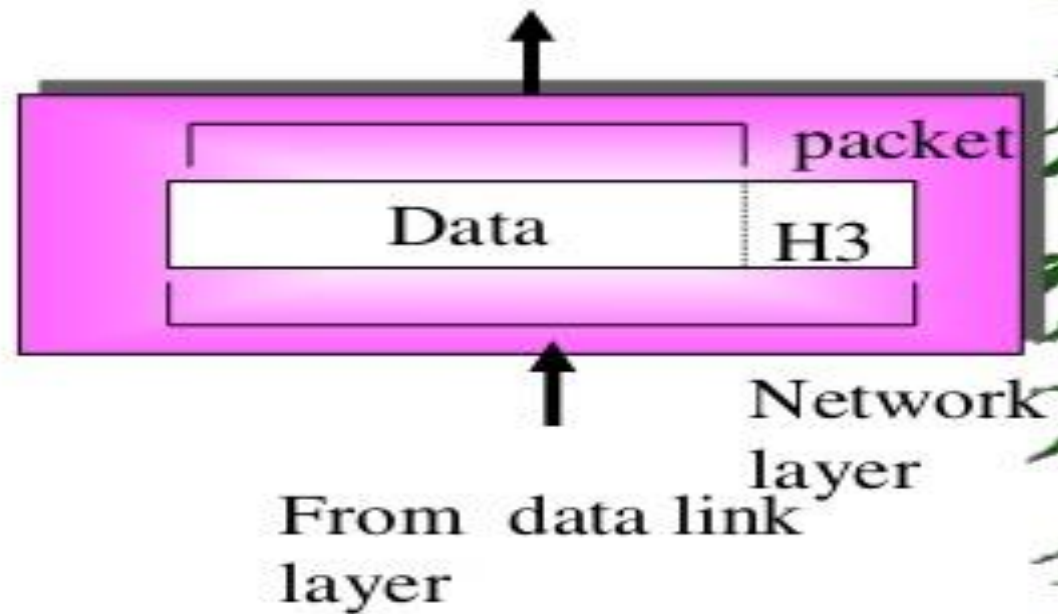
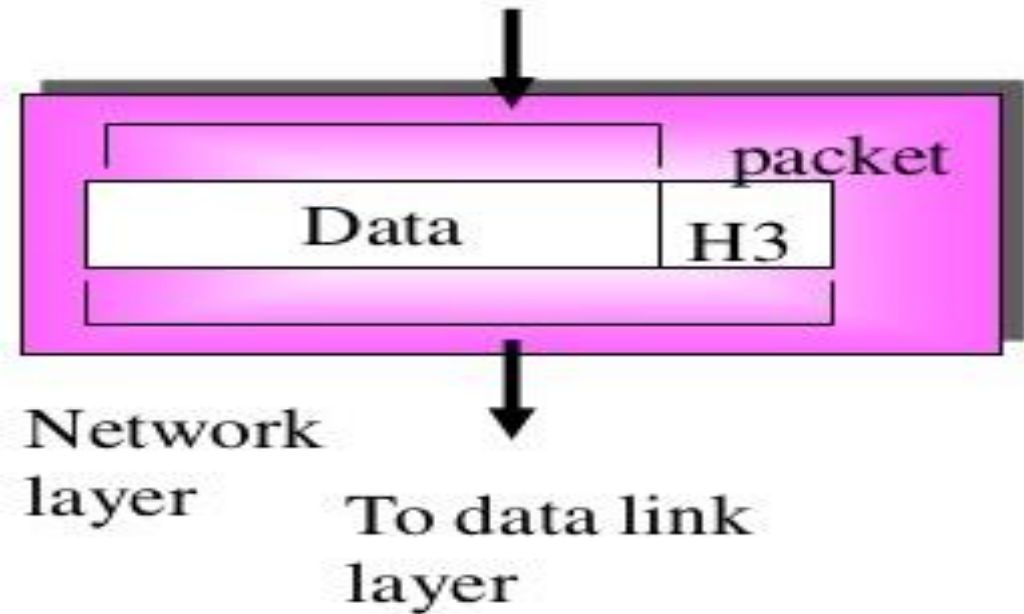
- **Routing** - When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

One of the functions of the network layer is to provide this mechanism.

# NETWORK LAYER

From transport layer

To transport layer



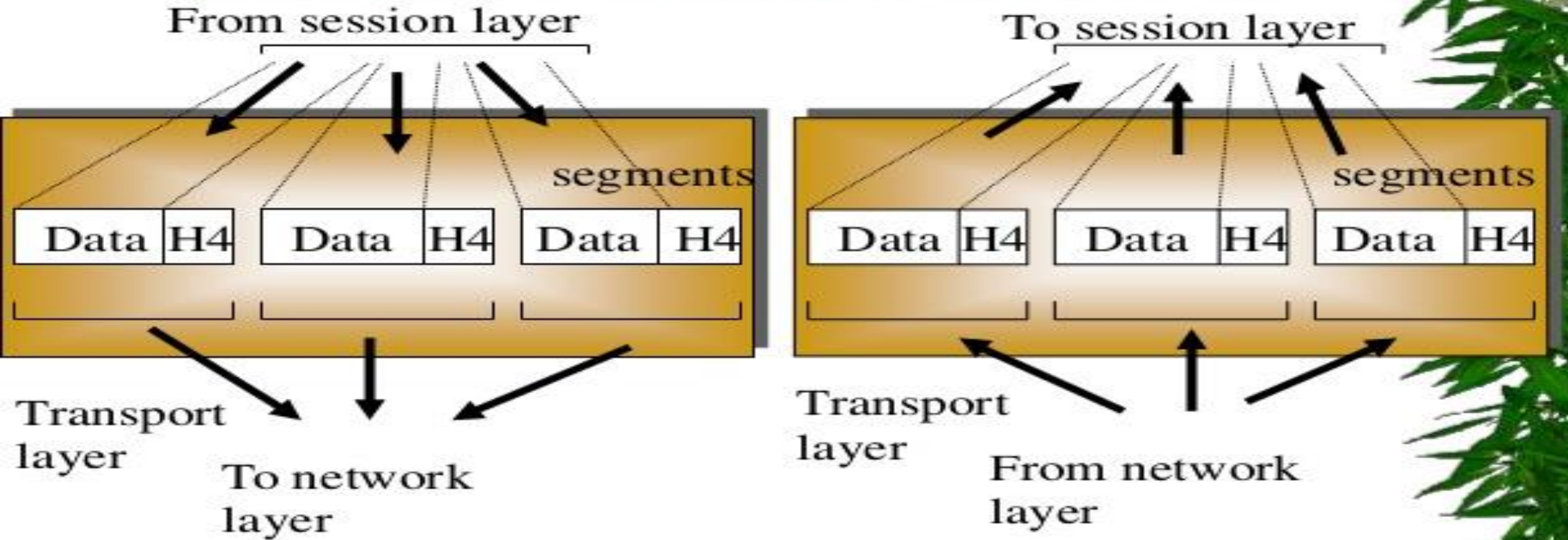
## 4. Transport Layer

- The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets.
- It treats each one independently, as though each piece belonged to a separate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Other function includes

- **Connection control** - The transport layer can be either connectionless or connection oriented.
- **Flow control** - Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission

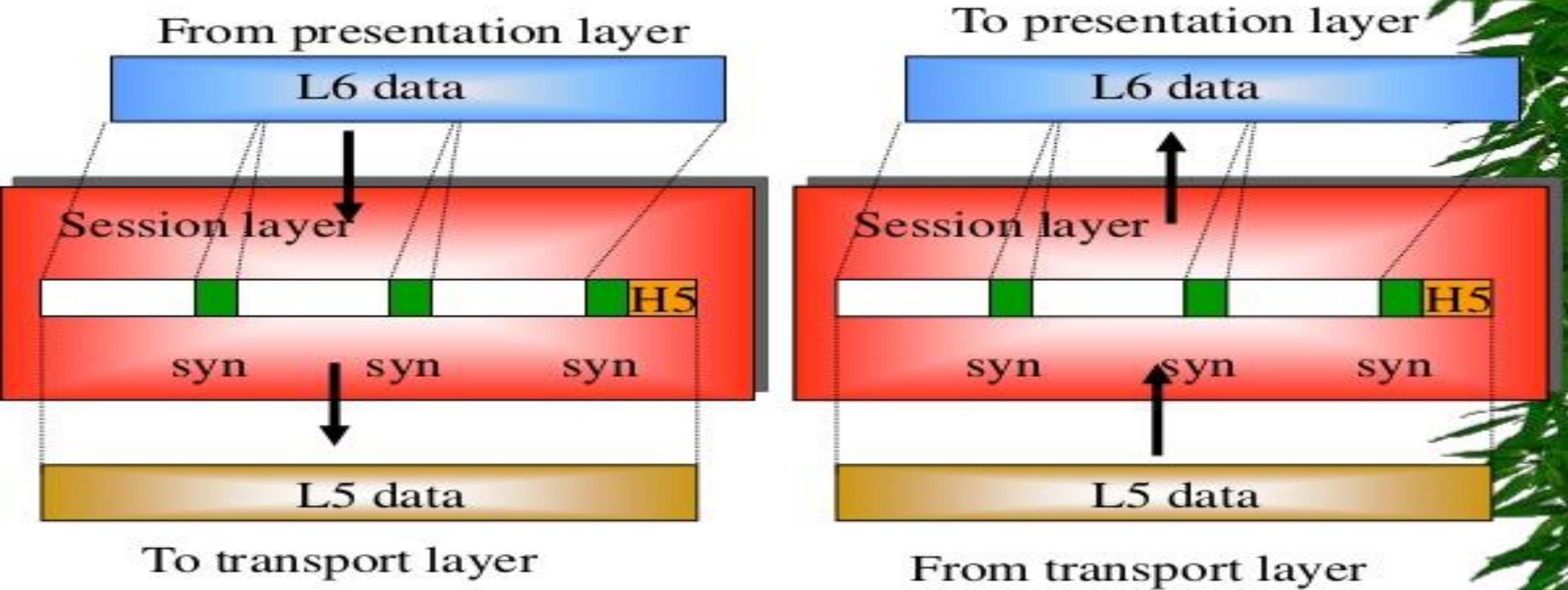
# TRANSPORT LAYER



## 5. Session Layer

- The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes.
- The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.
- Specific responsibilities of the session layer include the following:
  - **Dialog control** - The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
  - **Synchronization** - The session layer allows a process to add checkpoints, or synchronization points, to a stream of data

# SESSION LAYER

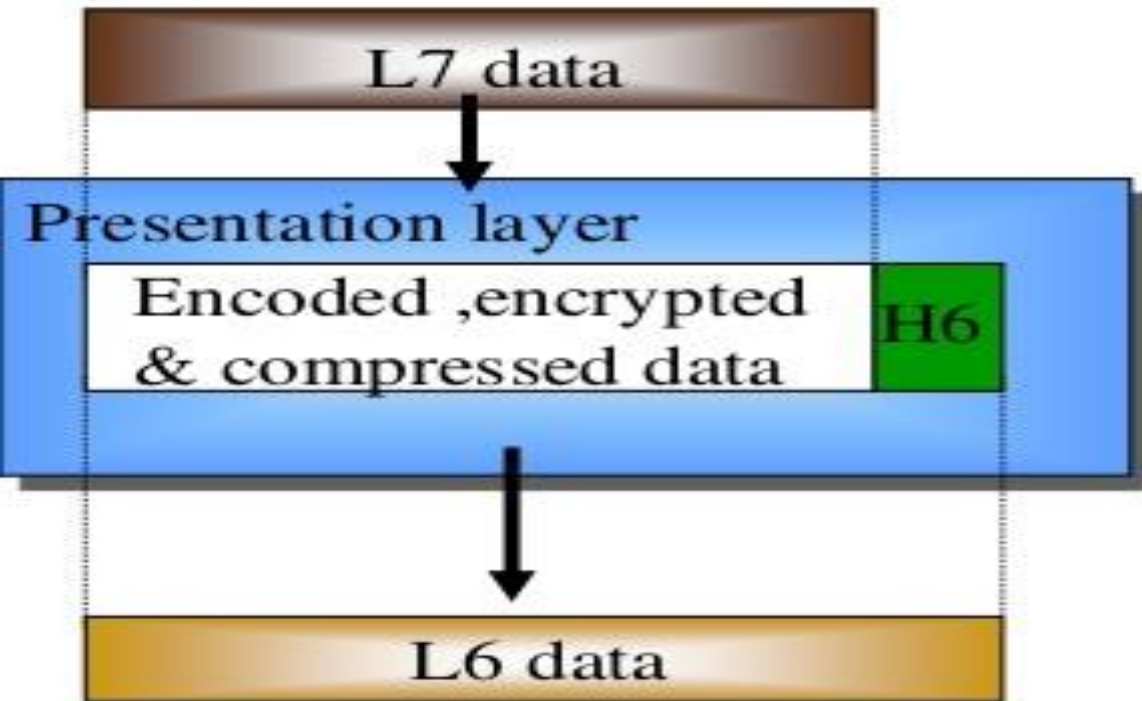


## 6. Presentation Layer

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems
  - **Translation** - Different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format
  - **Encryption** - To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
  - **Compression** - Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

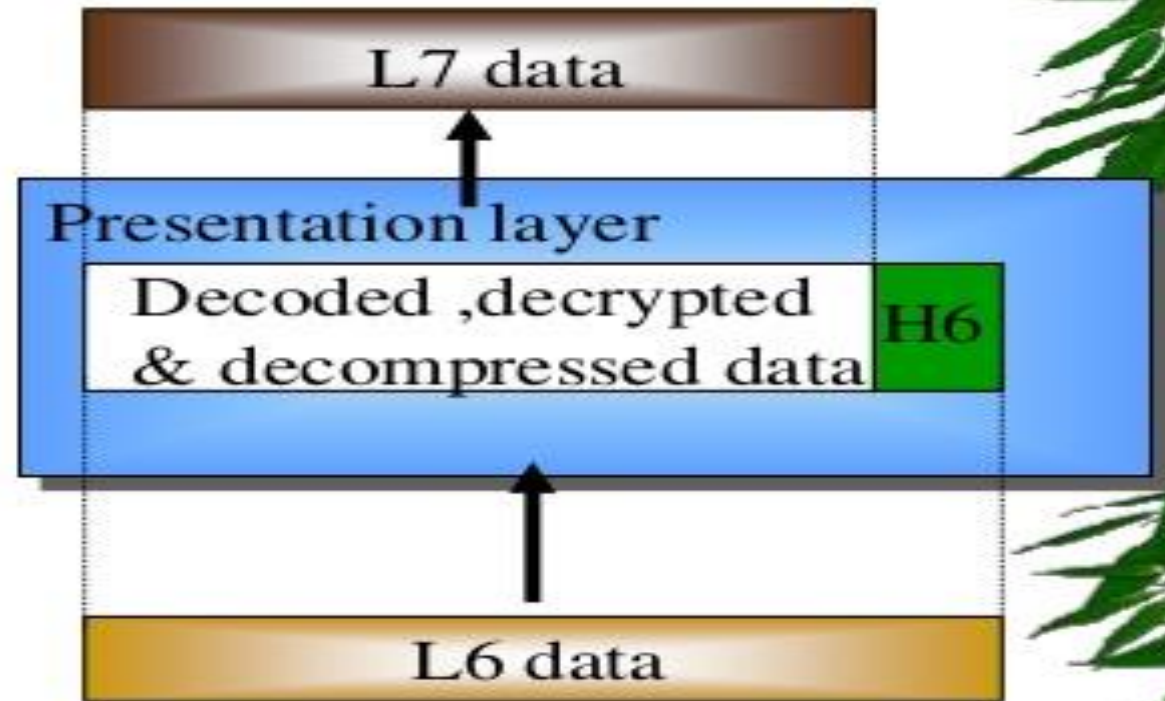
# PRESENTATION LAYER

From application layer



To session layer

To application layer

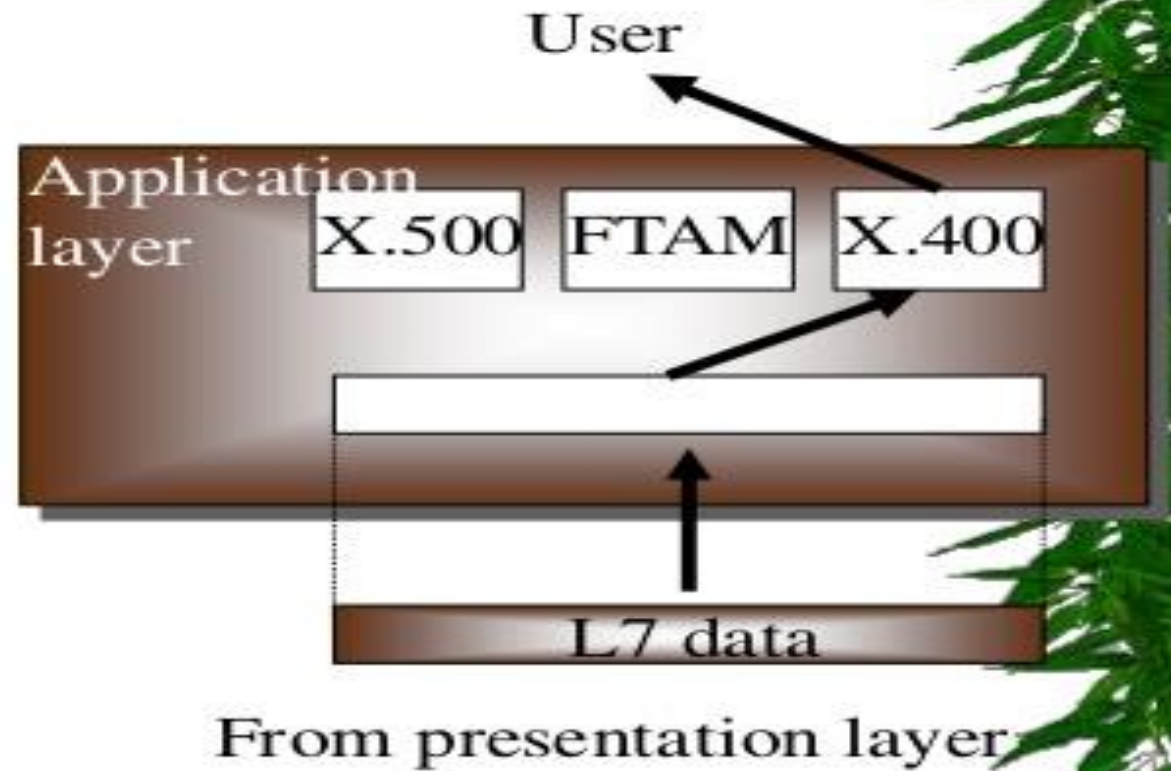
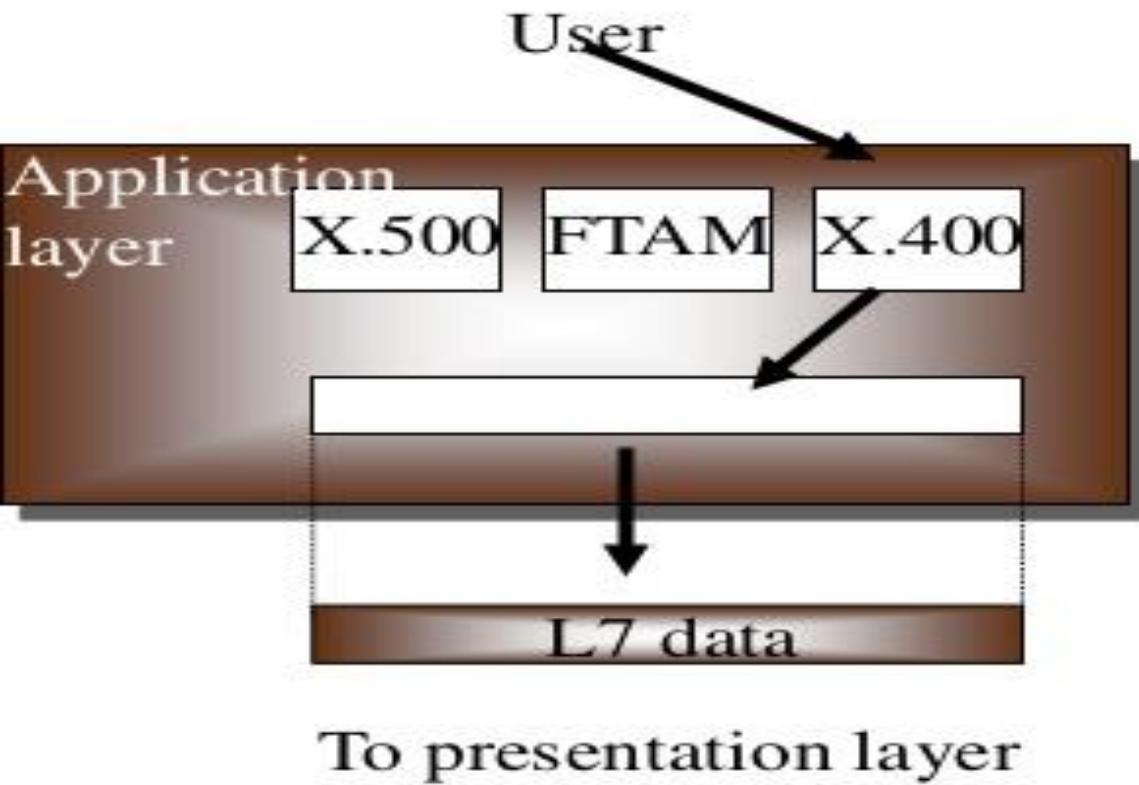


From session layer

## 7. Application Layer

- The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- Specific services provided by the application layer include the following:
  - **Network virtual terminal** - A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
  - **File transfer, access, and management** - This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
  - **Mail services** - This application provides the basis for e-mail forwarding and storage.
  - **Directory services** - This application provides distributed database sources and access for global information about various objects and services

# APPLICATION LAYER



## Application Layer Cont..

- The **X.500** directory service is a global directory service. Its components cooperate to manage information about objects such as countries, organizations, people, machines, and so on in a worldwide scope. It provides the capability to look up information by name (a *white-pages* service) and to browse and search for information (a *yellow-pages* service).
- **X. 400 addresses** are usually referred to as an Originator/Recipient [OR] **address** that have two purposes: Identify the mailbox of the originator or the recipient; Globally identify the domain where a mailbox is located
- **FTAM**, ISO standard 8571, is the OSI application layer protocol for file transfer, access and management.

# Communication Protocols

- All communications between devices require that the devices agree on the format of the data.
- The set of rules defining a format is called a protocol.
- At the very least, a communications protocol must define the following:
  - rate of transmission
  - whether transmission is to be synchronous or asynchronous
  - whether data is to be transmitted in half-duplex or full-duplex mode

**Network Protocols** are a set of rules governing exchange of information in an easy, reliable and secure way.

# Communication Protocols Cont..

- **Transmission Control Protocol (TCP)** – a connection-oriented communications protocol that facilitates the exchange of messages between computing devices in a network.
- It is the most common protocol in networks that use the Internet Protocol (IP); together they are sometimes referred to as TCP/IP.
- TCP takes messages from an application/server and divides them into packets, which can then be forwarded by the devices in the network – switches, routers, security gateways – to the destination.
- TCP numbers each packet and reassembles them prior to handing them off to the application/server recipient.
- Because it is connection-oriented, it ensures a connection is established and maintained until the exchange between the application/servers sending and receiving the message is complete.

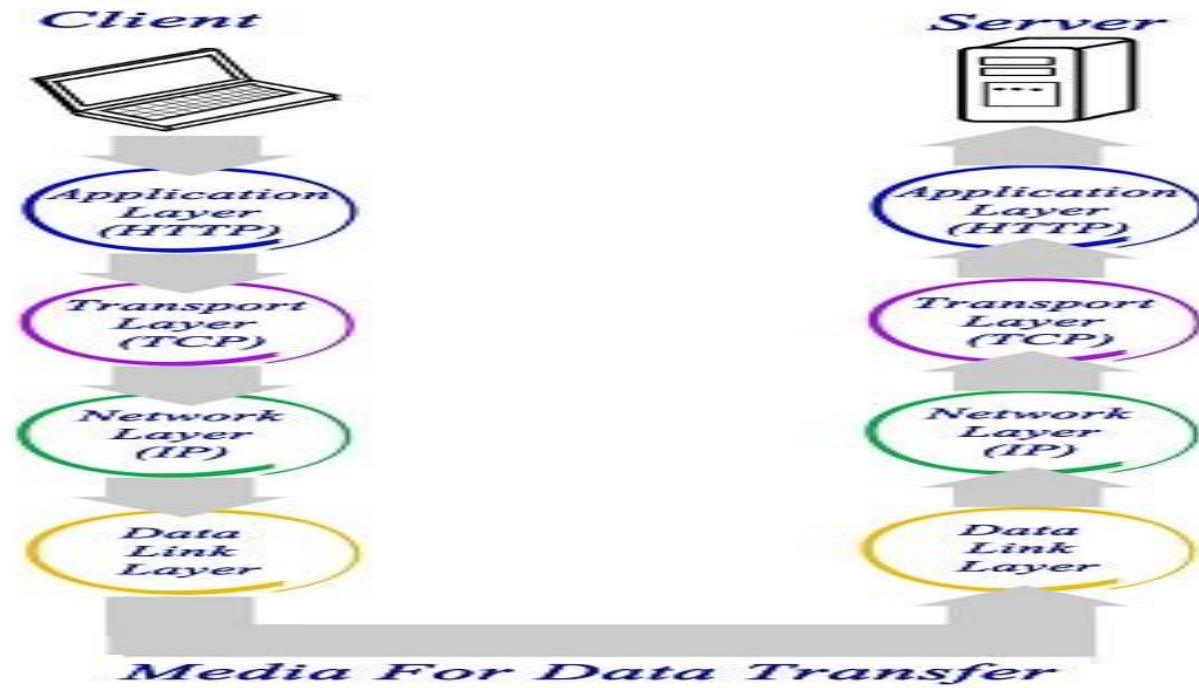
# TCP/IP (Transmission control Protocol/ Internet Protocol)

- TCP/IP is a set of layered protocols used for communication over the Internet. The communication model of this suite is client-server model.
- A computer that sends a request is the client and a computer to which the request is sent is the server.

## **TCP/IP has four layers –**

- **Application layer** – Application layer protocols like HTTP and FTP are used.
- **Transport layer** – Data is transmitted in form of datagram using the Transmission Control Protocol (TCP).
- TCP is responsible for breaking up data at the client side and then reassembling it on the server side.
- **Network layer** – Network layer connection is established using Internet Protocol (IP) at the network layer.
- Every machine connected to the Internet is assigned an address called IP address by the protocol to easily identify source and destination machines.
- **Data link layer** – Actual data transmission in bits occurs at the data link layer using the destination address provided by network layer.

# TCP/IP Cont..



# FTP (File Transfer Protocol)

- The **File Transfer Protocol (FTP)** is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network.
- File transfer protocol (**FTP**) is a set of rules that computers follow for the transferring of files from one system to another over the internet.
- It may be used by a business to transfer files from one computer system to another, or websites may use **FTP** to upload or download files from a website's server.
- The protocol that handles these requests is **File Transfer Protocol** or **FTP**.
- Using FTP to transfer files is helpful in these ways –
- Easily transfers files between two different networks
- Can resume file transfer sessions even if connection is dropped, if protocol is configured appropriately
- Enables collaboration between geographically separated teams

# FTP (File Transfer Protocol) Cont..

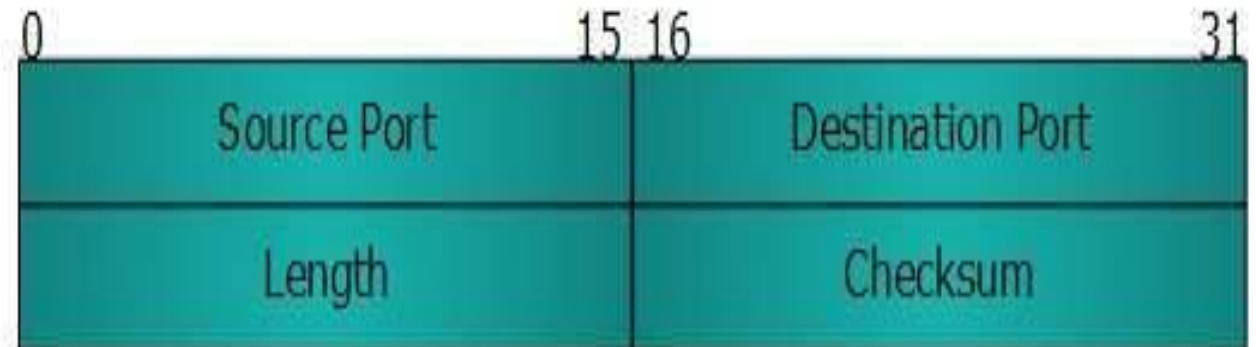


# UDP ( User Datagram Protocol)

- The **User Datagram Protocol (UDP)** is simplest Transport Layer Communication **protocol** available of the TCP/IP **protocol** suite. It involves minimum amount of communication mechanism.
- **UDP** is said to be an unreliable transport **protocol** but it uses IP services which provides best effort delivery mechanism. In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent.
- This shortcoming makes this protocol unreliable as well as easier on processing.
- **Features**
- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

# UDP ( User Datagram Protocol) Cont..

- **UDP Header**
- UDP header is as simple as its function.
- UDP header contains four main parameters:
- **Source Port** - This 16 bits information is used to identify the source port of the packet.
- **Destination Port** - This 16 bits information, is used identify application level service on destination machine.
- **Length** - Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.
- **Checksum** - This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero.



# Communication Protocols Cont..

## What is HTTP (Hypertext Transfer Protocol)?

- The Hypertext Transfer Protocol is an application protocol for distributed, collaborative, hypermedia information systems that allows users to communicate data on the World Wide Web.
- HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.
- Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well.
- It provides a standardized way for computers to communicate with each other.
- HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

# PPP ( Point to Point Protocol)

- Point to Point Protocol or PPP is a data link layer protocol that enables transmission of TCP/IP traffic over serial connection, like telephone line.
- To do this, PPP defines these three things –
- A framing method to clearly define end of one frame and start of another, incorporating errors detection as well.
- Link control protocol (LCP) for bringing communication lines up, authenticating and bringing them down when no longer needed.
- Network control protocol (NCP) for each network layer protocol supported by other networks.

# Wireless Networking

- **Wireless** networking **technology** is an alternative to traditional cable and fiber optic networks.
- It is fast becoming a vital productivity tool for today's mobile workforce.
- A **wireless** network uses radio waves instead of cables to connect devices such as laptops to the internet, or to your business network.
- **Wireless technology** refers to **technology** that allows us to communicate without using cables or wires. At the time it meant “communication via radio waves rather than with cables or wires.” The term may also refer to devices that draw power without using cables.
- **The Different Types of Wireless Communication**
- Satellite Communication. Satellite communication is a crucial form of **wireless** communication. .
- Broadcast Radio. ...
- Microwave Communication. ...
- Wi-Fi. ...
- Mobile Communication Systems. ...
- Bluetooth **Technology**.

# Wireless Networking Cont..

- **Mobile Communication** is the use of technology that allows us to communicate with others in different locations without the use of any physical connection (wires or cables). Mobile communication makes our life easier, and it saves time and effort.
- **A mobile phone** (also called mobile cellular network, cell phone or hand phone) is an example of mobile communication (wireless communication). It is an electric device used for full duplex two way radio telecommunication over a cellular network of base stations known as cell site.
- **Applications of wireless communication** involve security systems, television remote control, Wi-Fi, **Cell phones**, **wireless** power transfer, computer interface devices, and various **wireless communication**-based projects.

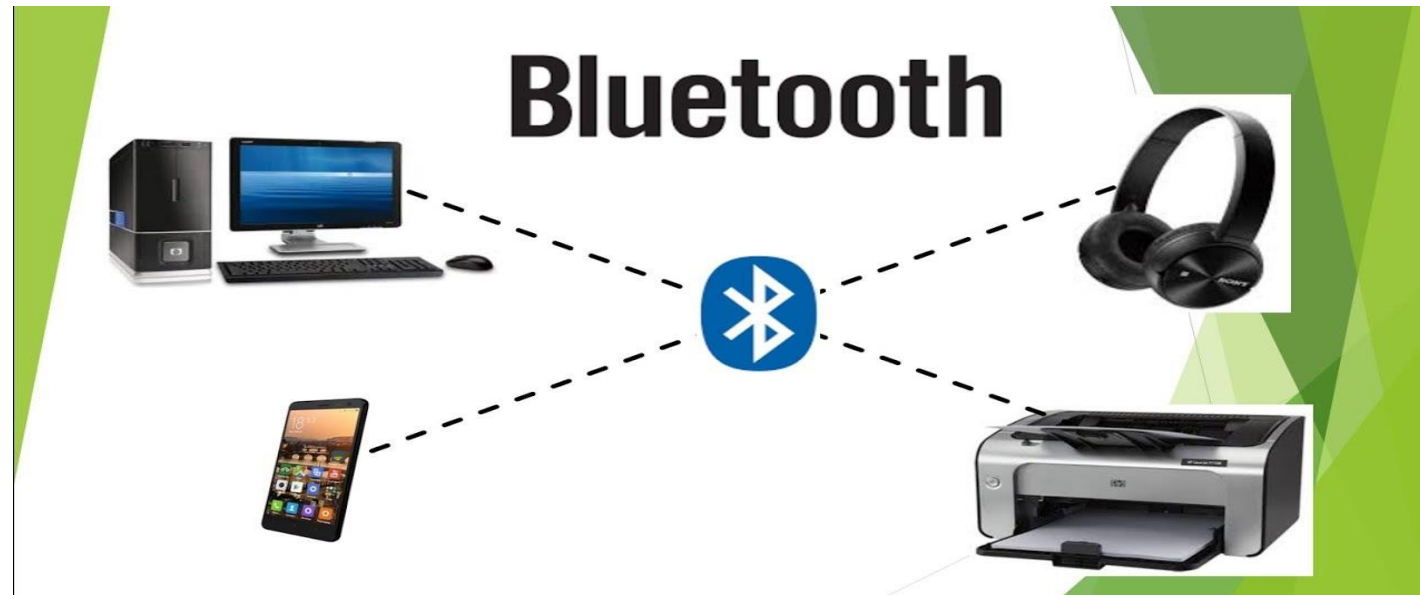
# Wireless Networking Cont..

## WiFi ( Wireless Fidelity)

- Wi-Fi is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to interface with the Internet.
- Internet connectivity occurs through a wireless router. Wi-Fi is a popular wireless networking technology. Wi-Fi stands for “wireless fidelity”.
- **The applications of WiFi include the following.**
- Mobile **applications**.
- Business **applications**.
- Home **applications**.
- Computerized **application**.
- Automotive segment.
- Browsing **internet**.
- Video conference.

# Wireless Networking Cont..

- **Bluetooth technology** is a short-range wireless communications **technology** to replace the cables connecting electronic **devices**, allowing a person to have a phone conversation via a headset, use a wireless mouse and synchronize information from a mobile phone to a PC, all using the same core system





Thank you!