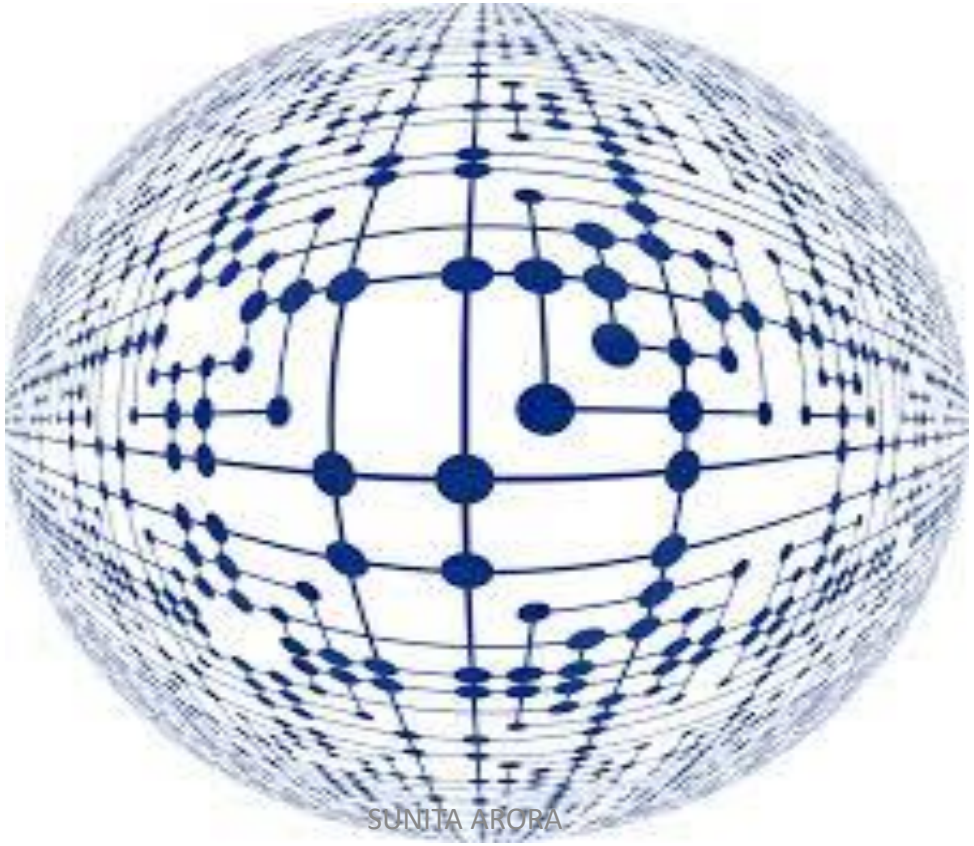
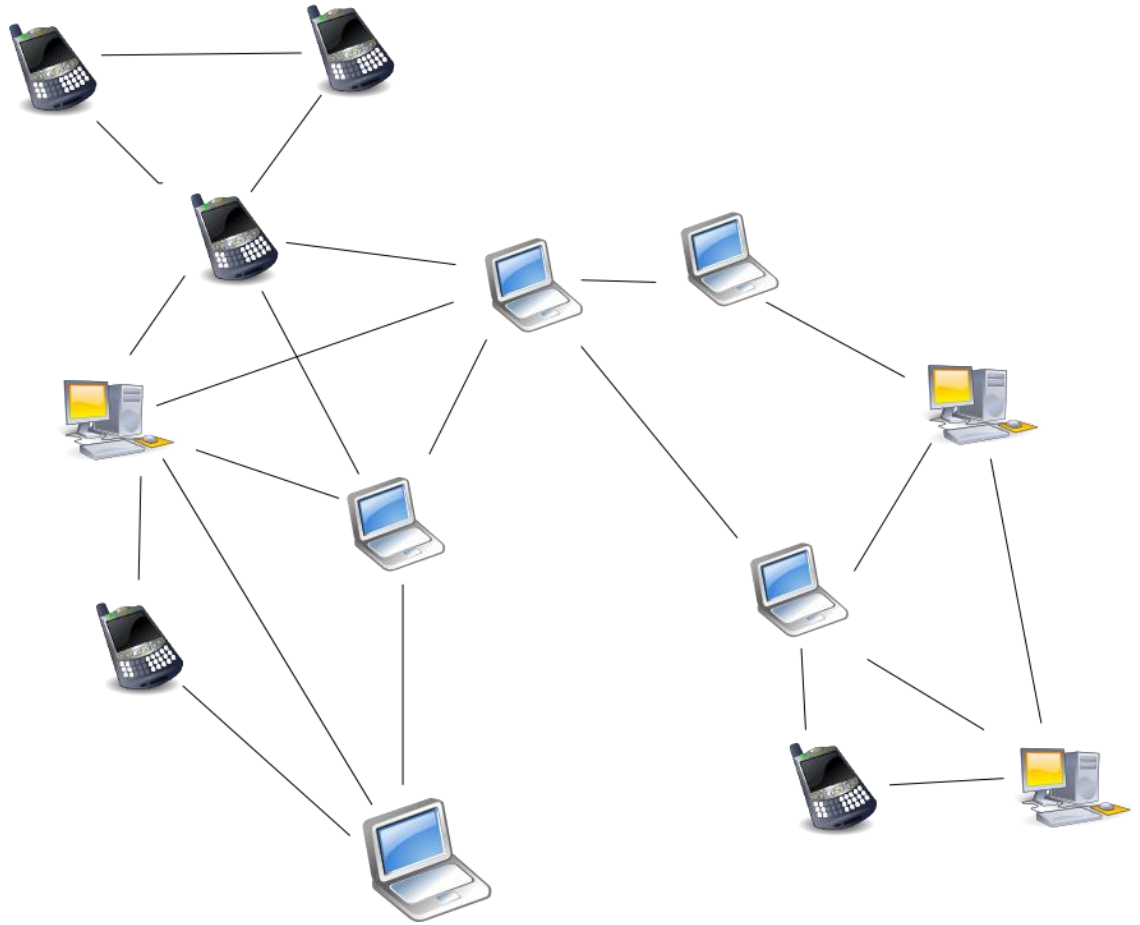
COMPUTER NETWORKING



PART 1

TOPICS

1. Computer Networks
2. Network Topologies
3. Types of Networks
4. Network Devices
5. The Cloud
6. Internet of Things (IoT)



COMPUTER NETWORKS

- Connections among humans make human network and connections among computes make computer networks.
- A computer network is a collection of interconnected autonomous computing devices so as to exchange information or share resources.
- For example, if in your home, you can connect your smartphone, your laptop with smart TV, gaming console and a printer simultaneously either using cables or through WiFi, it will be termed as a computer network.

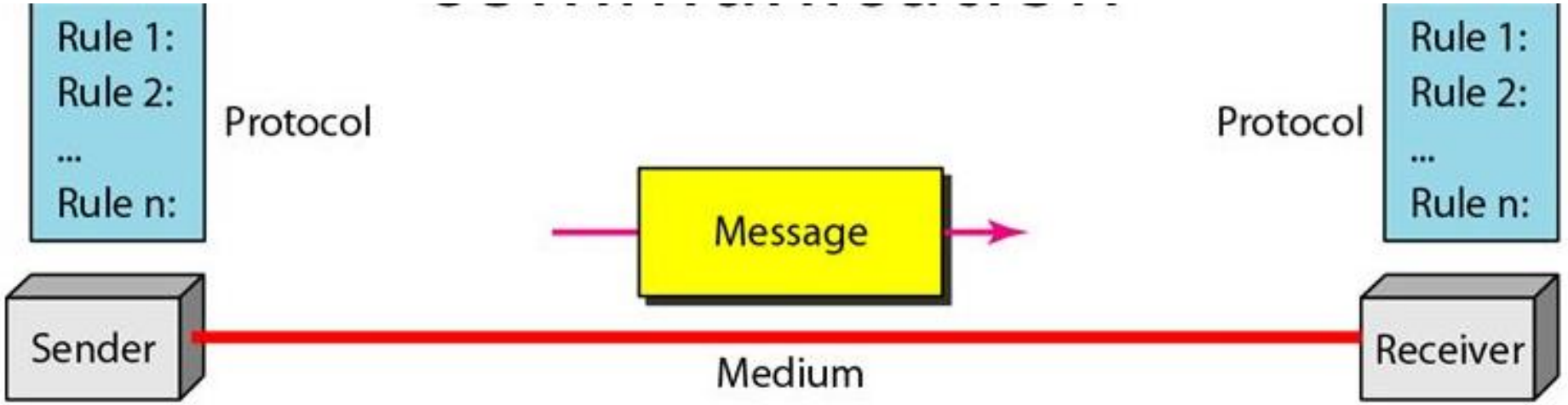
- **Advantages of Networks:**
- **1. Share resources:** such as printers and scanners. This is cheaper than buying equipments for each computer.
- **2. Share software:** Software can be installed centrally rather than on each machine. Metering software can then be used to limit the number of copies being run at any one time. This is much cheaper than buying licenses for every machine.
- **3. Share storage:** being able to access files from any machines on the network can share data.
- **4. Improve communication:** Messages can be sent – eg., internal email.

- **Disadvantages of networks:**
- **1.** The systems are **more sophisticated** and **complex** to run. This can add to costs and you may need specialist staff to run the network.
- **2.** If software and files are being held **centrally,** it may be impossible to carry out any work if the central server fails. People become reliant on the communications. If these fail, it can cause havoc.
- **3.** If the networks are **badly managed**, services can become unusable and productivity fails.
- **4. File security** is more important especially if connected to WANs e.g., protection from viruses.

- **Components of a computer network:**
- **1. Hosts/Nodes:**
- A computer becomes a workstation of a network as soon as it is attached to a network.
- The term host or node refers to the computers that are attached to a network and are seeking to share the resources of the network.
- PCs, laptops, smartphones etc. when connect to a network becomes hosts.
- **2. Servers:**
- A computer that facilitated the sharing of data, software, and hardware resources (e.g., printers, modems etc.) on the network, is termed as a server.
- A server is responsible for making the networking tasks happen.
- A server facilitates networking tasks like sharing of data, resources-sharing, communication among hosts etc.
- On small networks, sometimes, all the shareable stuff (like files, data, software etc.) is stored on the server.

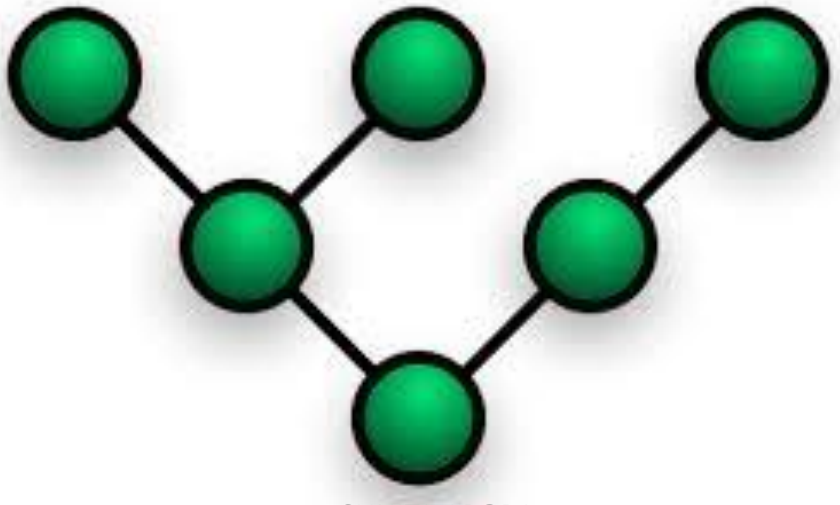
- A network can have more than one server also.
- Each server has a unique name on the network and all users of network identify the server by its unique name.
- On big networks, there can be servers dedicated to specialized tasks e.g., a file server only handles files related requests; a printer server only handles printing requests and so on.
- **3. Clients:** A client computer is a host computer that requests for some services form a server. Likewise, a server computer serves the requests of client computers.
- **4. Network hardware:** A network requires specialized hardware to carry out various roles, such as establishing connections, controlling network traffic etc. Some examples of network hardware are, NIC, hub, switch, router, gateway, modem, repeater.

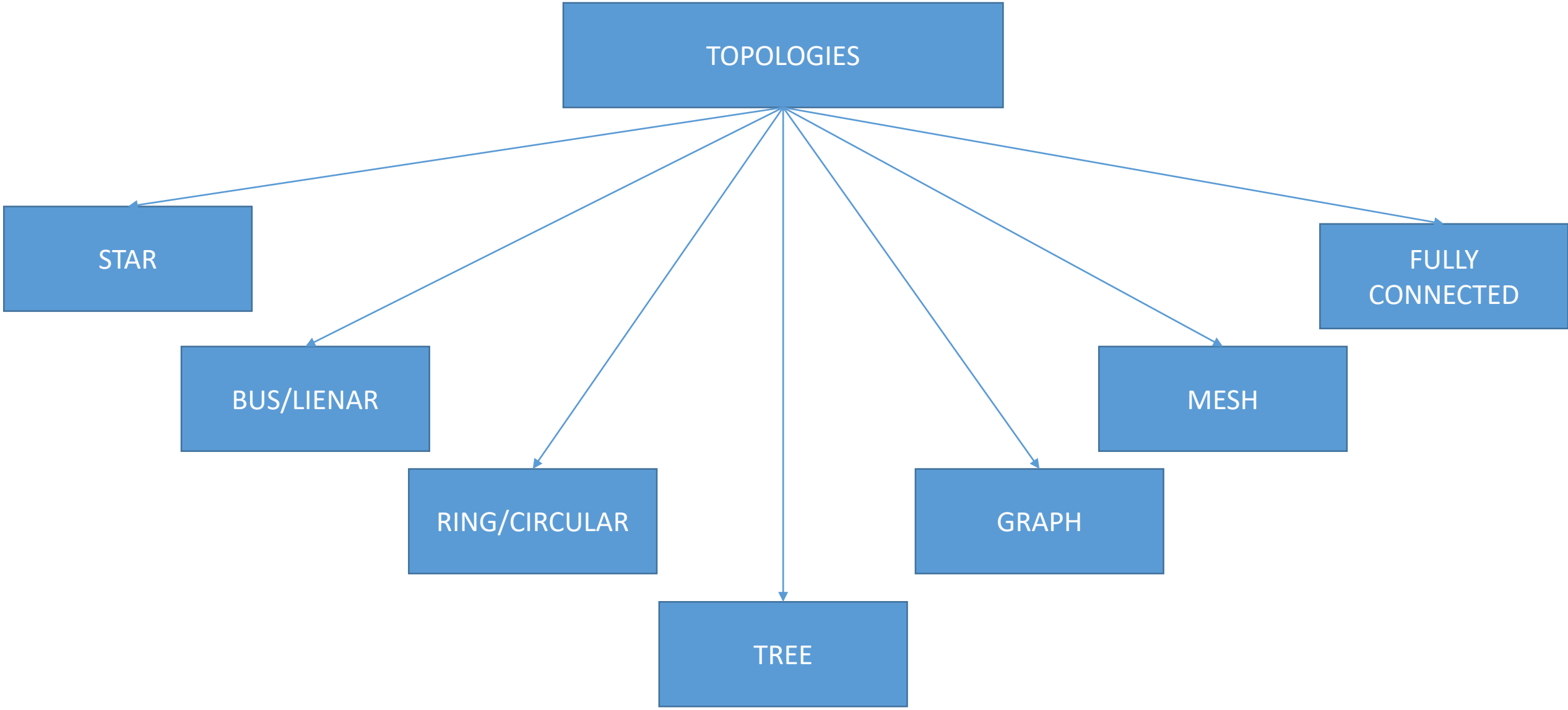
- **5. Communication channel:** Hosts in a network interact with other hosts and server(s) through a communication channel or communication medium. The communication channel can either be wired or wireless.
- **6. Software:** The software layers of a network make networking possible. These comprise of network protocols, network operating system etc.
- **7. Network services:** These refer to the applications that provide different functionalities over a network, such as DNS (Domain Name System), File sharing, VoIP (Voice over IP).



NETWORK TOPOLOGIES

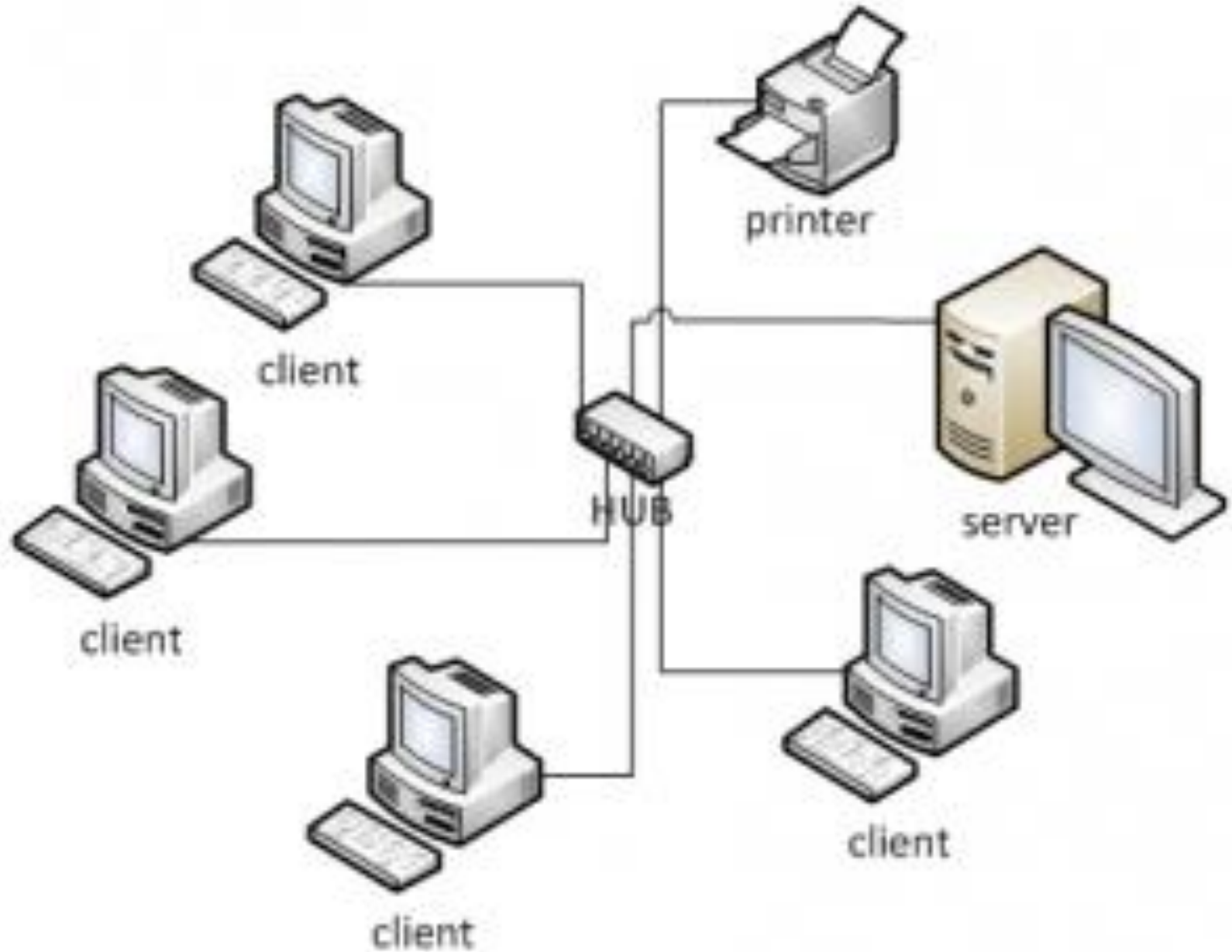
- The pattern of interconnection of nodes in a network is called the topology.
- Factors to consider in selecting the type of topology:
- **1. cost**
- **2. flexibility**
- **3. reliability**




TOPOLOGIES
STAR
BUS/LIENAR
RING/CIRCULAR
TREE
GRAPH
MESH
FULLY CONNECTED

- **<u>Star topology</u>**
- This topology consists of a central node to which all other nodes are connected by a single path.
- **advantages:**
- **1.ease of service**
- **2. one device per connection**
- **3. centralized control/ problem diagnosis**
- **4. simple access protocols**

- **Disadvantages:**
- **1. long cable length**
- **2.Difficult to expand**
- **3. central node dependency**

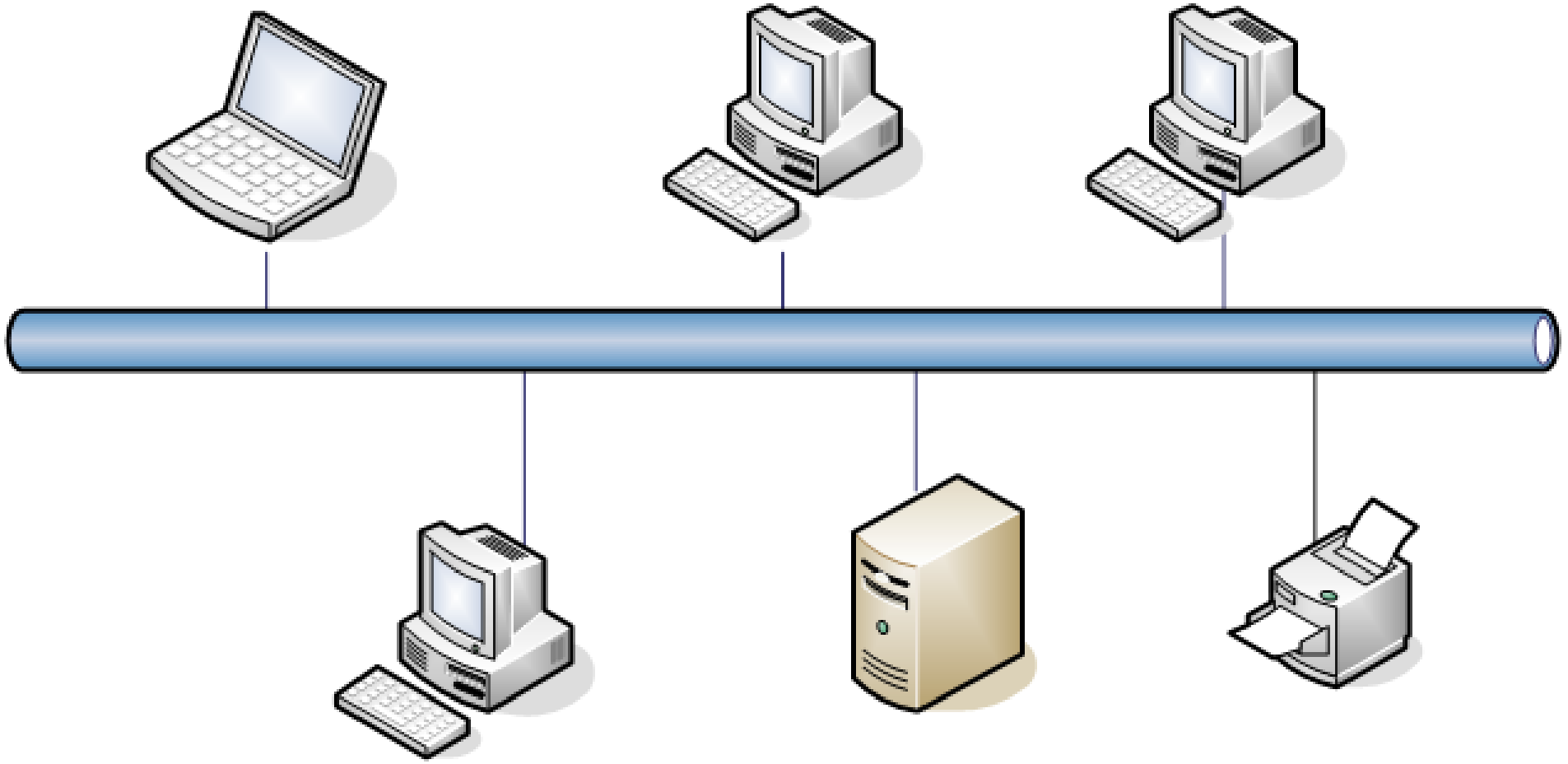

printer
client
client
HUB
server
client
client

- **<u>Bus or linear topology:</u>**
- This consists of a single length of transmission medium (normally coaxial cable) onto which the various nodes are attached.

- **Advantages:**
- **1. short cable length and simple wiring**
- **2. resilient architecture**
- **3. easy to extend**

- **Disadvantages:**
- **1. fault diagnosis is difficult**
- **2.fault isolation is difficult**
- **3. repeater configuration**
- **4. nodes must be intelligent**

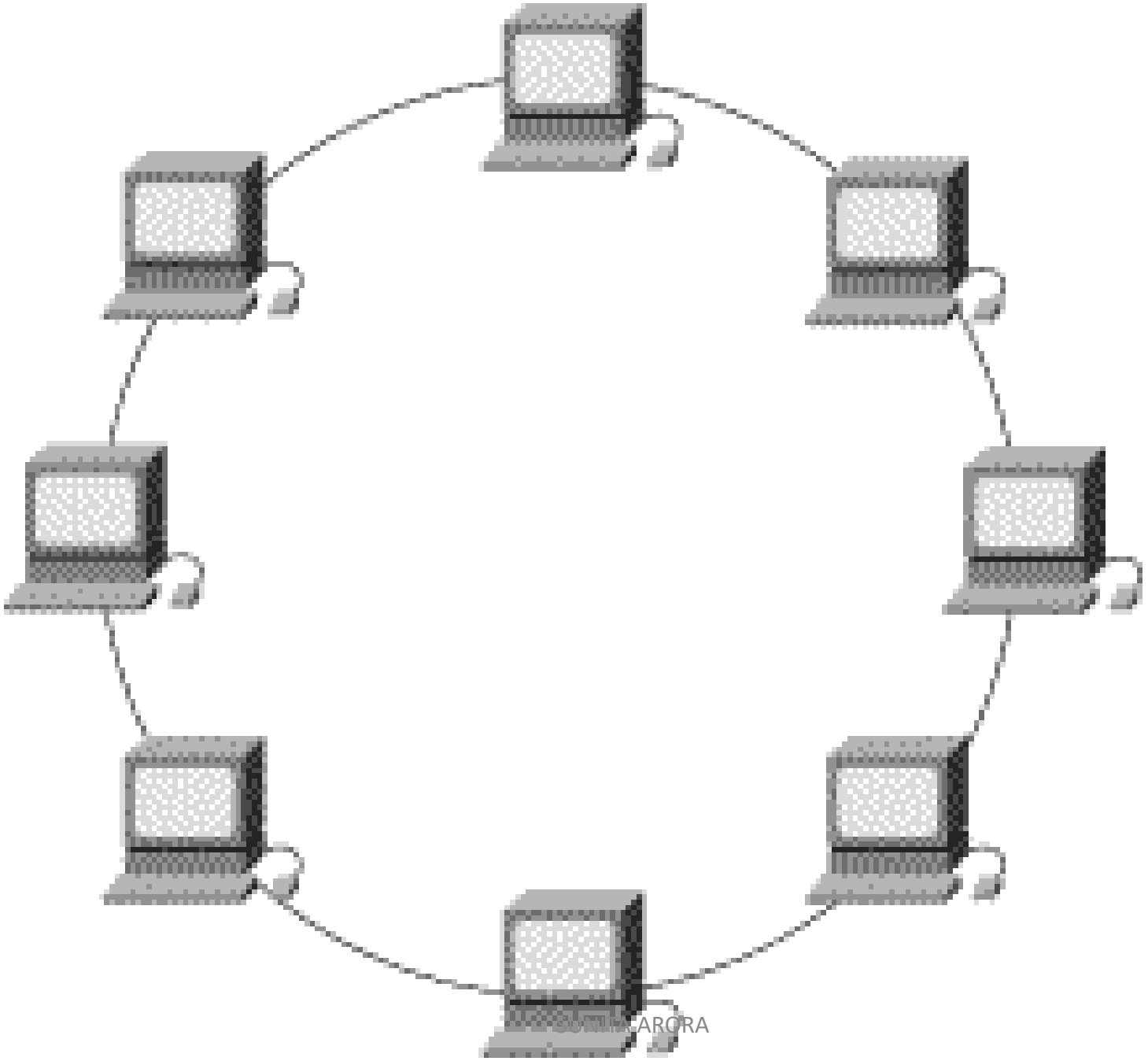
BUS Topology



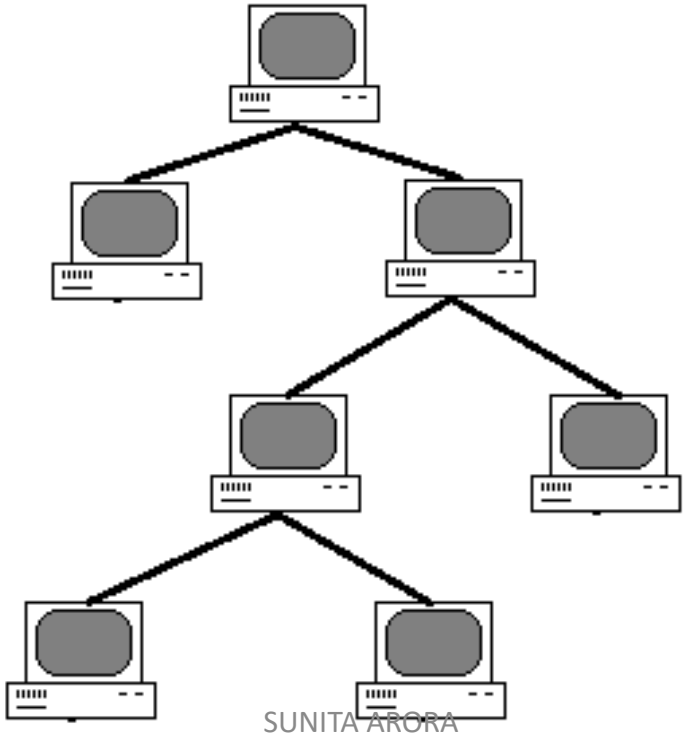
- **<u>The ring or circular topology:</u>**
- Each node is connected to two and only two neighbouring nodes.
- Data is accepted from one of the neighbouring nodes and is transmitted onwards to another.

- **Advantages:**
- **1. short cable length**
- **2. no wiring closet space required**
- **3. suitable for optical fibres**

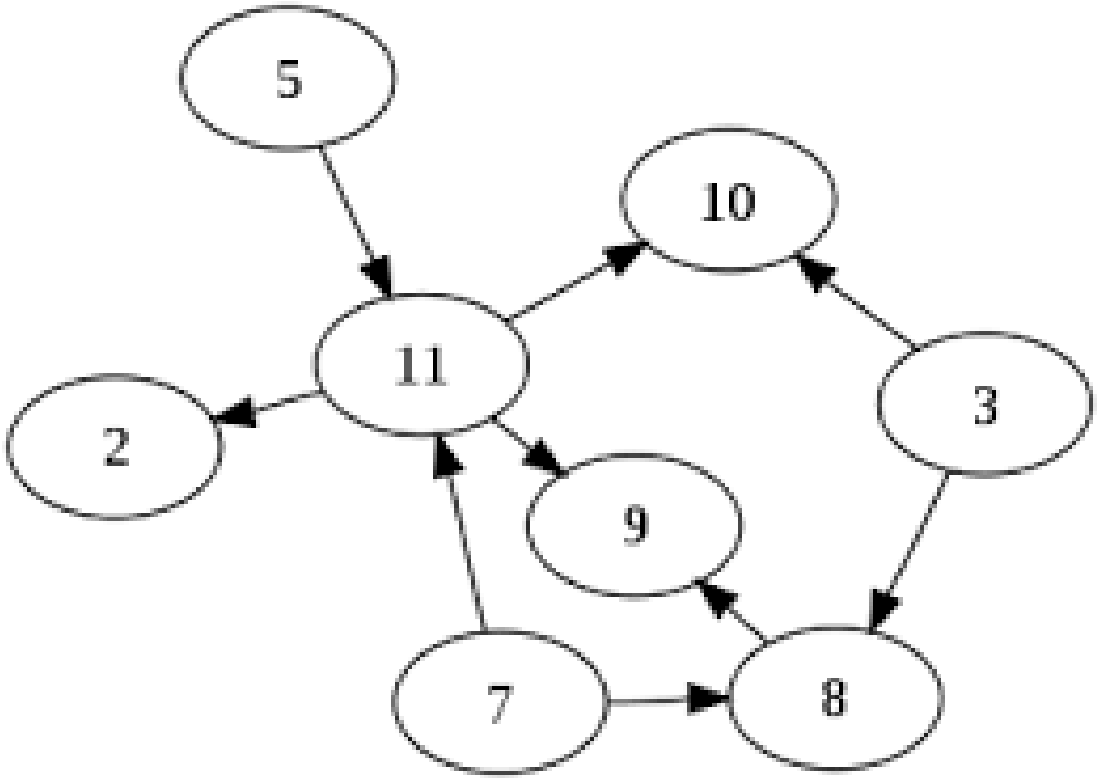
- **Disadvantages:**
- **1. node failure causes network failure**
- **2. difficult to diagnose faults**
- **3. Network reconfiguration is difficult**



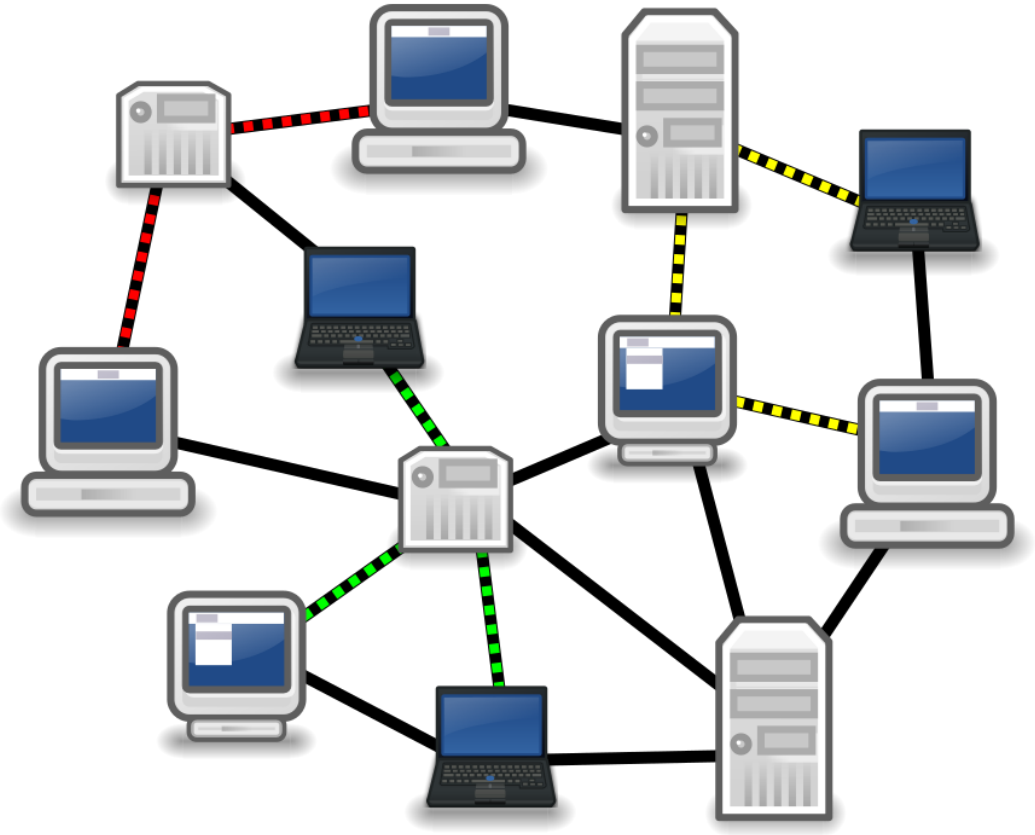
- **<u>Tree topology:</u>**
- Variation of bus topology is tree topology.
- The shape of the network is that of an inverted tree with the central root branching and sub-branching to the extremities of the network.
- Transmission in this topology takes place in the same way as in the bus topology



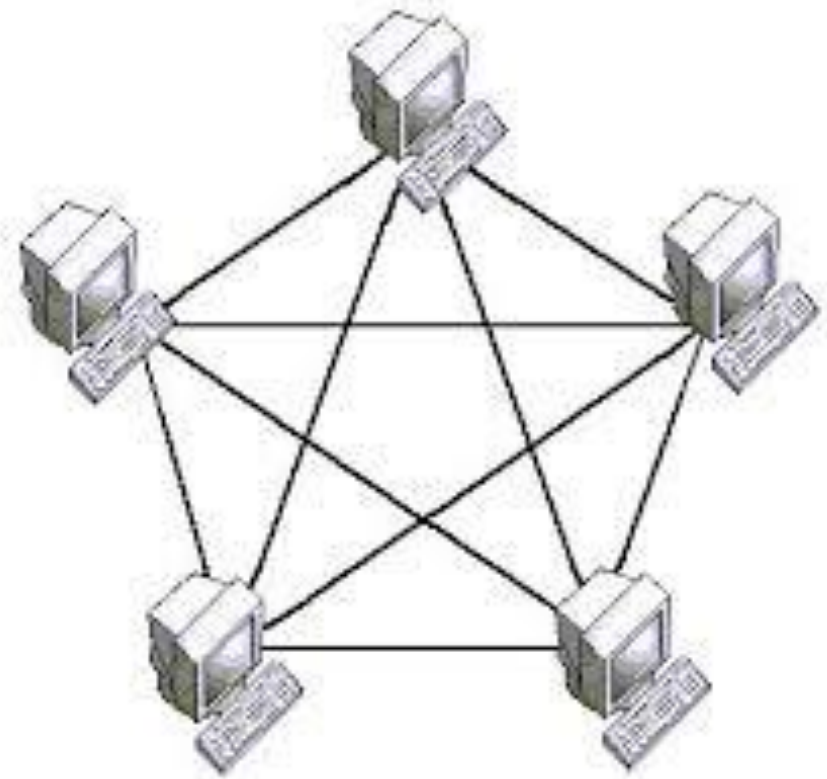
- **<u>Graph topology:</u>**
- Nodes are connected together in an arbitrary fashion.
- A link may or may not connect two or more nodes.



- **Mesh topology:**
- Each node is connected to more than one node to provide an alternative route in the case the host is either down or too busy.
- It is an extension to P-P network.

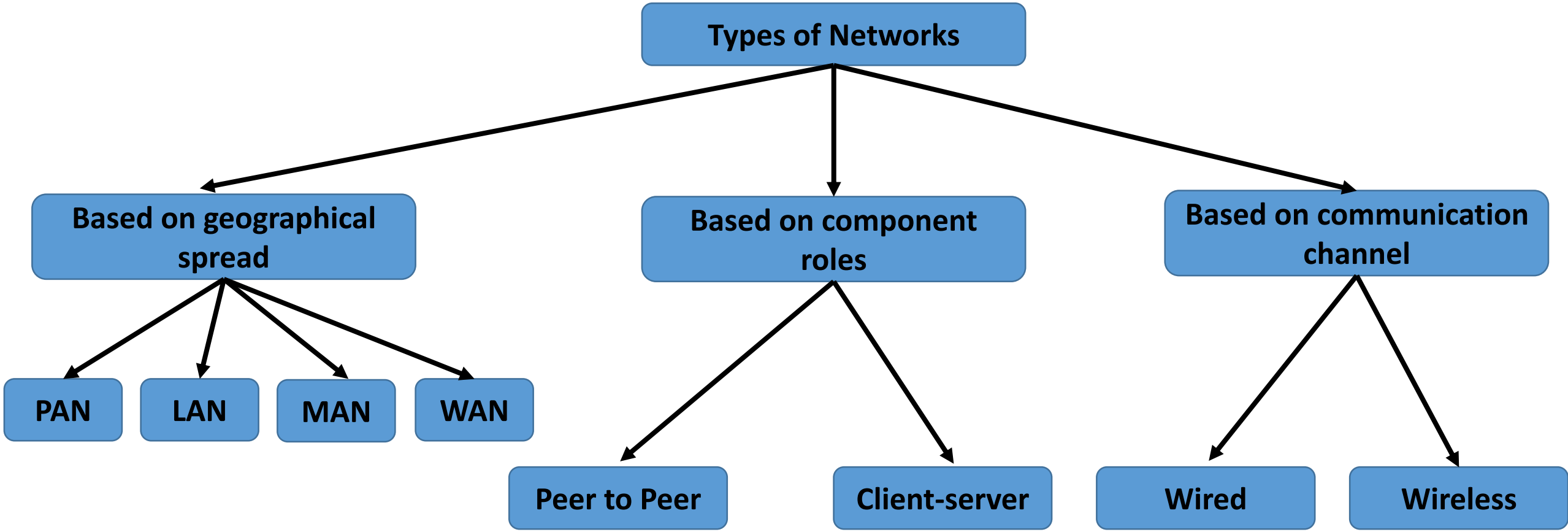


- **<u>Fully connected:</u>**
- When in a network each host is connected to other directly i.e there is a direct link between each host, then the network is said to be fully connected.

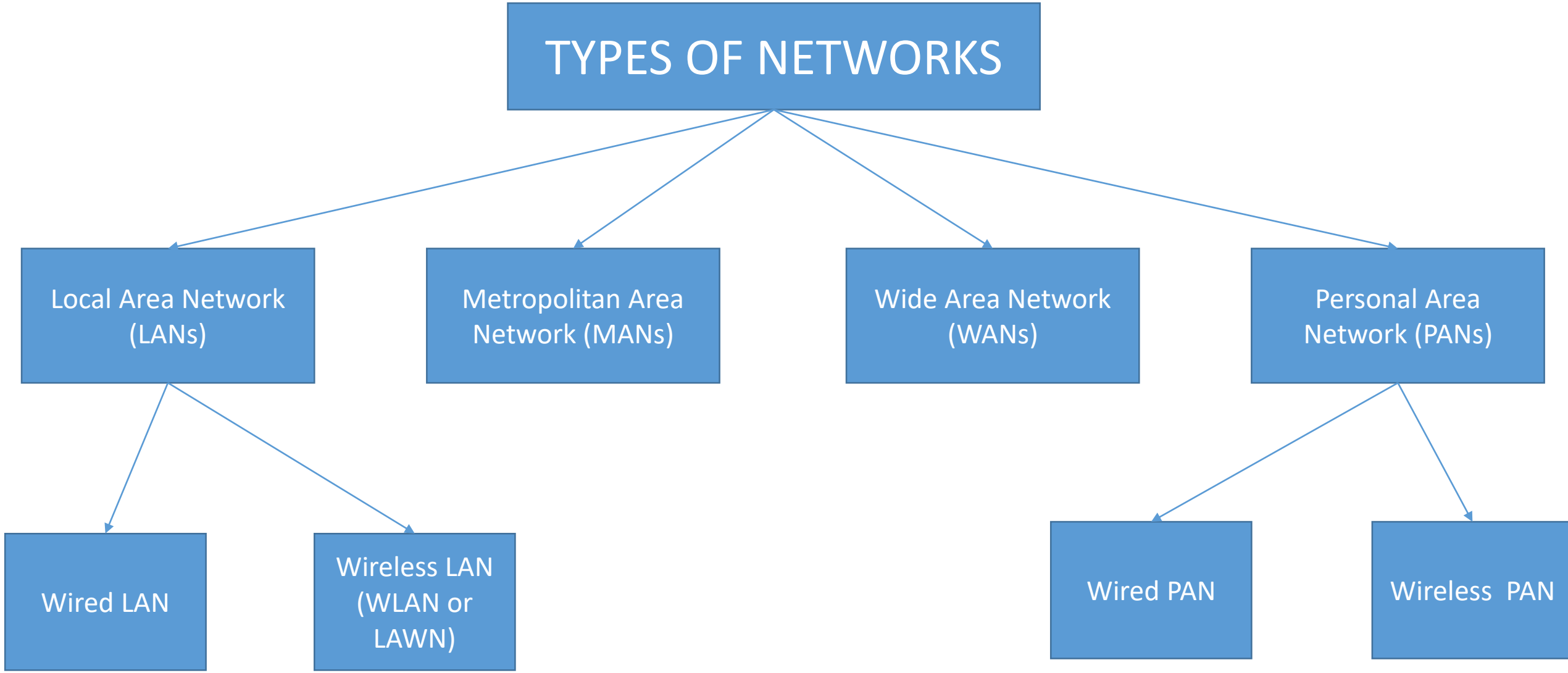


TYPES OF NETWORKS

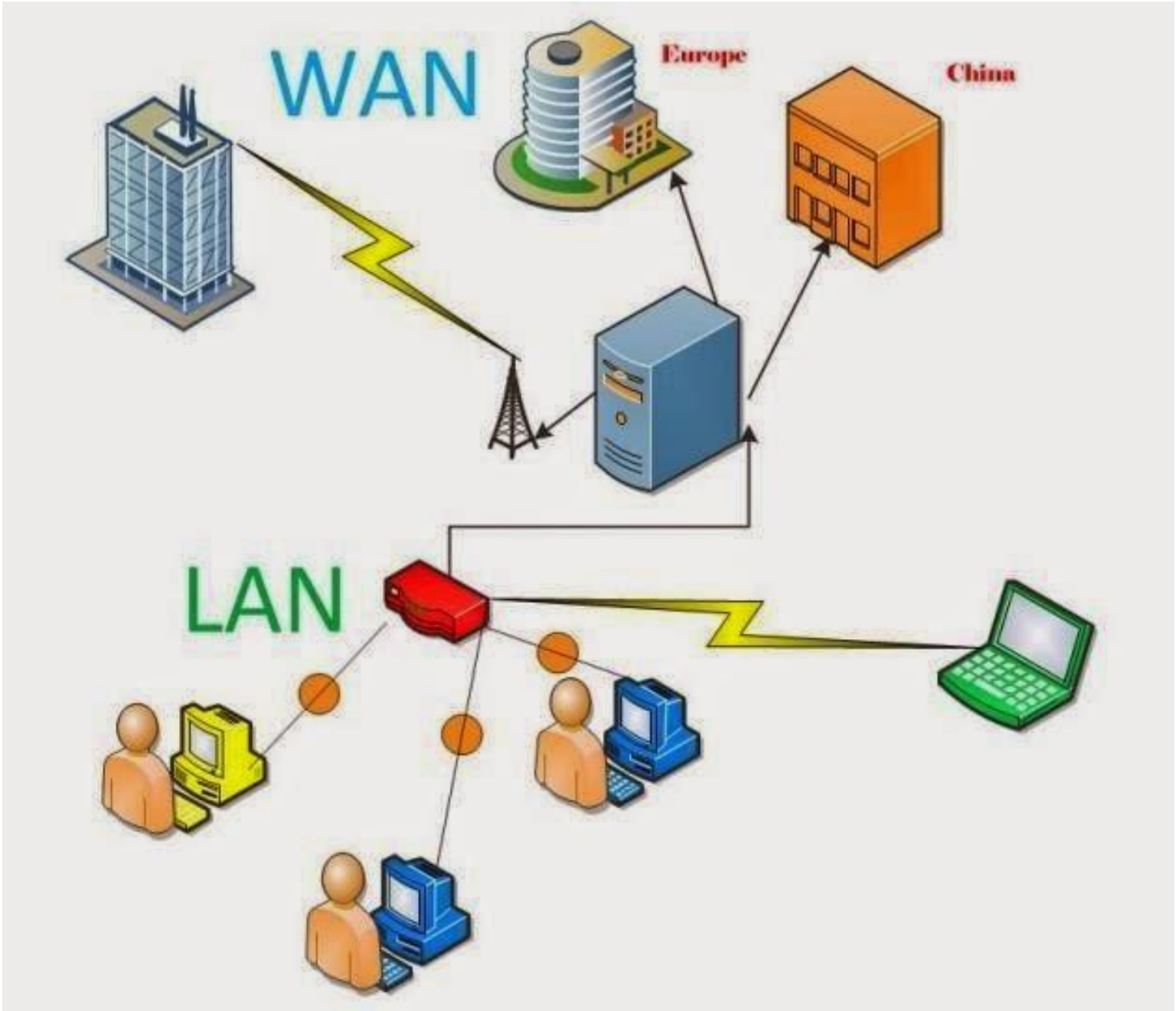
- Networks vary in size, complexity and geographical spread.



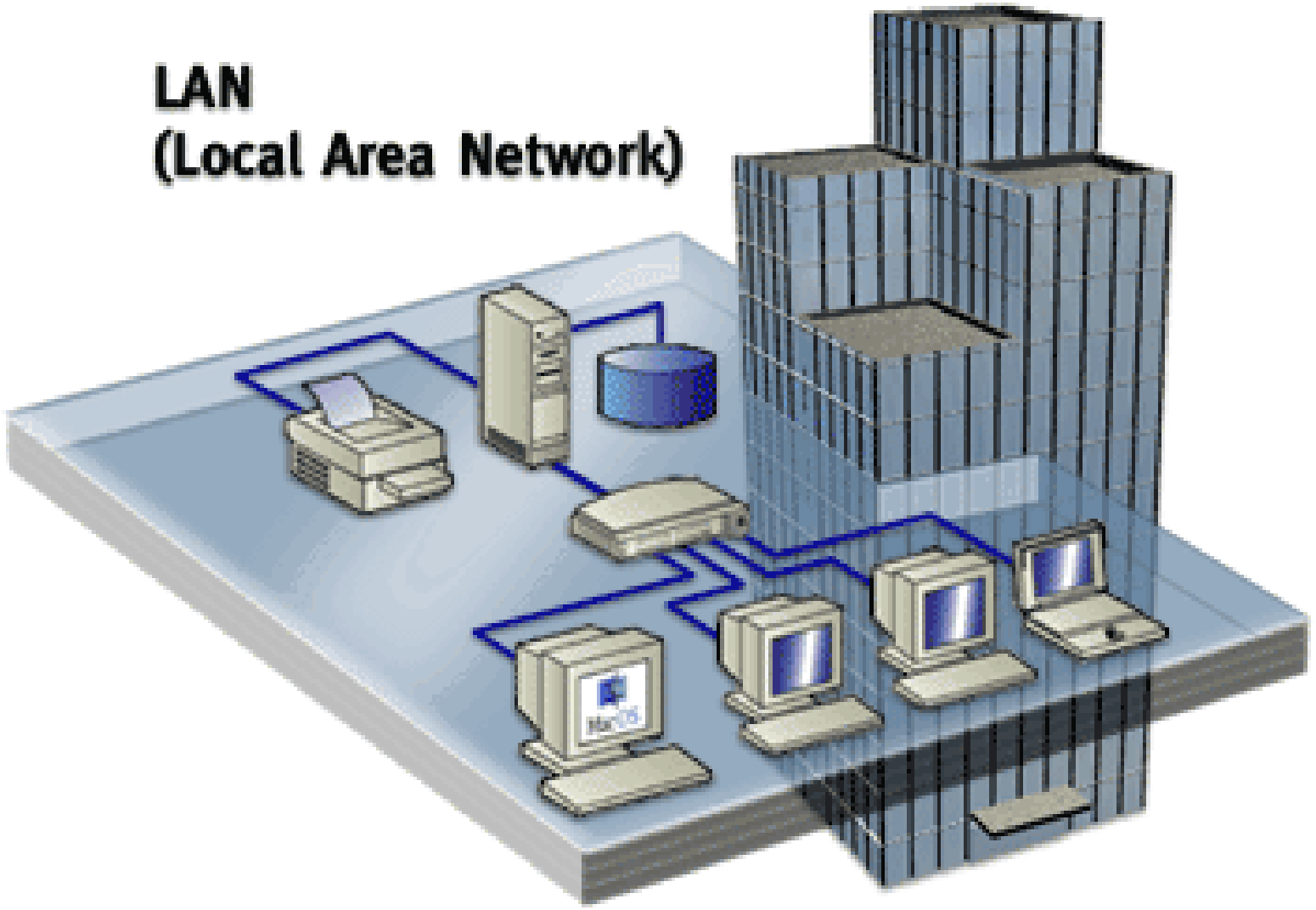
- **Types of Networks based on geographical spread:**
- 1. PAN (Personal Area Network)
- 2. LAN (Local Area Network)
- 3. MAN (Metropolitan Area Network)
- 4. WAN (Wide Area Network)

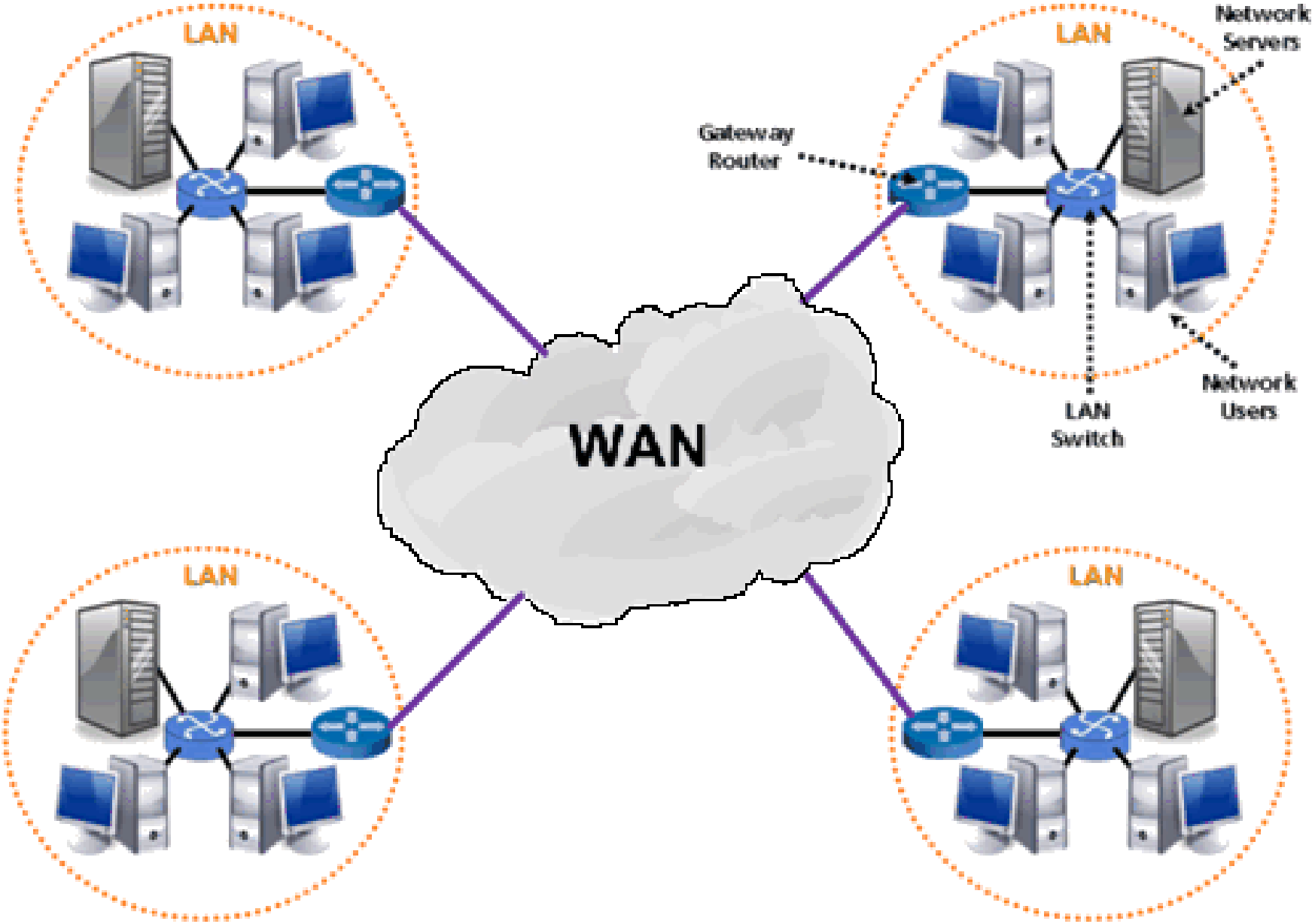

TYPES OF NETWORKS
Local Area Network (LANs)
Metropolitan Area Network (MANs)
Wide Area Network (WANs)
Personal Area Network (PANs)
Wired LAN
Wireless LAN (WLAN or LAWN)
Wired PAN
Wireless PAN


WAN
Wide Area Network
Reti geografiche
MAN
Metropolitan
Area Network
Reti metropolitane
LAN
Local Area Network
Reti locali


WAN
Europe
China
LAN

LAN
(Local Area Network)



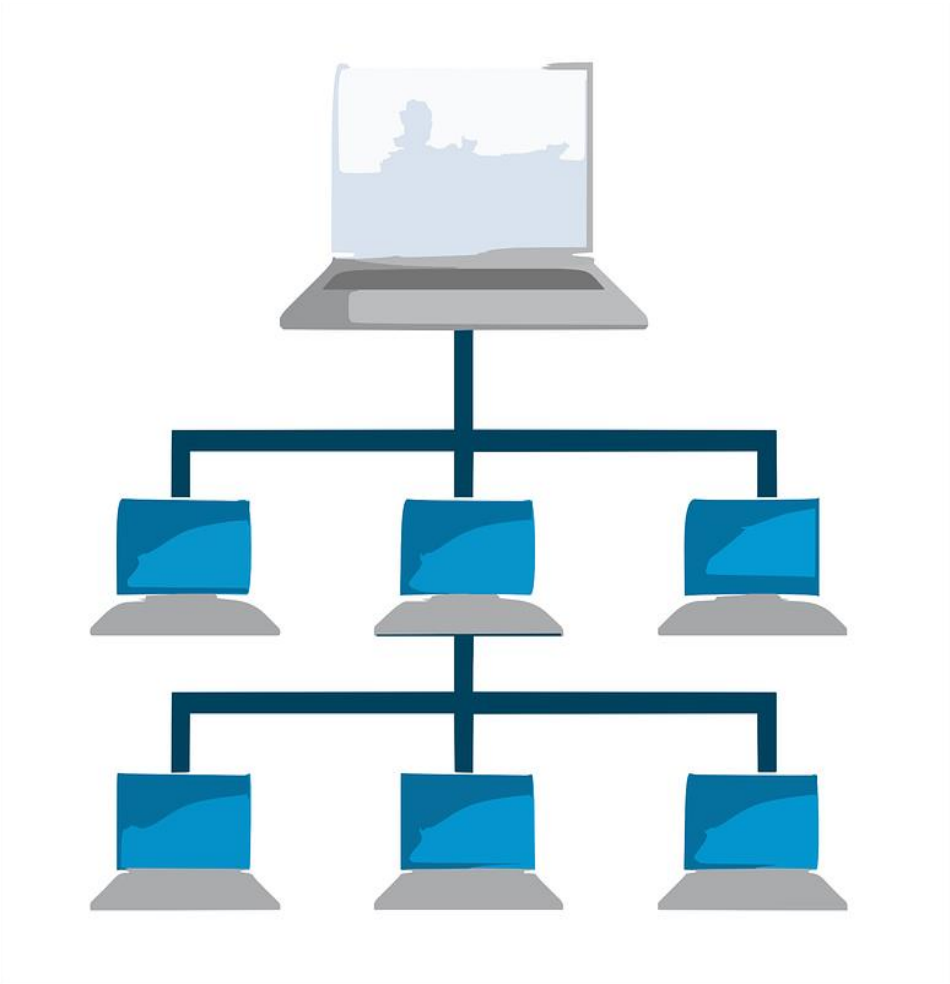

LAN
LAN
Network
Servers
Gateway
Router
WAN
LAN
Switch
Network
Users
LAN
LAN

Parameters	PAN	LAN	MAN	WAN
Full form	Personal area network	Local area network	Metropolitan area network	Wide area network
Meaning	small network of communication capable devices within a range of reachability of an individual person.	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example internet.
Area covered	Small area (upto 10m radius)	A few meters to a few kilometers (upto 10km radius)	A city and its vicinity (upto 100km)	Entire country, continent or globe (no upper limit)
Error rates	lowest	lowest	moderate	Highest
Transmission speed	High speed	High speed	Moderate speed	Low speed
Networking cost	negligible	inexpensive	Moderately expensive equipment	Expensive
Ownership of network	Private	Private	Private or public	Private or public
Design and maintenance	easy	easy	difficult	difficult
Propagation delay	Very short	short	moderate	long
Used for	personal	College, hospital, school	Small towns, cities	Country/continent

- **LAN:**
- Small computer networks that are confined to a localised area (e.g., an office, a building or a factory) are known as LAN.
- The key purpose of a LAN is to serve its users in resource sharing.
- The hardware as well as software resources are shared through LANs.
- For instance, LAN users can share data, information, programs, printers, hard-disks, modems etc.
- LANs are said to have geographical spread of upto 1km.
- In a typical LAN configuration, one computer is designated as the file server. It stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network.
- Computers connected to the server are called workstations.
- On most LANs, cables are used to connect the network interface cards in each computer.

- **MAN:**
- It refers to a network that is spread over an area as big as a city.
- **WAN:**
- The networks spread across countries or on a very big geographical area are known as WANs.
- A WAN is a group of computers that are separated by large distances and tied together.
- It can even be a group of LANs that are spread across several locations and connected together to look on big LAN.
- Computers connected to a WAN are often connected through public networks, such as the telephone system.
- Sometimes they can be connected through leases lines or satellites.
- A leased line is a permanent telephone connection between two points set up by a government-regulated organization that provides telecommunications services to the public.
- The largest WAN in existence is the Internet.

- **Types of networks based by component roles:**
- 1. Peer to Peer Networks
- 2. Client-Server Networks



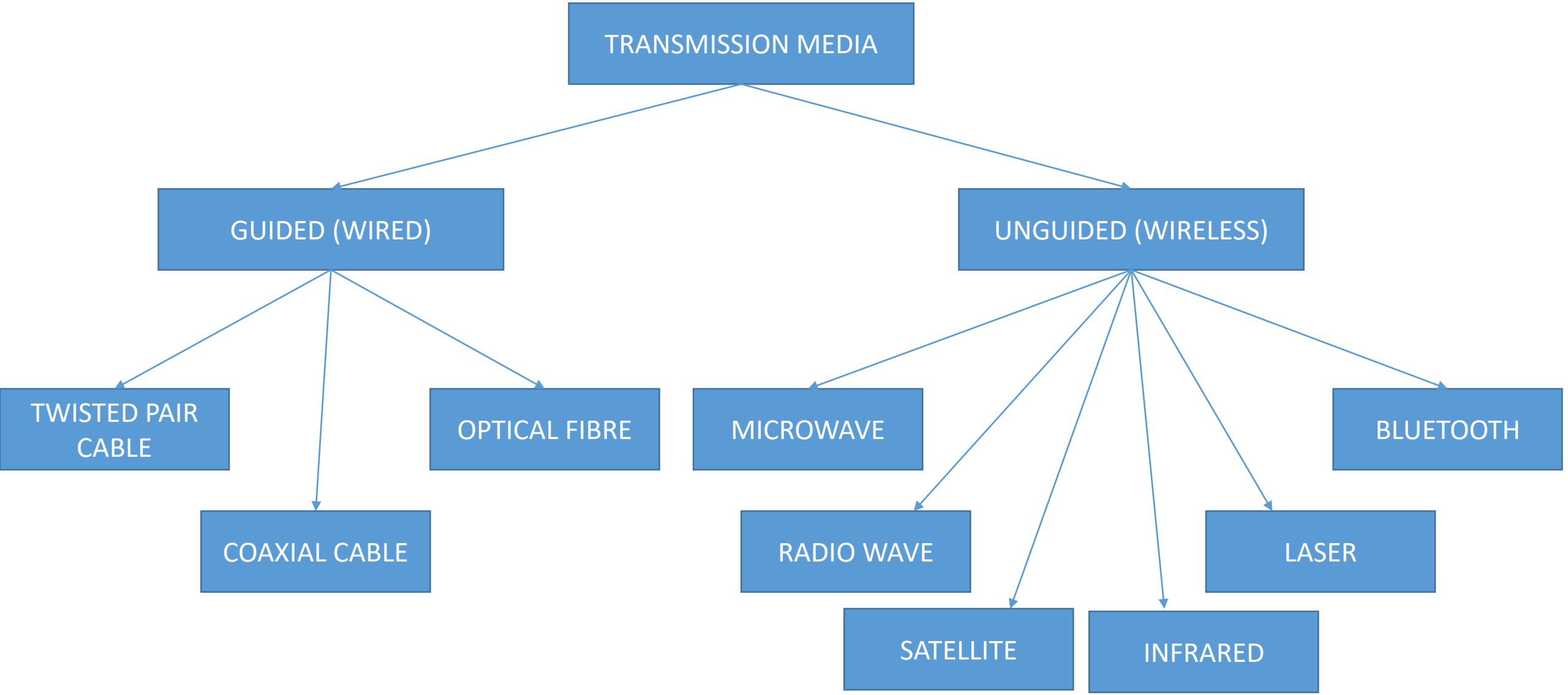
- **Peer to Peer Network:**
- Peer-to-Peer networks are popular as home networks and for use in small companies as they are inexpensive and easy to install, but they are limited in scope and are difficult to secure.
- Each computer on a Peer to Peer (P2P) network is equal.
- Each computer can play the role of a client or a server.
- There is no computer designated as in charge of network operation.
- The computers that serves on a peer-to-peer are often termed as non-dedicated servers.
- On small networks, a workstation that can double up as a server, is known as non-dedicated server since it is not completely dedicated to the cause of serving.
- Such servers can facilitate the resource-sharing among workstations on a proportionately smaller scale.
- Since one computer works as a workstation as well as a server, it is slower and required more memory.
- A Peer-to-Peer network has up to ten computers.

- **Client-Server Network:**
- Bigger networks prefer to have centralized control.
- They do this by clearly designating servers and clients.
- Such networks are called client-server networks or even master-slave networks.
- On bigger network installations, there is a computer reserved for the server's job and its only job is to help workstations access data, software and hardware resources.
- It does not double-up as a workstation and such a server is known as dedicated server.
- The networks using such a server are known as master-slave networks.
- In a client-server model the client is dependent of the server to provide and manage the information.
- For example, websites are stored on web servers.
- A web browser is the client which makes a request to the server, and the server sends the website to the browser

- On a network, there may be several servers that allow workstations to share specific resources. For example, there may be a server exclusively for serving files-related requests like storing files, deciding about their access privileges and regulating the amount of space allowed for each user. This server is known as file server. Similarly, there may be printer server and modem server. The printer server takes care of the printing requirements of a number of workstations and the modem server helps a group of network users use a modem to transmit long distance messages.
- A dedicated server operates solely as a server on a network while a non-dedicated server can shuttle between the client as well as server roles.

Client-Server	Peer-to-Peer
The server controls security of the network.	No central control over security.
The server manages the network. Needs a dedicated team of people to manage the server.	No central control over the network. Anyone can set up.
Clients are dependent on the server.	Clients are not dependent on a central server.
The server can be upgraded to be made more powerful to cope with high demand.	If machines on a network are slow they will slow down other machines.
Data is all backed up on the main server.	Each computer has to be backed up. Data can be deleted by users.

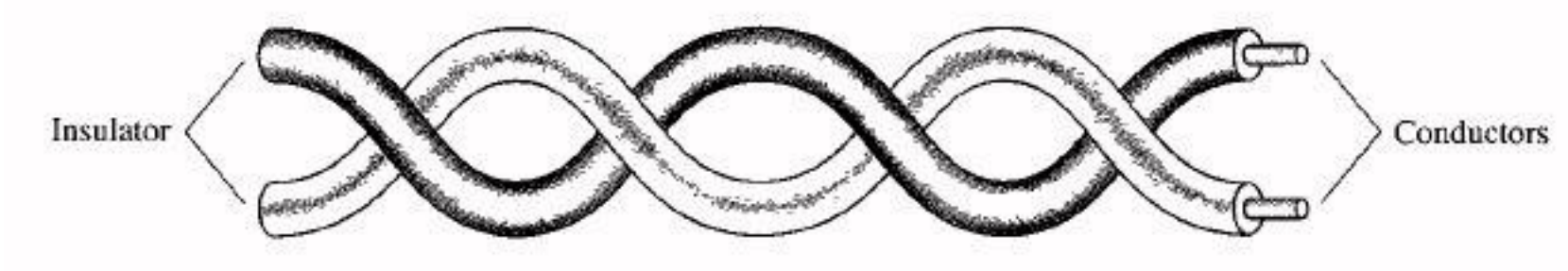
- **Types of networks based on communication channel:**
- 1. Wired Computer Networks.
- 2. Wireless Computer Networks.

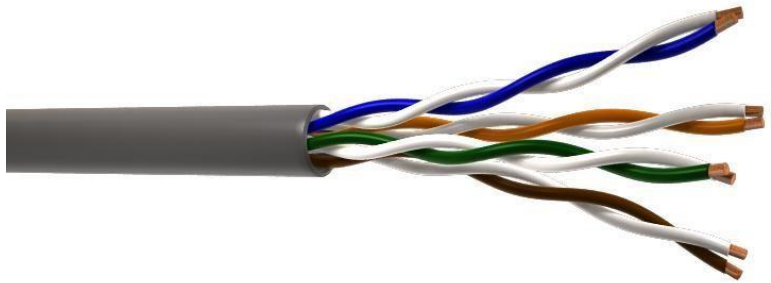

TRANSMISSION MEDIA
GUIDED (WIRED)
UNGUIDED (WIRELESS)
TWISTED PAIR CABLE
COAXIAL CABLE
OPTICAL FIBRE
MICROWAVE
RADIO WAVE
SATELLITE
INFRARED
LASER
BLUETOOTH

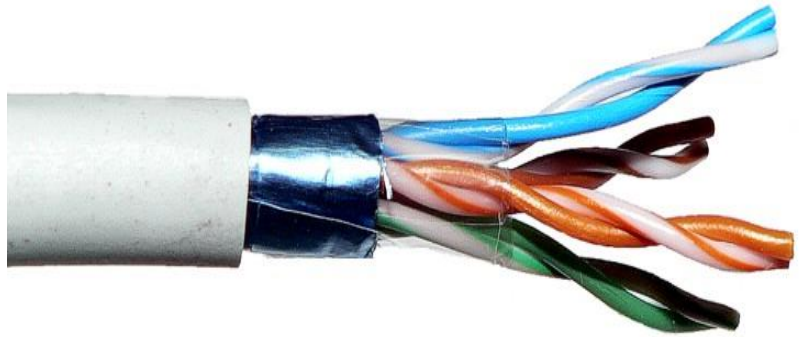
- **Wired Computer Network:**
- In wired computer networks, the hosts and other devices are interconnected through wiring or cables.
- Most wired computer networks are of LAN type.
- Most commonly used cables in wired networks are:
- **A. Twisted pair cable**
- **B. Coaxial Cable (Coax)**
- **C. Fibre Optic Cable (optic fibre)**

- **<u>Twisted pair cable:</u>**
- A twisted pair cable is a pair of insulated wires that are twisted together to improve electromagnetic capability and to reduce noise from outside sources.
- These are available in various forms such as CAT1, CAT2, CAT3, CAT4, CAT5, CAT6.
- It consists of two identical wires wrapped together in a double helix.
- A special type of twisted pair cable known as CAT5 or CAT6 is mostly used in a specific type of LAN namely Ethernet, hence it is known as Ethernet cable.
- The twisting of wires reduces crosstalk. Forms of signal interference is called crosstalk.
- **Advantages:**
- **1. it is simple.**
- **2. Physically flexible.**
- **3. can be easily connected.**
- **4. easy to install and maintain.**
- **5. Has low weight.**
- **6. Very inexpensive.**

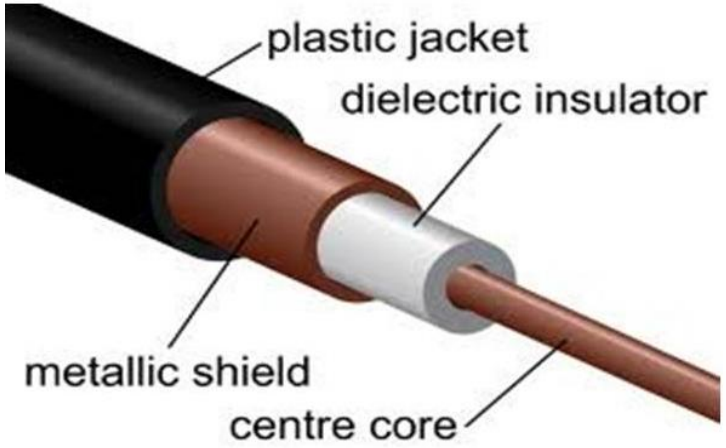
- **Disadvantages:**
- 1. because of high attenuation, it is not capable of carrying a signal over long distances without use of repeaters.
- 2. its low bandwidth capabilities make it unsuitable for broadband applications.

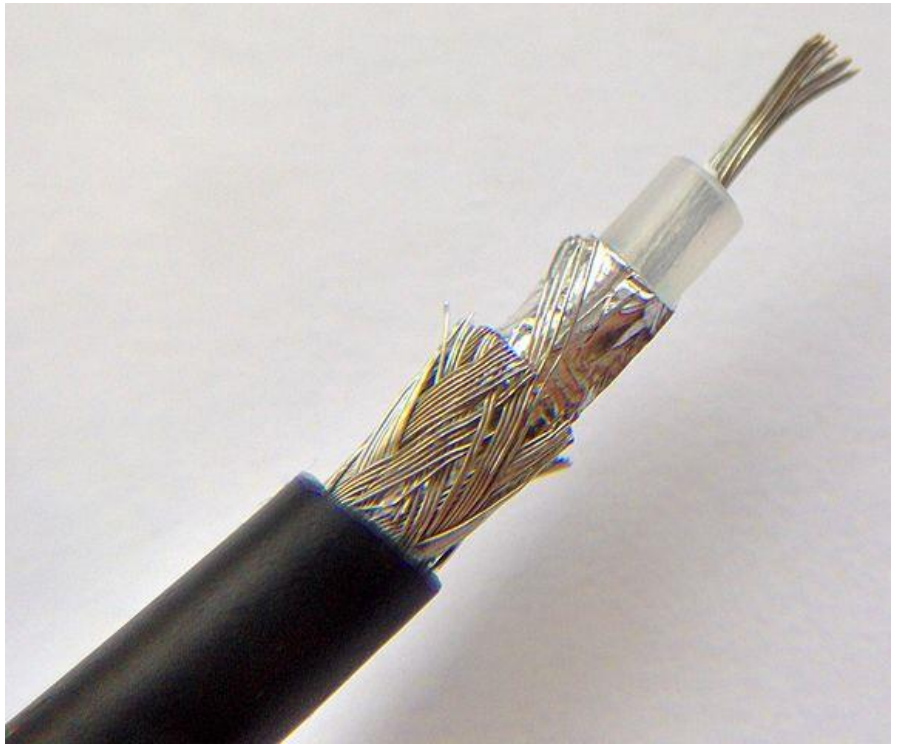




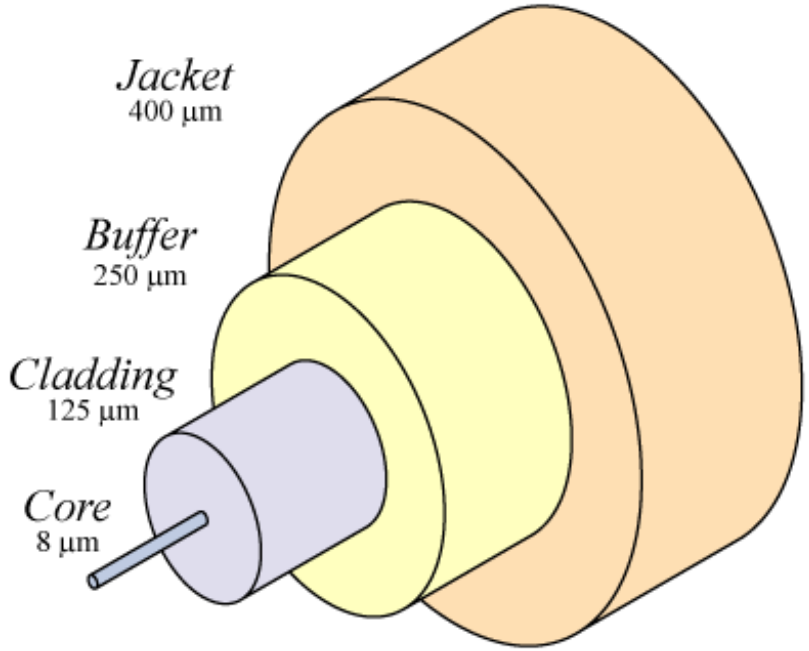


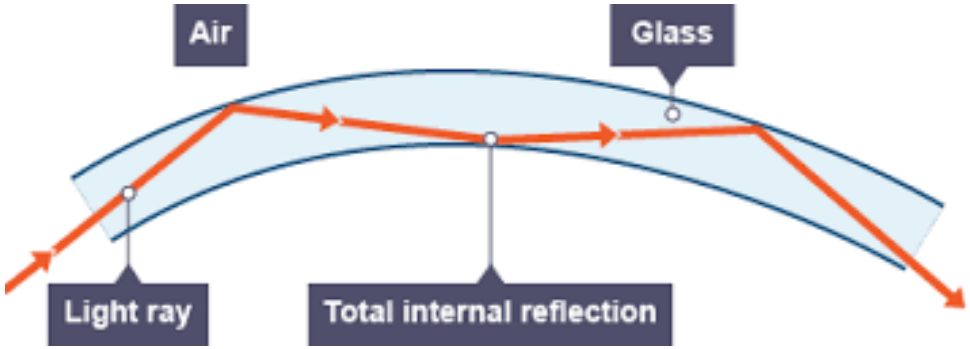
- **Coaxial cable:**
- This type of cable consists of a solid wire core surrounded by one or more foil or wire shields, each separated by some kind of plastic insulator.
- The two most commonly used types of coaxial cables are thicknet and thinnet.
- Consists of a solid wire core surrounded by one or more foil or wire shields, separated by some kind of plastic insulator.
- The inner core carries the signal, and the shield provides the ground.
- Widely used for television signals.
- **Advantages:**
- The data transmission characteristics are better than twisted pair.
- Used for broadband transmission
- Offer higher bandwidth upto 400 MBPS.
- **Disadvantages:**
- Expensive compared to twisted pair cable.
- Not compatible with twisted pair cable





- **Optical fibres:**
- A fibre optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves. Common types of optic cables are single node and multi node.
- Consists of thin stands of glass or glass like material which are so constructed that they carry light from a source at one end of the fibre to a detector at the other end.
- The fibre cable consists of three pieces:
- 1. the **core**. Ie. The glass or plastic through which the light travels.
- 2.The **cladding** which Is a covering of the core that reflects light back to the core.
- 3. **protective coating**, which protects the fibre cable from hostile environment.

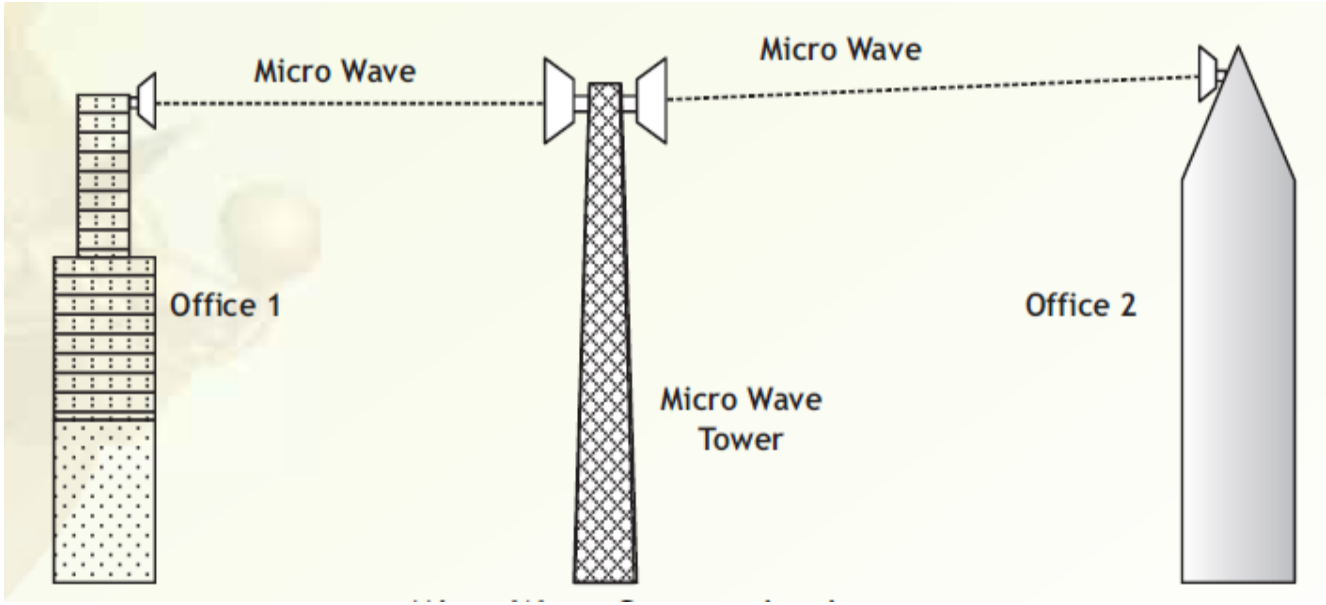


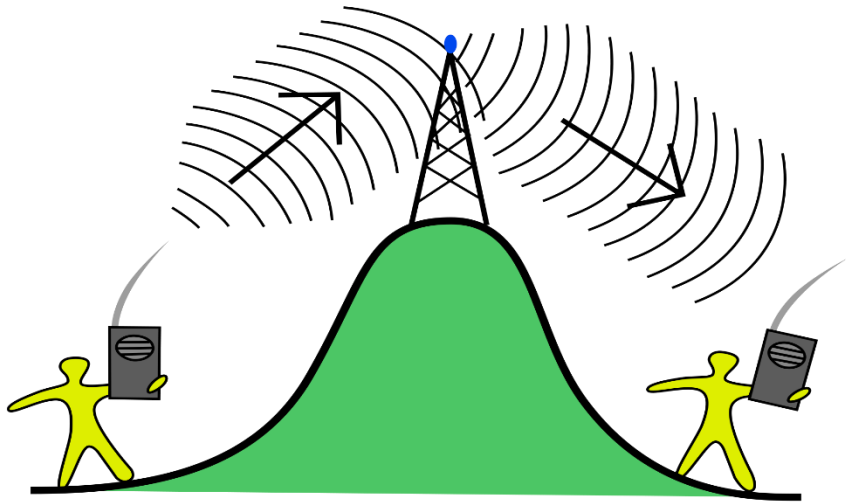


- **Advantages:**
- Immune to electrical and magnetic interference.
- Highly suitable for harsh industrial environments.
- Guarantees secure transmission and has a very high transmission capacity.
- Can be used for broadband transmission.
- **Disadvantages:**
- Installation problems.
- Connecting either two fibres together is a difficult process.
- Because of high immunity, impossible to tap.
- Light can reach receiver out of phase.
- Fibre optic cables are more difficult to solder.
- They are the most expensive of all the cables.

Factors	Twisted Pair Cable	Coaxial Cable	Optical Fiber Cable
Data Transfer Rate	10Mbps-10 Gbps	100 Mbps	> 100 Gbps
Distance (range)	100 mt.	185-500 mt.	>10 Km.
EMI susceptibility	More	Less	Nil
Cost	Least cost	More than Twisted Pair	Very expensive

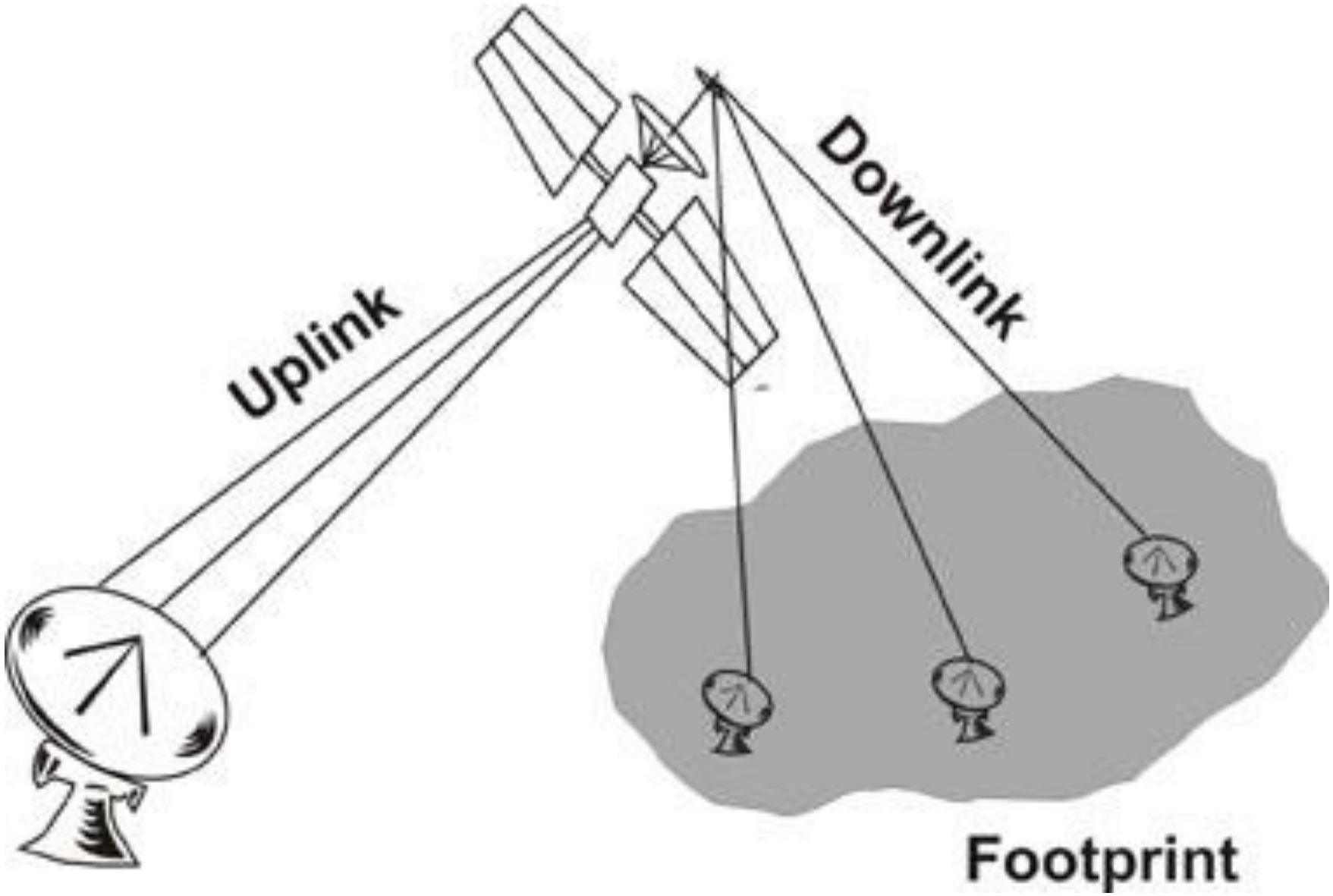
- **Wireless computer networks:**
- The computer networks that use environment or air as the media, through which information is transmitted without requiring any cable or wires or other electronic conductors, rather by using electromagnetic waves like IR (Infrared) , RF (Radio Frequency), satellite etc are wireless computer networks.
- Most commonly used transmission media are:
- **A. Microwave:** Microwave waves are high frequency waves that can be used to transmit data wirelessly over long distances. The microwave transmission consists of a transmitter, receiver and the atmosphere. Microwave radiation can be used to transmit signals such as mobile phone calls. When the frequency is higher that 3 GHz, it is named microwave.
- **B. Radiowaves:** Radio waves can be classified by frequency and wavelength. Radio waves are used to transmit television and radio programmes. All radios today, use continuous sine waves to transmit information (audio, video, data). WiFi that has become a common word today also used radio wave to transmit data among connected devices.


Micro Wave
Micro Wave
Office 1
Office 2
Micro Wave
Tower



- **C. Satellite (Satellite Microwave):** Satellite communication is a special case of microwave relay system.
- Satellite communication is the synchronous satellite to relay the radio signal transmitted from ground station.
- A number of communication satellite, owned by both governments and private organizations, have been placed in stationary orbits about 22,300 miles above the earth's surface.
- These satellites act as relay stations for communication signals.
- The satellites accept data/signals transmitted from an earth station, amplify them, and retransmit them to another earth station.
- Using such a setup, data can be transmitted to the other side of the earth in only one step.

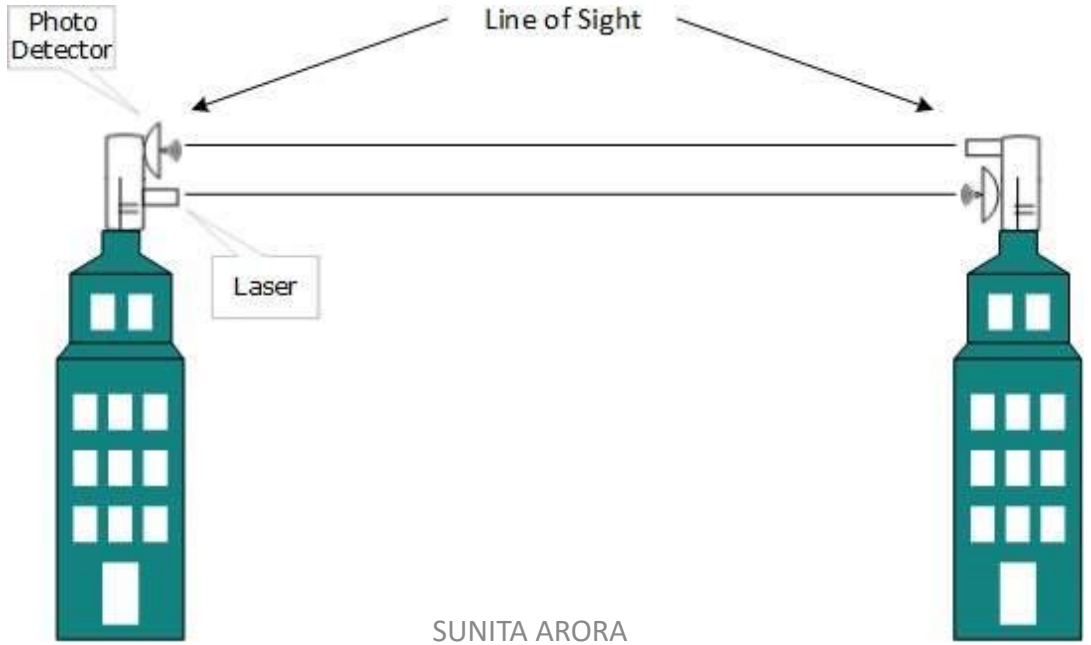
- Other wireless communication media are infrared, laser, Bluetooth.


Uplink
Downlink
Footprint


Satelliet op de Clarke Belt
transponders
14 GHz
uplink
12 GHz
downlink
grondstation
TV STUDIO

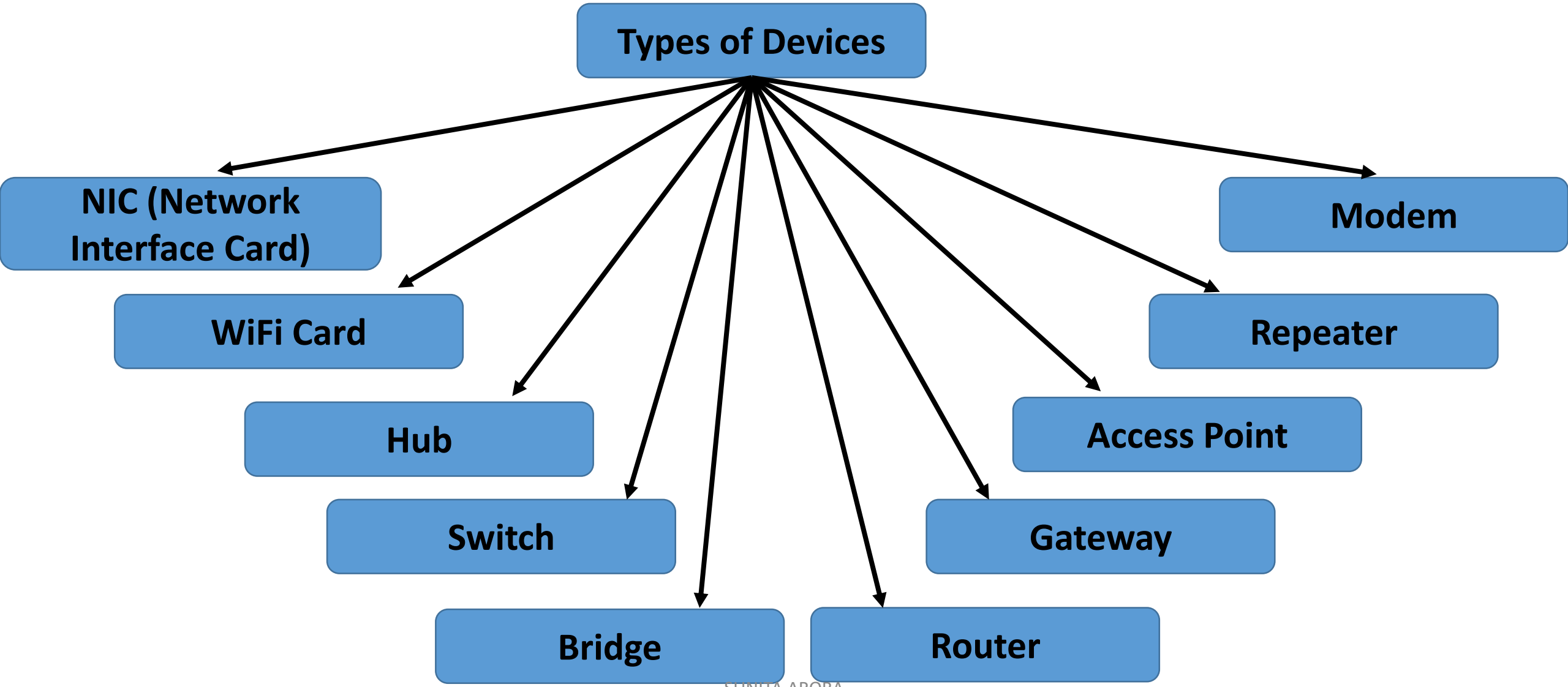
- **<u>Other unguided media:</u>**
- **Infrared:**
- Have a frequency range of 300Ghz to 400Thz.
- Used for short range communication (5m) in a variety of wireless communication.
- Example: Home entertainment remote-control device, cordless mouse.
- It is a line-of-sight transmission, therefore information is passed to one device is not leaked to another device and at a time only two devices can communicate.
- No government licence is required for their use.
- The waves do not cross any solid object in between.
- Performance drops with longer distances.

- **Laser:**
- requires direct line of sight.
- Unidirectional like microwave, but higher speed.
- Requires use of a laser transmitter and a photo sensitive receiver at each end.
- It is point to point transmission.
- Between buildings.
- It can be adversely affected by weather.

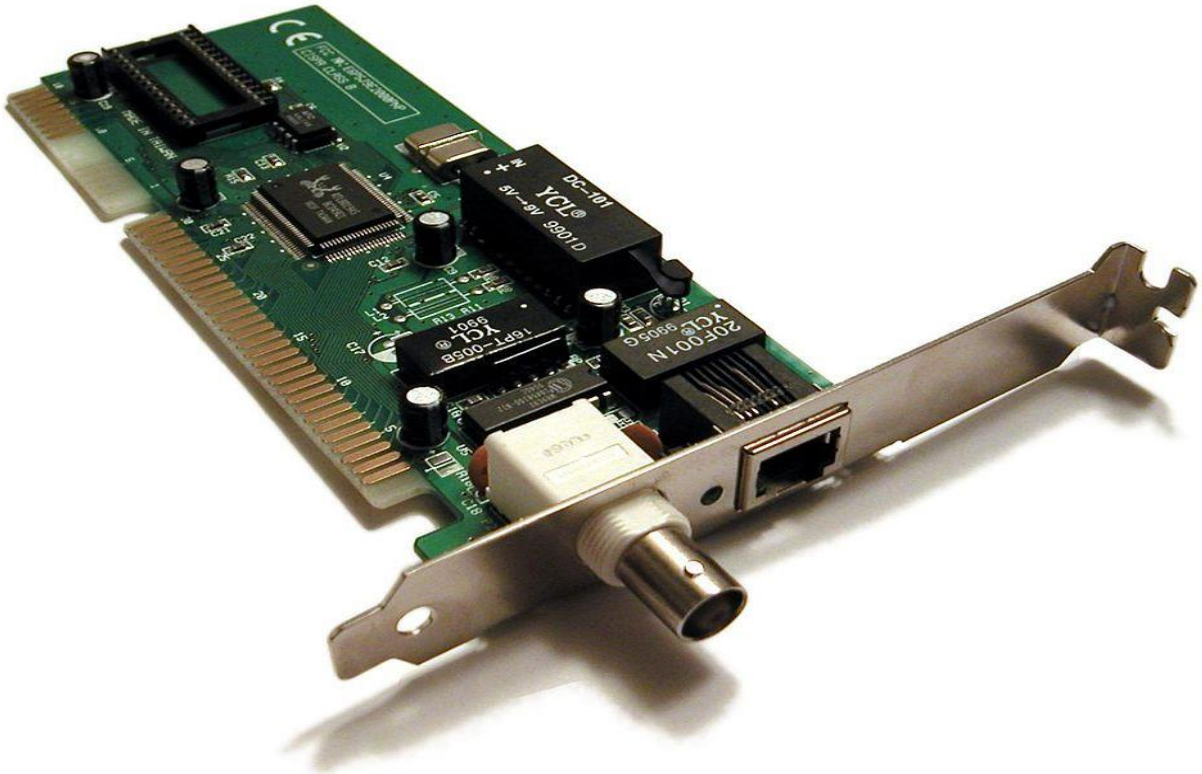


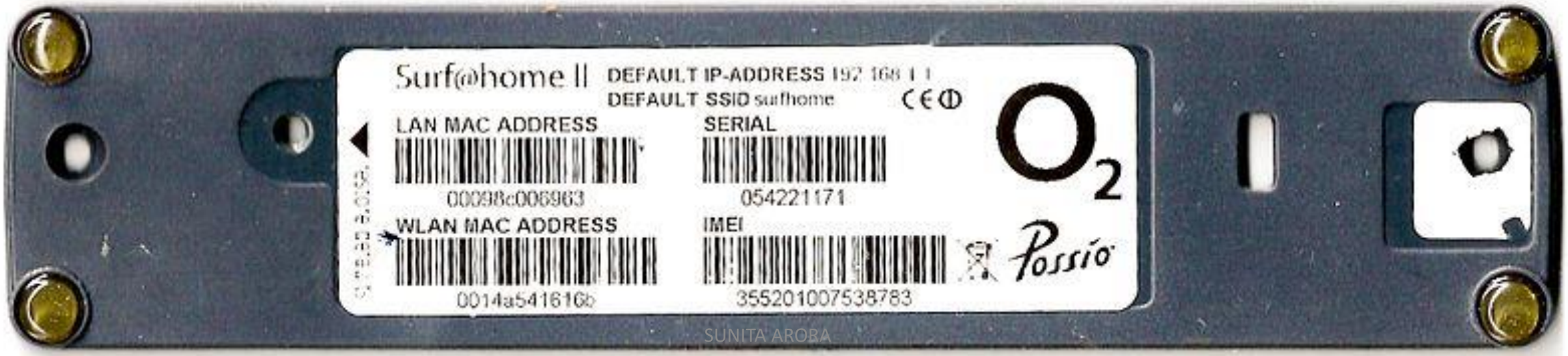
- **Bluetooth:**
- Named after *harald Bluetooth,* king of Denmark.
- Uses radio waves in the frequency range of 2.402 GHz to 2.580GHz.
- Used for short range communication (10m) in a variety of devices for wireless communication.
- Example: Baby monitors, door openers, and cell phones.
- Max range is 10 meters.
- Line of sight between communicating devices is not required.
- Bluetooth can connect upto 8 devices simultaneously.
- Wi-Fi (Wireless Fidelity) communication is similar to Bluetooth in operation but covers a large range of coverage (50-200 mts).

NETWORK DEVICES/HARDWARE



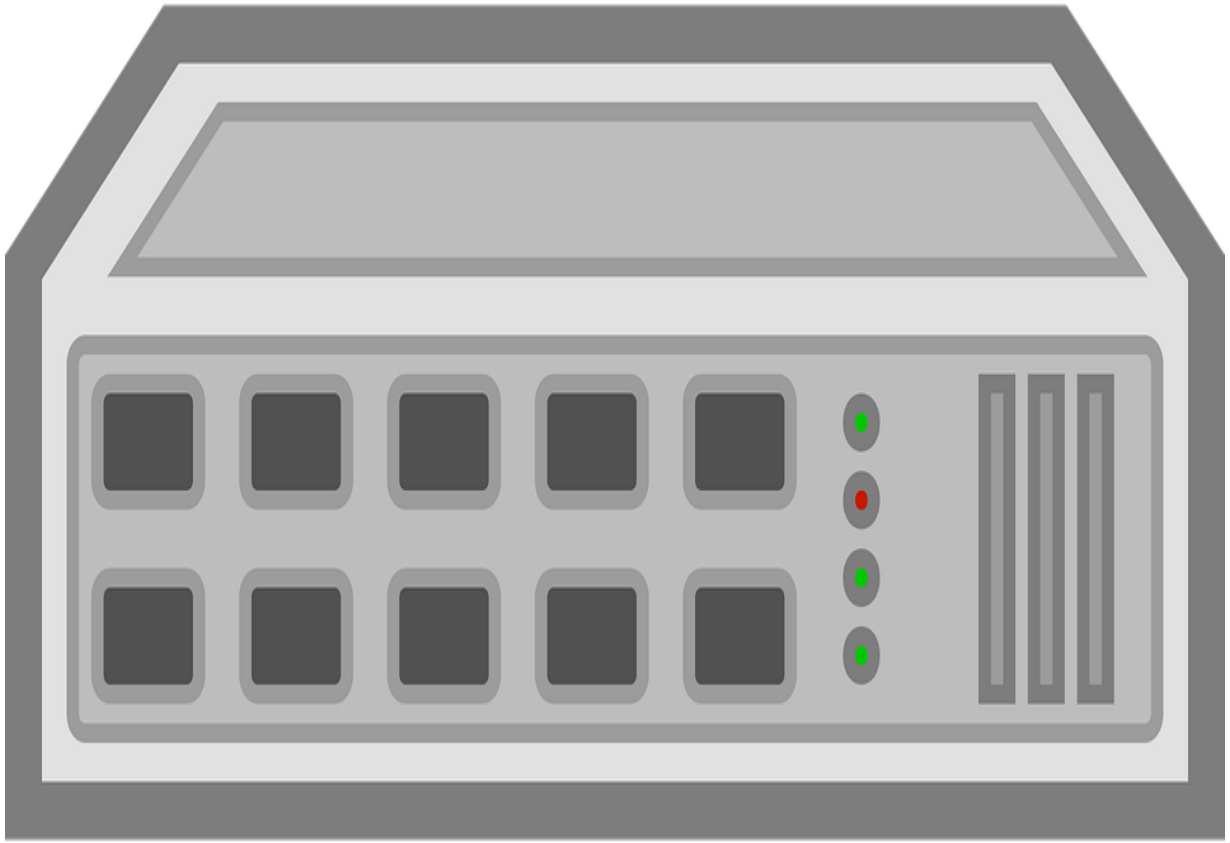
- **1. NIC (Network Interface Card):**
- The NIC is a device that is attached to each of the workstations and the server, and helps the workstation establish all the important connection with the network.
- Each NIC that is attached to a workstation has a unique number identifying it, which is known as the node address.
- The NIC is also called Terminal Access Point (TAP) or Network Interface Unit (NIU).
- The NIC manufacturers assigns a unique physical address to each NIC card, this physical address is known as MAC address (Media Access Control).
- A MAC address is a 6-byte address with each byte separated by a colon e.g., a sample MAC address could be: 10:B5:03:63:2E:FC
- This MAC address is actually the number assigned to the NIC of your computer.
- The first three bytes of MAC address are the manufacturer-id (assigned to the manufacturer by an international organization namely IEEE) and the last three bytes are the card-no (assigned by manufacturer).

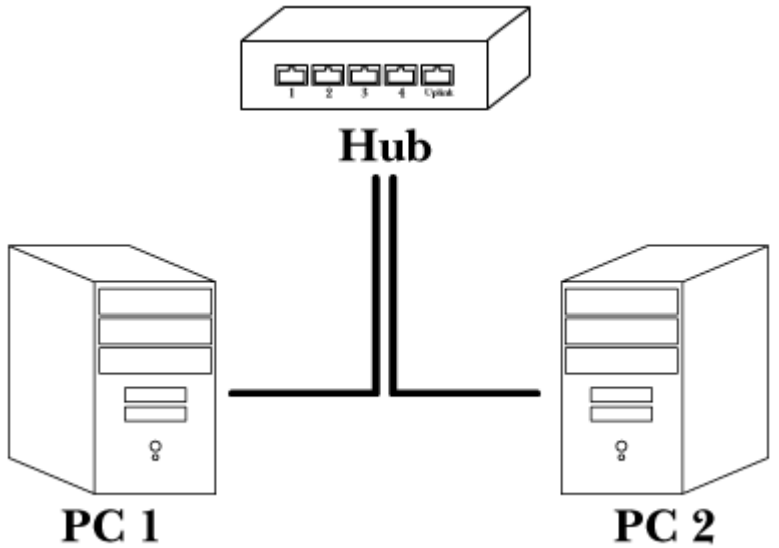




- **2. WiFi card:**
- A WiFi (Wireless Fidelity) card is either an internal or external Local Area Network adapter with a built-in wireless radio and antenna.
- The most common WiFi cards are used in desktop computers and PCI-Express WiFi cards made to fit the PCI-Express card slots on the motherboard.
- The benefit of using a WiFi card in a desktop computer is that it allows you to setup your workstation or home office without considering the proximity or availability of hard line network access.

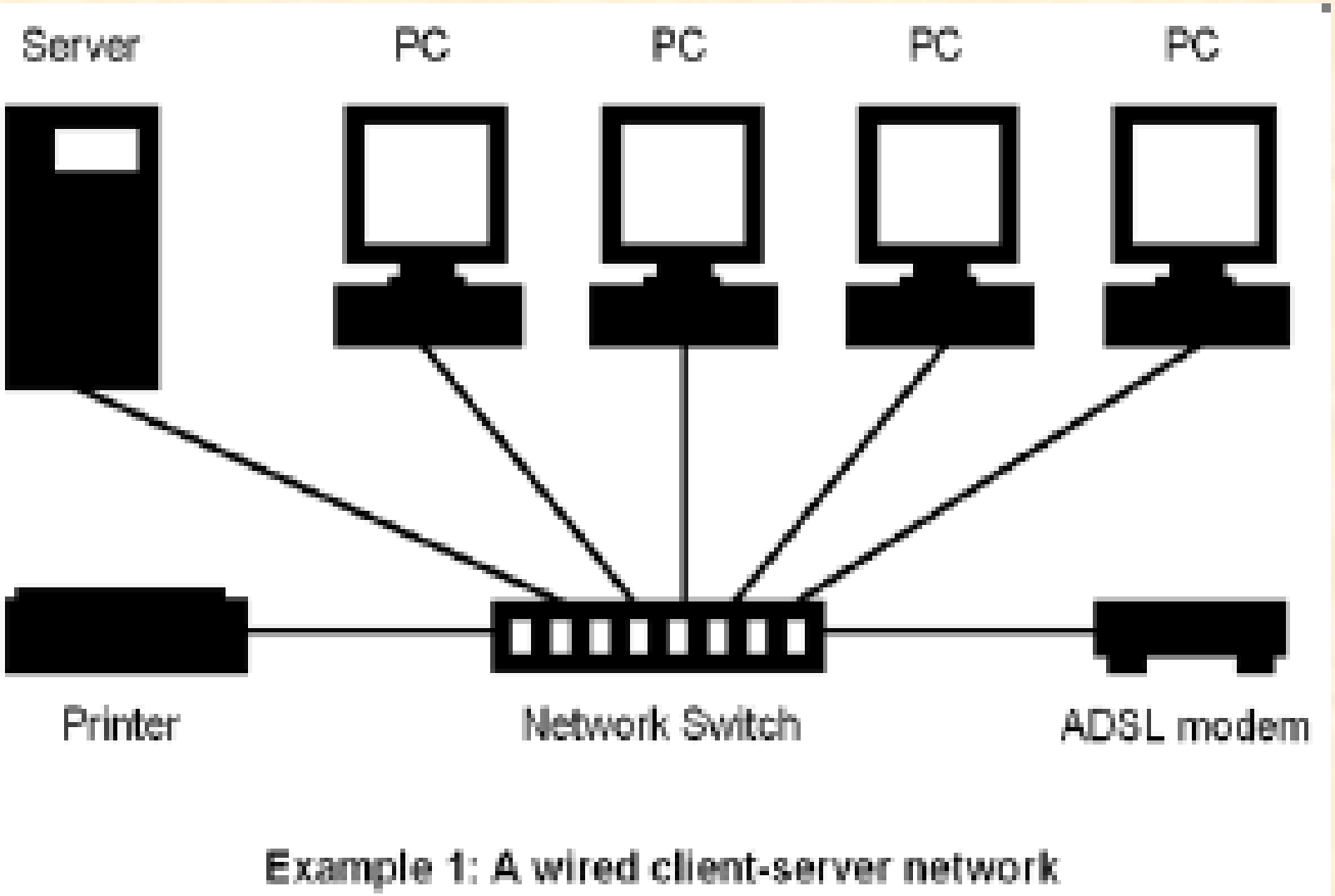
- **3. Hub:**
- A hub is networking device having multiple ports that are used for connecting multiple computers or segments of a LAN together.
- A hub is a hardware device used to connect several computers together.
- Hubs are multi-slot concentrators into which a number of multi-port cards can be plugged to provide additional access as the network grows in size.
- A concentrator is a device that provides a central connection point for cables from workstations, servers, and peripherals.
- Hubs can be either passive or active/
- **Active Hubs** electrically amplify the signals as it moves from one connected device to another. Active concentrators are used like repeaters to extend the length of a network.
- **Passive Hubs** allow the signal to pass from one computer to another without any change.




Hub
PC 1
PC 2

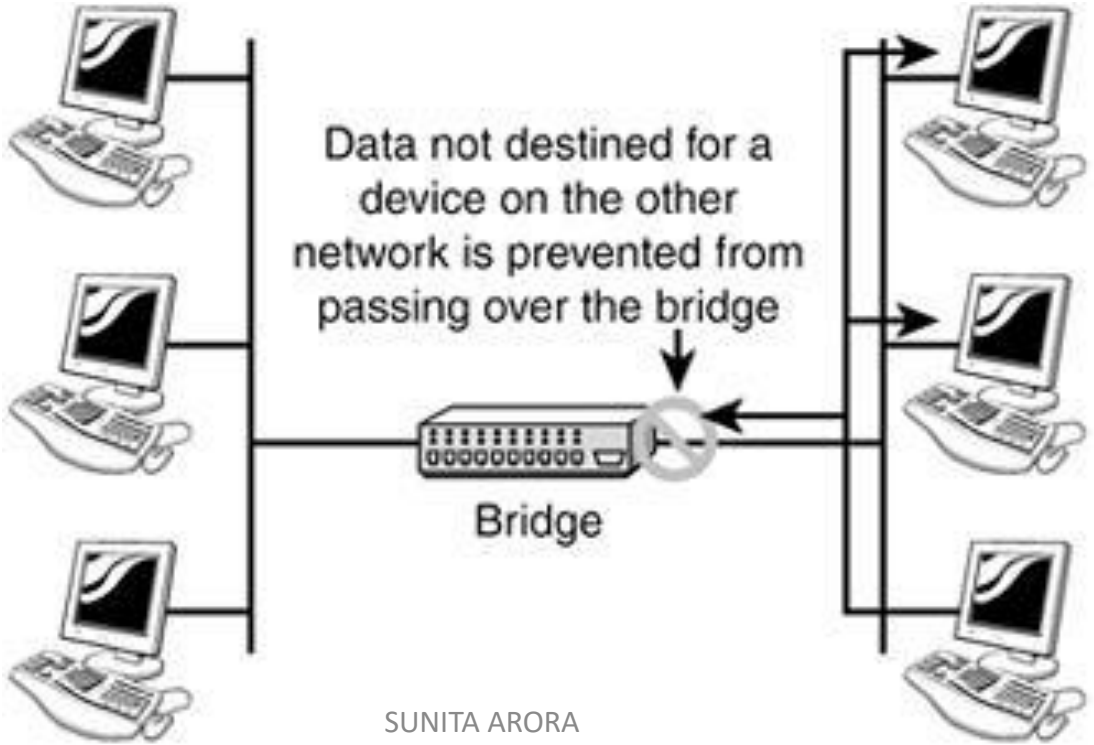
- **4. Switch:**
- A switch is a device that is used to segment networks into different subnetworks called subnets or LAN segments.
- Segmenting the network into smaller subnets, prevents traffic overloading in a network.
- A switch is responsible for filtering ie., transforming data in a specific way and for forwarding packets (a piece of message being transmitted) between LAN segments.
- LANs that are segmented through switches are called switched LANs.
- To insulate the transmission from the other ports, the switch establishes a temporary connection between the source and destination, and then terminates the connection once the conversation is done.


5-Port 10/100Mbps Ethernet Switch

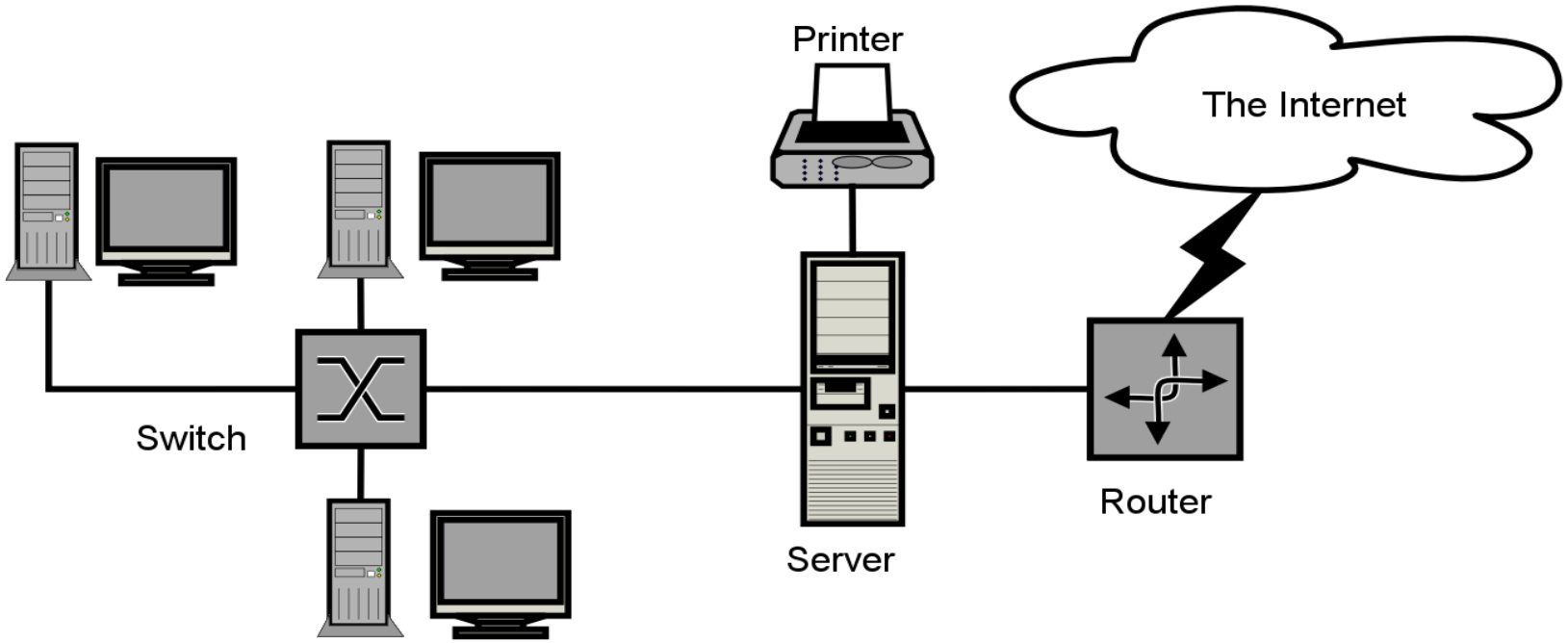


Example 1: A wired client-server network

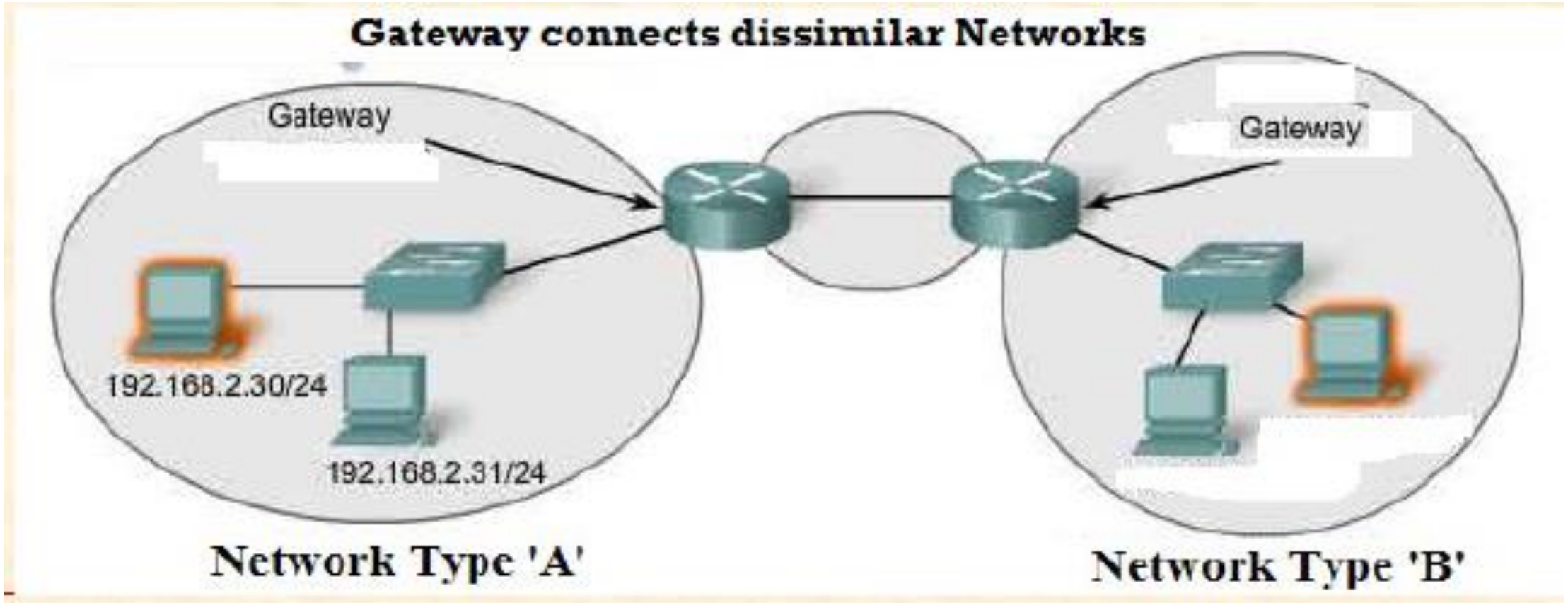
- **5. Bridge:**
- A bridge is a device that lets you link two networks together.
- Bridges are smart enough to know which computers are on which side of the bridge, so they only allow those messages that need to get to the other side to cross the bridge.
- Bridges can handle networks that follow same protocols.

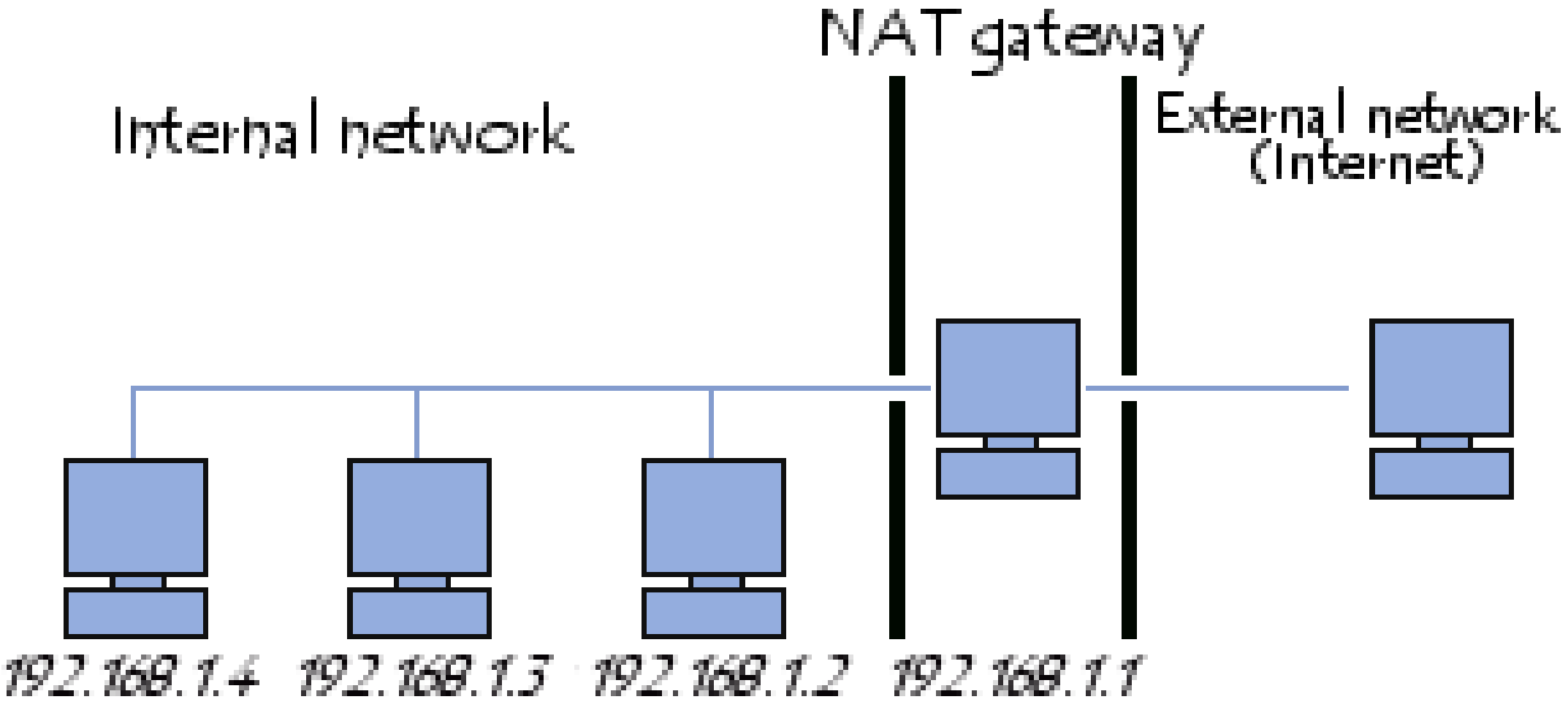


- **6. Router:**
- A router is a network device that forwards data from one network to another.
- A router works like a bridge but can handle different protocols.
- A device that works like a bridge but can handle different protocols, is known as a router.
- For example, a router can link Ethernet to a mainframe.
- The router is responsible for forwarding data from one network to a different network.
- If the destination is unknown to a router it sends the traffic to another router which knows the destination.
- Based on a network road map called routing table, routers can help ensure that packets are travelling the most efficient paths to their destinations.
- If a link between two routers fails, the sending router can determine an alternate route to keep traffic moving.
- A router uses logical address (IP address) and bridge uses physical address (MAC address).


Printer
The Internet
Switch
Server
Router

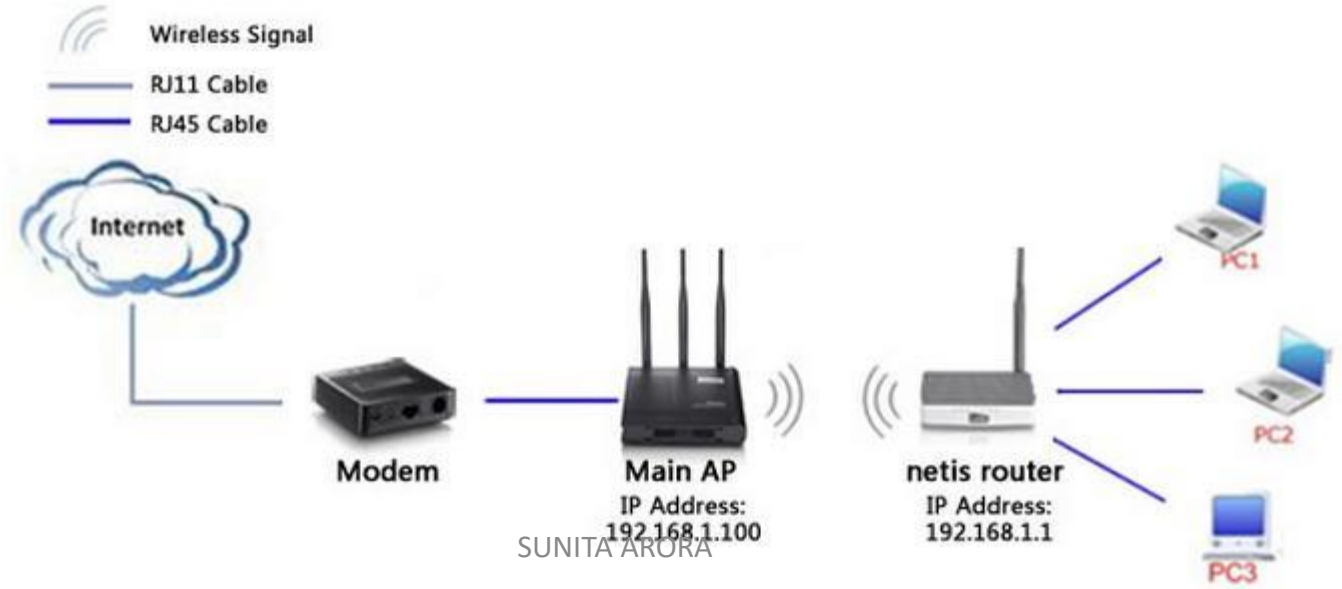
- **7. Gateway:**
- A gateway is a network device that connects dissimilar networks.
- It establishes an intelligent connection between a local network and external networks with completely different structures.
- A gateway is a node on a network that serves as an entrance to another network.
- In enterprises, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving the web pages.
- In homes, the gateway is the ISP that connects the user to the Internet.
- In enterprises, the gateway node often acts as a proxy server (a machine that is not actually a server but appears as a server) and a firewall (a system designed to prevent unauthorized access to or from a private network).
- The gateway is also associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch, which provides the actual path for the packet in and out of the gateway.


Gateway connects dissimilar Networks
Gateway
Gateway
192.168.2.30/24
192.168.2.31/24
Network Type 'A'
Network Type 'B'

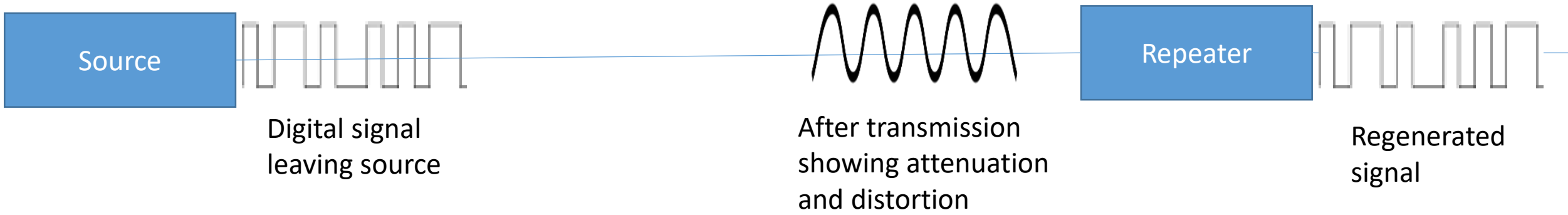

NAT gateway
Internal network
External network
(Internet)
192.168.1.4
192.168.1.3
192.168.1.2
192.168.1.1

- **8. Access Point (AP):**
- An access point (AP) also called wireless access point (WAP), is a hardware device that establishes connection(s) of computing devices on wireless LAN with a fixed network.
- The AP is connected to a fixed wire network and it then broadcasts wireless signals that computing devices having WiFi cards can detect; using these wireless signals, the computing devices get connected to fixed wired network via AP and use network as needed.
- AP is a station that transmits and receives data thus sometimes referred to as a transceiver.
- Every access point has a range (upto 150 feet for home based APs) and only the devices within this range can connect to the network using AP.

- The moment a device moves out of this range, its connection with AP breaks.
- Similarly, every AP also has a limit on number of computing devices it can attach to simultaneously.
- Different types of wireless access points are available that are suitable to different types of users with different needs, e.g., an AP at home is different from an AP at a large enterprise or college campus.
- Advantages of AP include: easier installation, easier maintenance, bigger network coverage, stable signals, and ease of work.
- Wireless routers can function as AP, but not all AP can work as routers.



- **9. Repeater:**
- **A repeater is a device that is used to regenerate a signal which is on its way through a communication channel. A repeater regenerates the received signal and re-transmits it to its destination.**
- Repeaters are of two kinds: amplifiers and signal repeaters.
- The first merely amplifies all incoming signals over the network. However, it amplifies both the signal and any concurrent noise. The second type collects the inbound packet and then retransmits the packet as if it were starting from the source station.



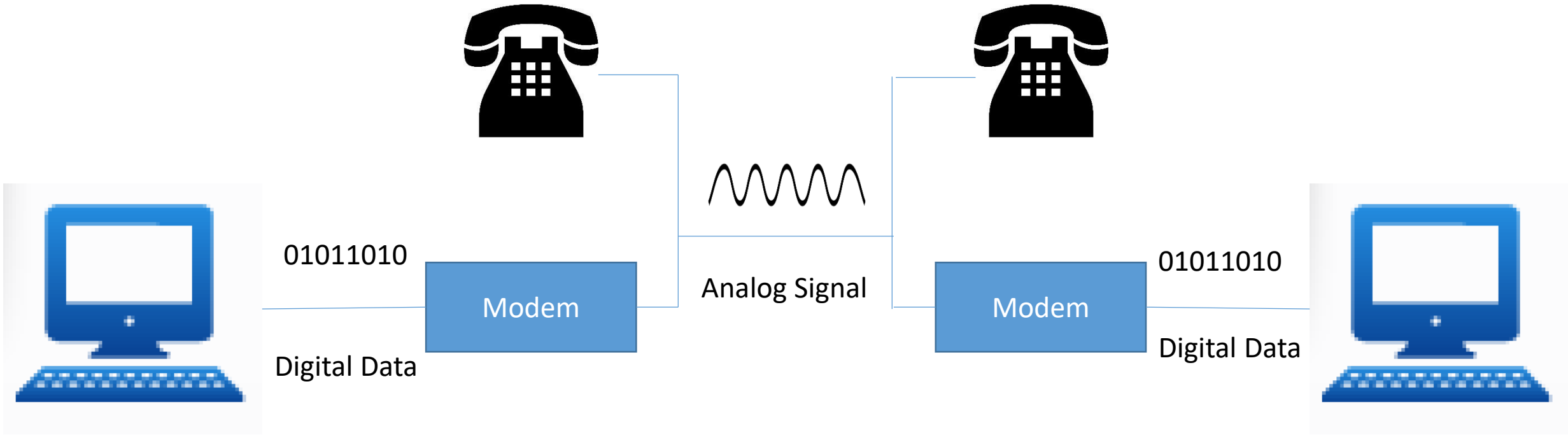
Digital signal leaving source

After transmission showing attenuation and distortion

Regenerated signal

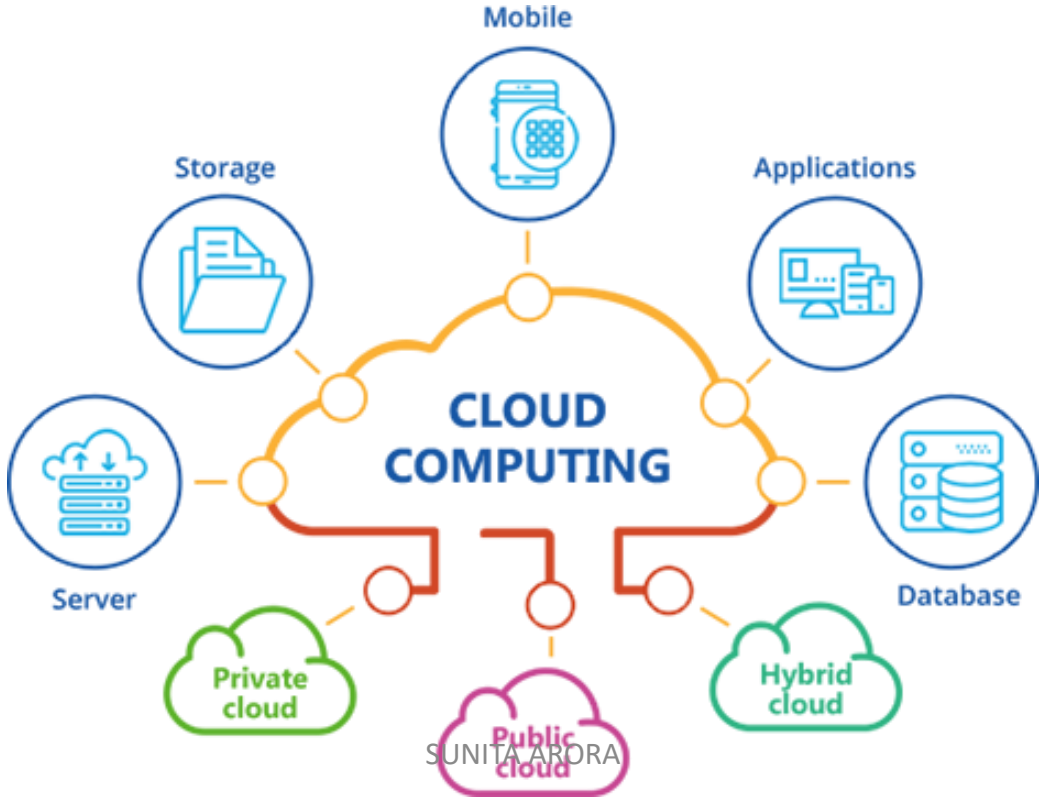
- **10. Modem:**
- A modem is a computer peripheral that allows you to connect and communicate with other computers via telephone lines.
- Modulation is the process of sending data on a wave. T
- Three types of modulation techniques are used:
- A. AM (amplitude modulation)
- B. FM (frequency modulation)
- C. PM (pulse modulation)
- With a modem and a standard telephone line you can send faxes to the office or important customers without leaving your computer.
- Two types of modem:
- A. internal modems: the modems that are fixed within the computer
- B. external modems: the modems that are connected externally to a computer as other peripherals are connected.


D-Link
Power
Status
DSL
WLAN
LAN
Internet
Wireless ADSL Router
DSL-2640B


01011010
Modem
Digital Data
Analog Signal
Modem
01011010
Digital Data

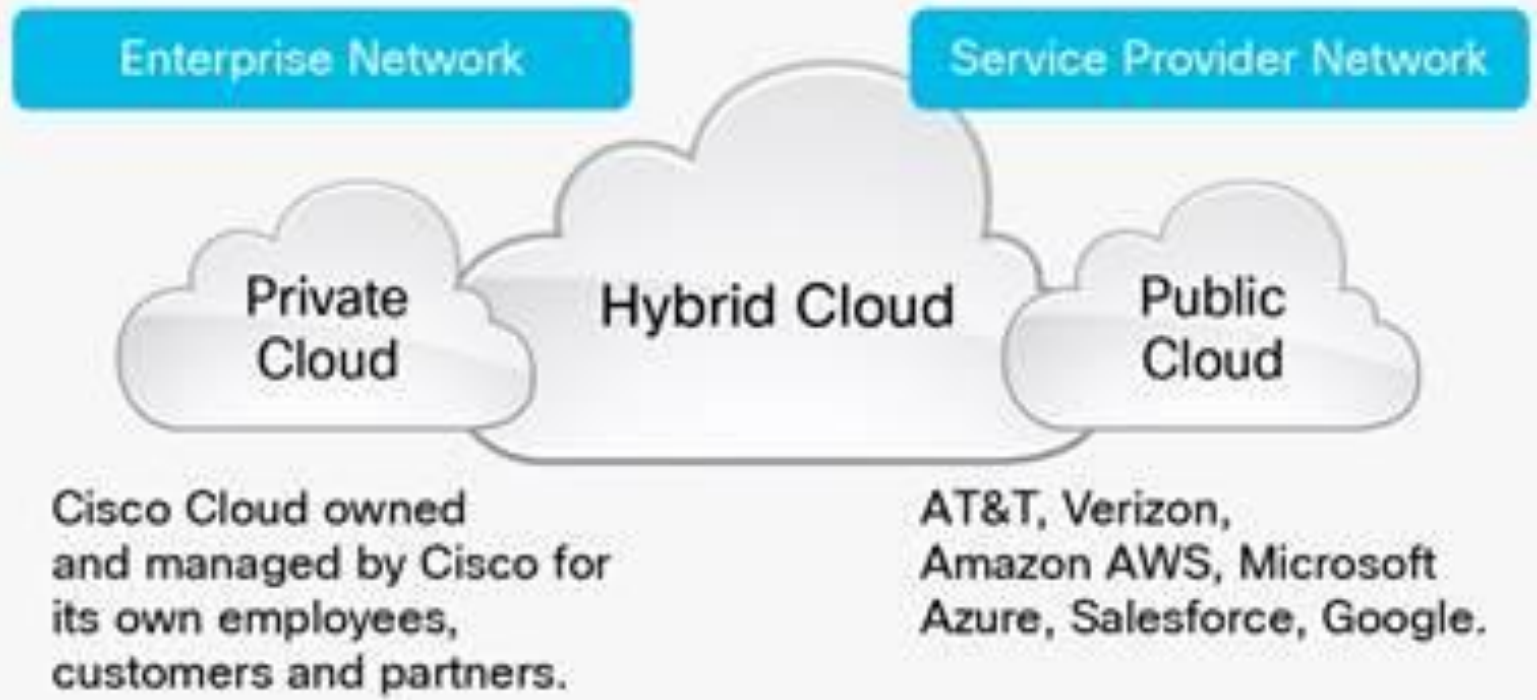
THE CLOUD

- The cloud is a generic term used for Internet.
- The term cloud was coined to refer to the collection of servers.
- Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand.

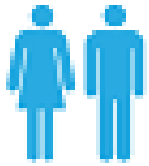


- Cloud computing is a new name for an old concept: the delivery of computing services from a remote location.
- Cloud computing services are delivered through a network, usually the Internet.
- Types clouds:
- **1. Private clouds:** These are the clouds for exclusive use by a single organization and typically controlled, managed and hosted in private data centres. The hosting and operation of private clouds may also be outsourced to a third party service provider, but a private cloud remains for the exclusive use of one organization.
- **2. Public clouds:** These are the clouds for use by multiple organizations (tenants) on a shared basis and hosted and managed by a third party service provider.

- **3. Community clouds:** These are the clouds for use by a group of related organizations who wish to make use of a common cloud computing environment. For example, a community might consist of the different branches of the military, all the universities in a given region, or all the suppliers to a large manufacturer.
- **4. Hybrid clouds:** When a single organization adopts both private and public clouds for a single application in order to take advantage of the benefits of both. For example, in a cloudbursting scenario, an organization might run the steady-state workload of an application on a private cloud, but when a spike in workload occurs, such as at the end of the financial quarter or during the holiday season, they can burst out to use computing capacity from a public cloud.

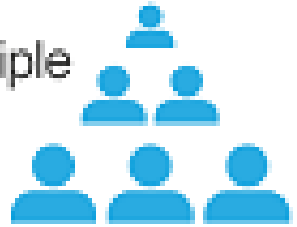

Enterprise Network
Service Provider Network
Private Cloud
Hybrid Cloud
Public Cloud
Cisco Cloud owned and managed by Cisco for its own employees, customers and partners.
AT&T, Verizon, Amazon AWS, Microsoft Azure, Salesforce, Google.

VS



Publically Shared
Virtualised Resources

Supports multiple
customers



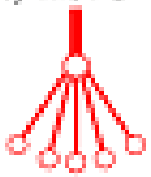
Supports connectivity
over the internet

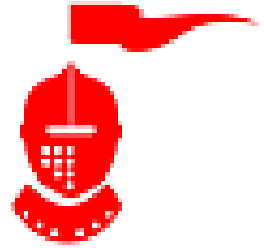
Suited for less
confidential information

Privately Shared
Virtualised Resources

Cluster of dedicated
customers

Connectivity over
internet, fibre and private network

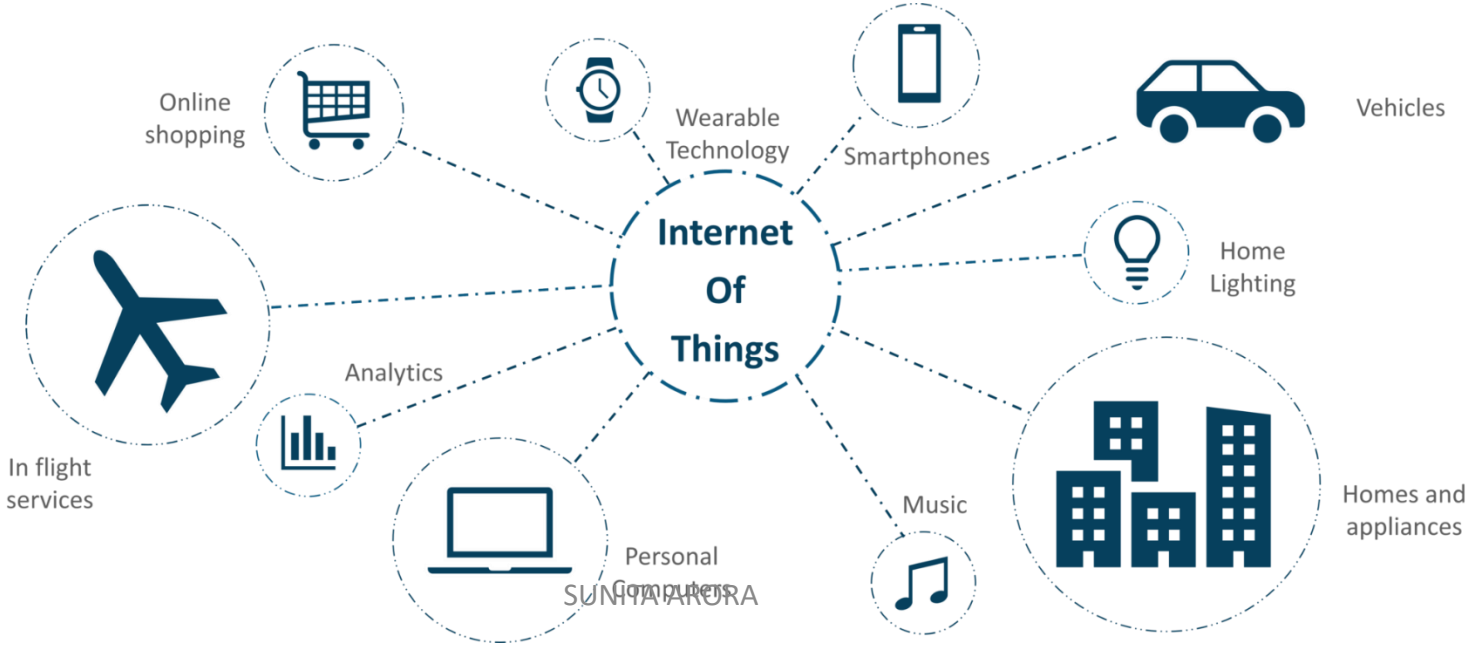




Suited for secured
confidential information
& core systems

INTERNET OF THINGS (IoT)

- IoT is a phenomenon that connects the things (the smart devices) to the internet over wired or wireless connections.
- Here the things could refer to every smart device of today's age i.e., from computers and smartphones to home appliances, wearables, vehicles, factory machines, to consumables etc.
- IoT allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service.



- **Enabling technologies for IoT:**
- To make IoT possible, different technological concepts are implemented together. These enabling technologies are:
- **1. RFID (Radio Frequency Identification):** This technology is designed to use radio waves to read and capture information stored on a tag, called an RFIF tag, attached to an object.
- **2. Sensors:** A sensor is a device that is able to detect changes in an environment. A sensor is able to measure a physical phenomenon (like temperature, pressure, and so on) and transform it into an electric signal. Modern age IoT contains different types of sensors for variety of applications. Most common types of sensors used in IoT are temperature sensors, proximity sensors, pressure sensors, optical sensors, humidity sensors, motion detection sensors, smoke sensors, gas sensors.

- **3. Smart technologies:** Smart technologies include additional functionality to take action and have other processing capabilities as per the requirements. For example, turning off or on a device, stopping a vehicle, locking/unlocking a door, adjusting the temperature of an oven and many more such actions.
- **4. Software:** The software provides the reusable solutions for connecting, taking actions and solving issues that may arise.
- **5. Efficient network connectivity:** IoT is formed through interconnections of devices to the internet. Hence the connectivity is very important. Modern age efficient network technologies play an important role in IoT.

- **Challenges and risks:**
- Most important and critical challenge and risk is the security of IoT.
- How secure the data is and how immune an IoT is, is a critical question.
- Like other networks, cyber-attacks, hackers, and unauthorized intruders can attack IoTs as well.
- With billions of “Things” connected to the Internet, it could also mean that by unauthorized access one can create disasters – something that is unimaginable.