GBN GOVERNMENT POLYTECHNIC NILOKHERI

Branch: ECE

Semester: 5^{th} Sem.

Subject: COMPUTER NETWORKS

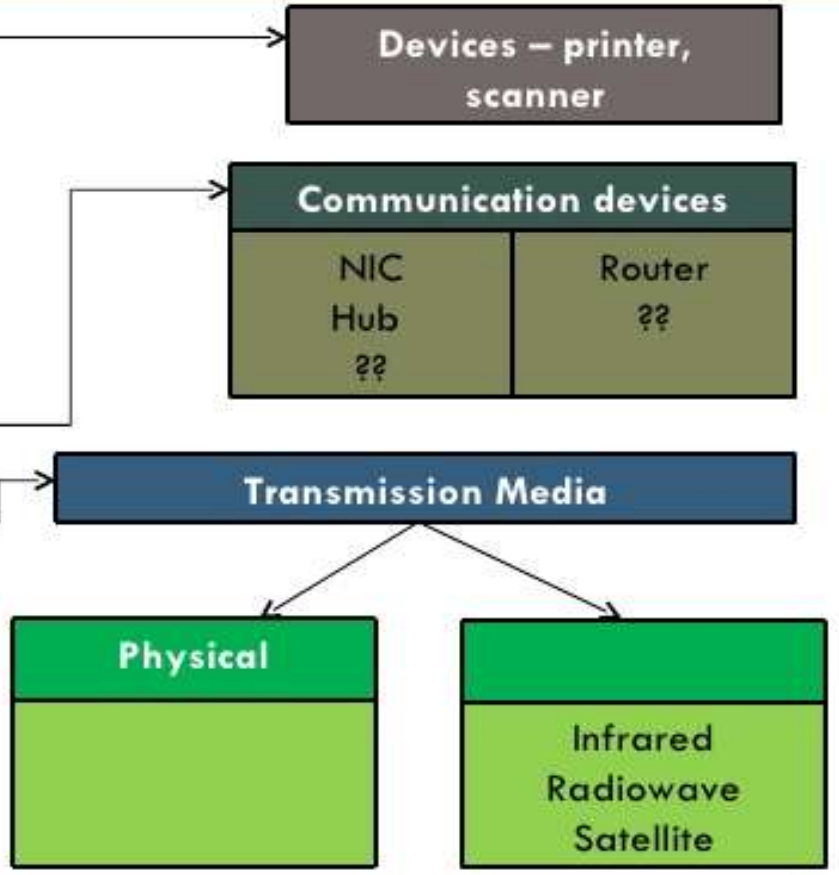
Chapter 1
(Network Basics)

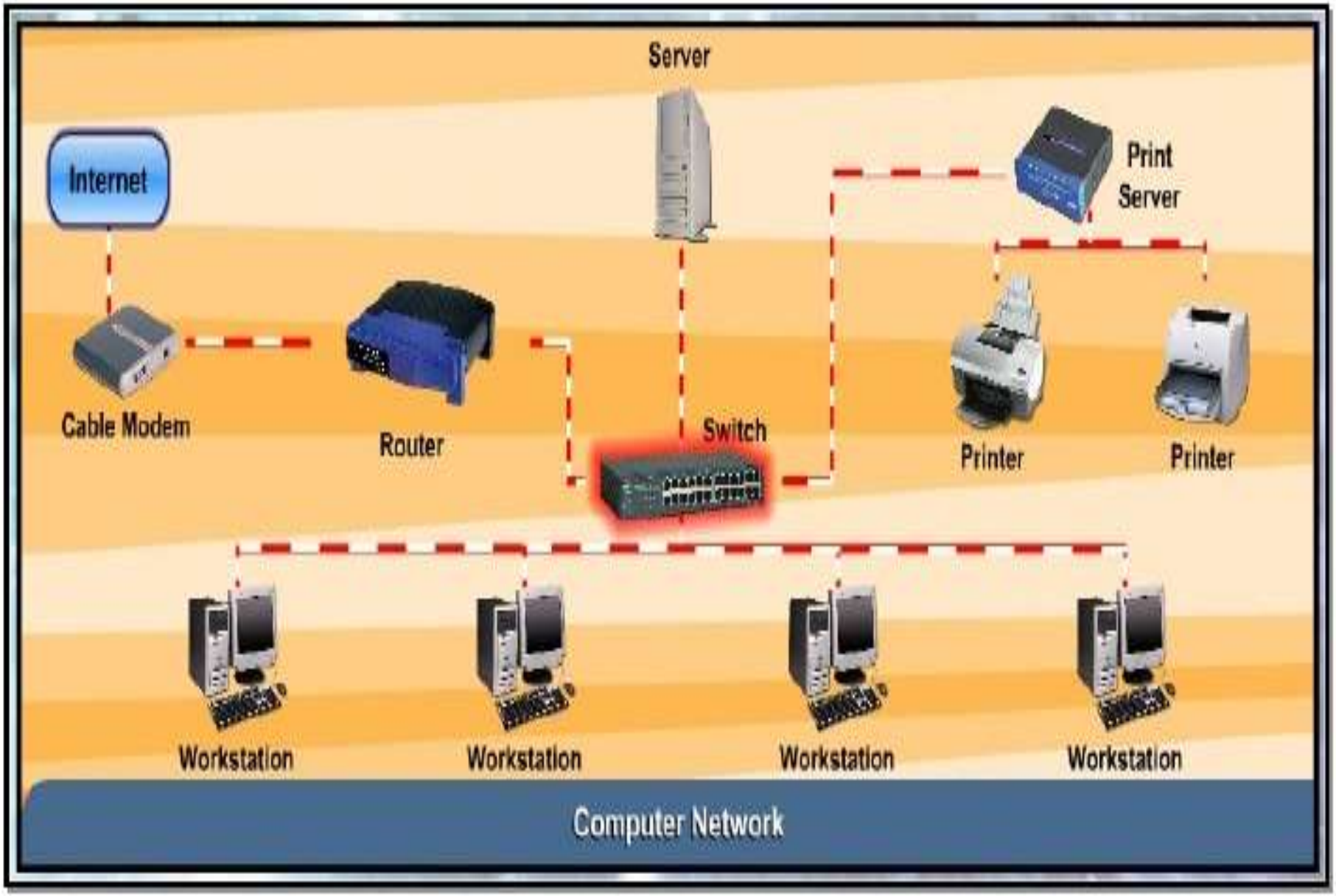
What is a network?

- The generic term "**network**" refers to a group of entities (objects, people, etc.) which are connected to one another.
- **computer network**: A group of computers and peripheral devices linked to each other with physical lines, exchanging information as digital data (binary values, i.e. values encoded as a signal which may represent either 0 or 1). Note that the smallest possible network is two computers connected together.
- **networking**: Implementing tools and tasks for linking computers so that they can share resources over the network.

Definition of Computer Networks

A computer network is a collection of **computers** and **devices** connected together via **communication devices** and **transmission media.** For examples it may connect computers, printers and scanners.




Server
Internet
Print
Server
Cable Modem
Router
Switch
Printer
Printer
Workstation
Workstation
Workstation
Workstation
Computer Network

Why networks are important?

A computer network can serve several distinct purposes:

- Sharing resources (files, applications or hardware, an Internet connection, etc.)
- Communication between people (email, live discussions, etc.)
- Communication between processes (such as between industrial computers)
- Guaranteeing full access to information for a specified group of people (networked databases).

The Importance/Advantage of Computer Networks

Sharing of **devices** such as printer and scanner

Sharing of **program**/software

Sharing of **files**

Sharing of **data**

Sharing of **information**

Sharing of **single high-speed internet connection**

Can access server centered **database**

Better communication using internet services such as email, mailing list and Internet Relat Chat (IRC)

Classification of Computer Networks

Computer networks are classified based on various factors. They includes:

- Geographical span
- Inter-connectivity
- Administration
- Architecture

Geographical Span

Geographically a network can be seen in one of the following categories:

- It may be spanned across your table, among Bluetooth enabled devices,. Ranging not more than few meters.
- It may be spanned across a whole building, including intermediate devices to connect all floors.
- It may be spanned across a whole city.
- It may be spanned across multiple cities or provinces.
- It may be one network covering whole world.

Inter-Connectivity

Components of a network can be connected to each other differently in some fashion. By connectedness we mean either logically , physically , or both ways.

- Every single device can be connected to every other device on network, making the network mesh.
- All devices can be connected to a single medium but geographically disconnected, created bus like structure.
- Each device is connected to its left and right peers only, creating linear structure.
- All devices connected together with a single device, creating star like structure.
- All devices connected arbitrarily using all previous ways to connect each other, resulting in a hybrid structure.

Administration

- From an administrator's point of view, a network can be private network which belongs a single autonomous system and cannot be accessed outside its physical or logical domain. A network can be public which is accessed by all.

Network Architecture

Computer networks can be discriminated into various types such as Client-Server, peer-to-peer or hybrid, depending upon its architecture.

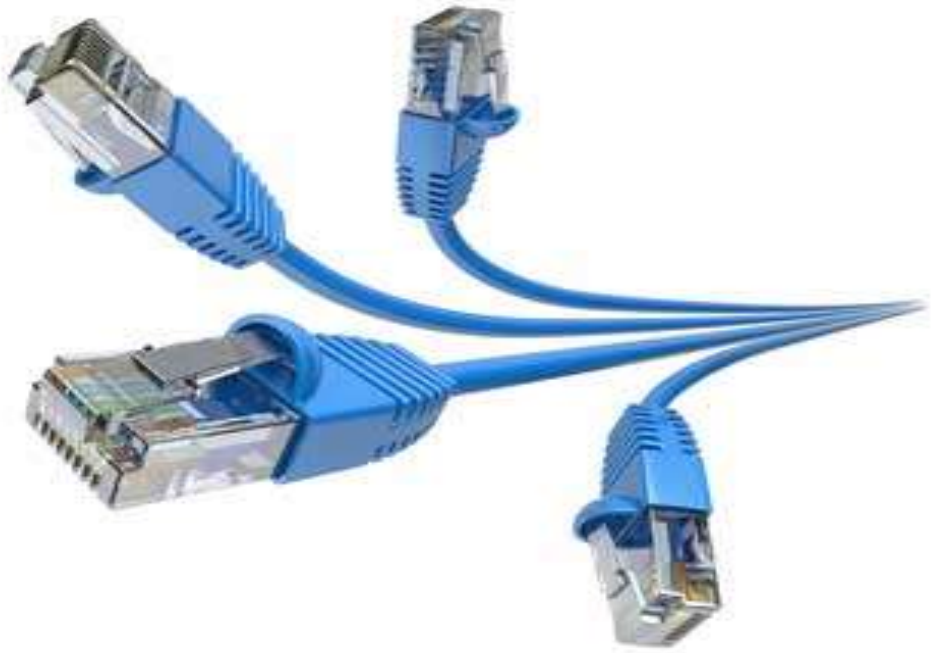
- There can be one or more systems acting as Server. Other being Client, requests the Server to serve requests. Server takes and processes request on behalf of Clients.
- Two systems can be connected Point-to-Point, or in back-to-back fashion. They both reside at the same level and called peers.
- There can be hybrid network which involves network architecture of both the above types.

List of hardware's required to set up a computer network

- Network Cables
- Distributors
- Routers
- Internal Network Cards
- External Network Cards

Network Cables

- Network cables are used to connect computers. The most commonly used cable is Category 5 cable RJ-45.



Distributors

- A computer can be connected to another one via a serial port but if we need to connect many computers to produce a network, this serial connection will not work.

- The solution is to use a central body to which other computers, printers, scanners, etc. can be connected and then this body will manage or distribute network traffic

Router

- A router is a type of device which acts as the central point among computers and other devices that are a part of the network. It is equipped with holes called ports. Computers and other devices are connected to a router using network cables. Now-a-days router comes in wireless modes using which computers can be connected without any physical cable.

Network Card

- Network card is a necessary component of a computer without which a computer cannot be connected over a network. It is also known as the network adapter or Network Interface Card (NIC). Most branded computers have network card pre-installed. Network cards are of two types: Internal and External Network Cards.

Internal Network Cards

- Motherboard has a slot for internal network card where it is to be inserted. Internal network cards are of two types in which the first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA). Network cables are required to provide network access.

External Network Cards

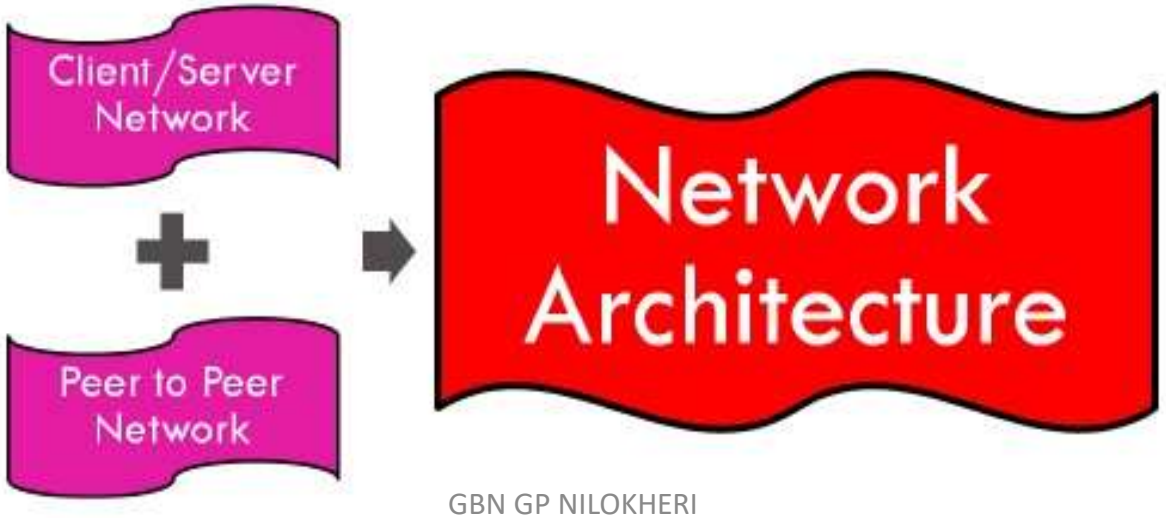
- External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network.

Universal Serial Bus (USB)

- USB card is easy to use and connects via USB port. Computers automatically detect USB card and can install the drivers required to support the USB network card automatically.

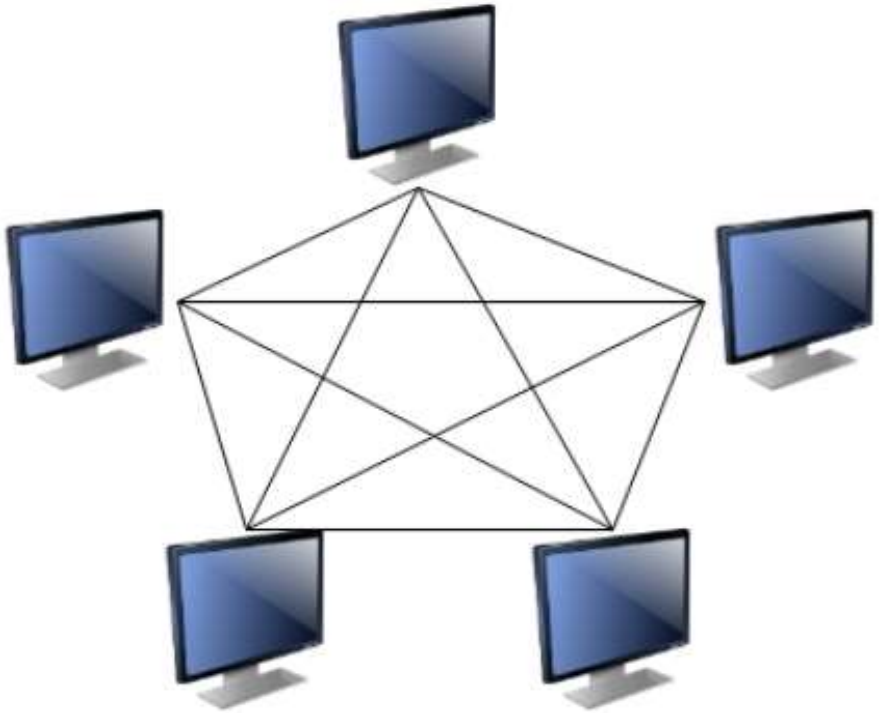
Network Architecture

- **Network architecture** is the overall **design of a computer network** that describes how a computer network is configured and what strategies are being used.
- It is mainly focuses on the function of the networks.
- It is also known as **network model** or **network design.**
- Two main network architecture:



Peer to Peer Network

- The peer to peer computing architecture contains nodes that are equal participants in data sharing. All the tasks are equally divided between all the nodes. The nodes interact with each other as required as share resources.



Characteristics of Peer to Peer Computing

- Peer to peer networks are usually formed by groups of a dozen or less computers. These computers all store their data using individual security but also share data with all the other nodes.
- The nodes in peer to peer networks both use resources and provide resources. So, if the nodes increase, then the resource sharing capacity of the peer to peer network increases. This is different than client server networks where the server gets overwhelmed if the nodes increase.
- Since nodes in peer to peer networks act as both clients and servers, it is difficult to provide adequate security for the nodes. This can lead to denial of service attacks.
- Most modern operating systems such as Windows and Mac OS contain software to implement peer to peer networks.

Advantages of Peer to Peer Computing

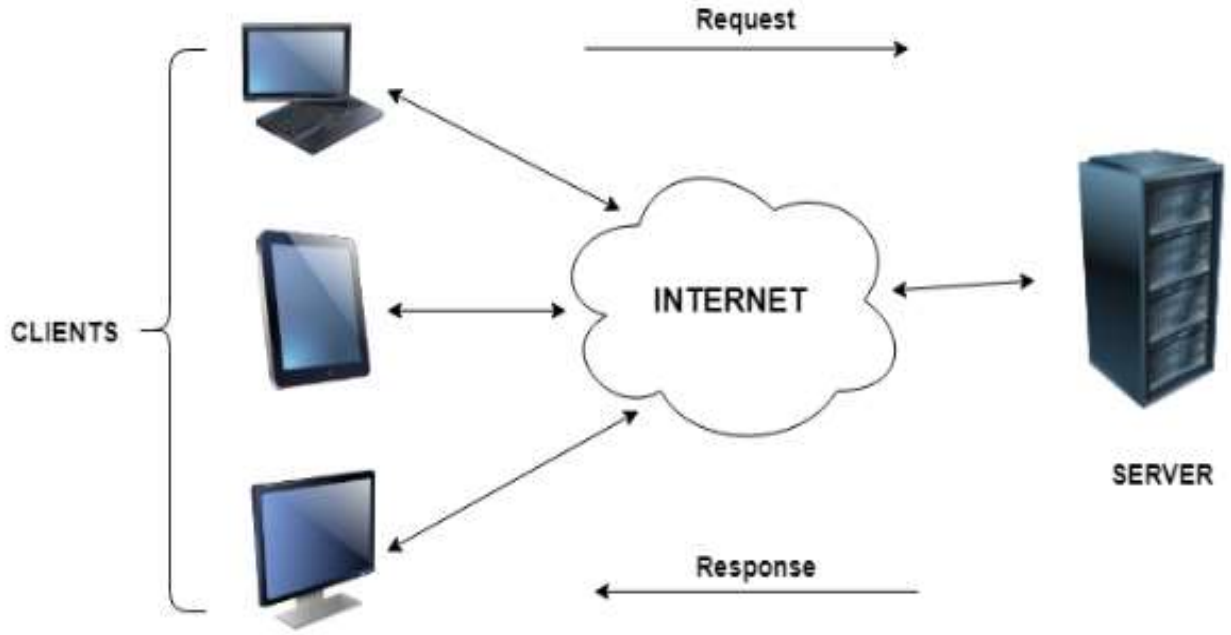
- Each computer in the peer to peer network manages itself. So, the network is quite easy to set up and maintain.
- In the client server network, the server handles all the requests of the clients. This provision is not required in peer to peer computing and the cost of the server is saved.
- It is easy to scale the peer to peer network and add more nodes. This only increases the data sharing capacity of the system.
- None of the nodes in the peer to peer network are dependent on the others for their functioning.

Disadvantages of Peer to Peer Computing

- It is difficult to backup the data as it is stored in different computer systems and there is no central server.
- It is difficult to provide overall security in the peer to peer network as each system is independent and contains its own data.

Client Server Network

- In client server computing, the clients requests a resource and the server provides that resource. A server may serve multiple clients at the same time while a client is in contact with only one server. Both the client and server usually communicate via a computer network but sometimes they may reside in the same system.



Characteristics of Client Server Computing

- The client server computing works with a system of request and response. The client sends a request to the server and the server responds with the desired information.
- The client and server should follow a common communication protocol so they can easily interact with each other. All the communication protocols are available at the application layer.
- A server can only accommodate a limited number of client requests at a time. So it uses a system based to priority to respond to the requests.
- Denial of Service attacks hinders servers ability to respond to authentic client requests by inundating it with false requests.
- An example of a client server computing system is a web server. It returns the web pages to the clients that requested them.

Advantages of Client Server Computing

- All the required data is concentrated in a single place i.e. the server. So it is easy to protect the data and provide authorization and authentication.
- The server need not be located physically close to the clients. Yet the data can be accessed efficiently.
- It is easy to replace, upgrade or relocate the nodes in the client server model because all the nodes are independent and request data only from the server.
- All the nodes i.e. clients and server may not be build on similar platforms yet they can easily facilitate the transfer of data.

Disadvantages of Client Server Computing

- If all the clients simultaneously request data from the server, it may get overloaded. This may lead to congestion in the network.
- If the server fails for any reason, then none of the requests of the clients can be fulfilled. This leads of failure of the client server network.
- The cost of setting and maintaining a client server model are quite high.

The Differences between Client/Server and Peer-to-Peer

Client/Server	Peer-to-Peer
1) Server has to control ability while client's don't	1) All computers have equal ability
2) Higher cabling cost	2) Cheaper cabling cost
3) It is used in small and large networks	3) Normally used in small networks with less than 10 computers
4) Easy to manage	4) Hard to manage
5) Install software only in the server while the clients share the software	5) Install software to every computer
6) One powerful computer acting as server	6) No server is needed

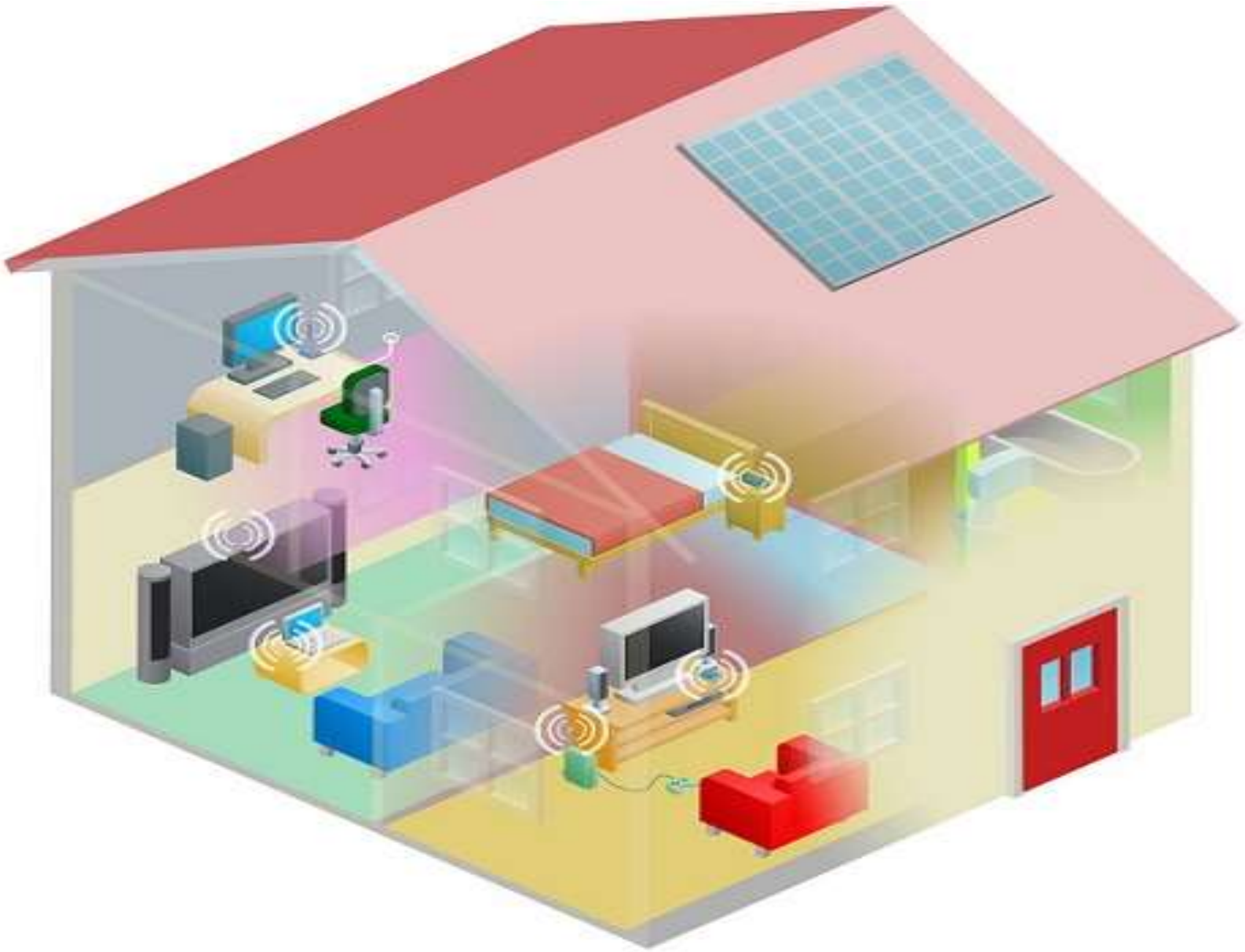
Types of Computer Network

- Networks can be categorized depending on size, complexity, level of security, or geographical range.

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

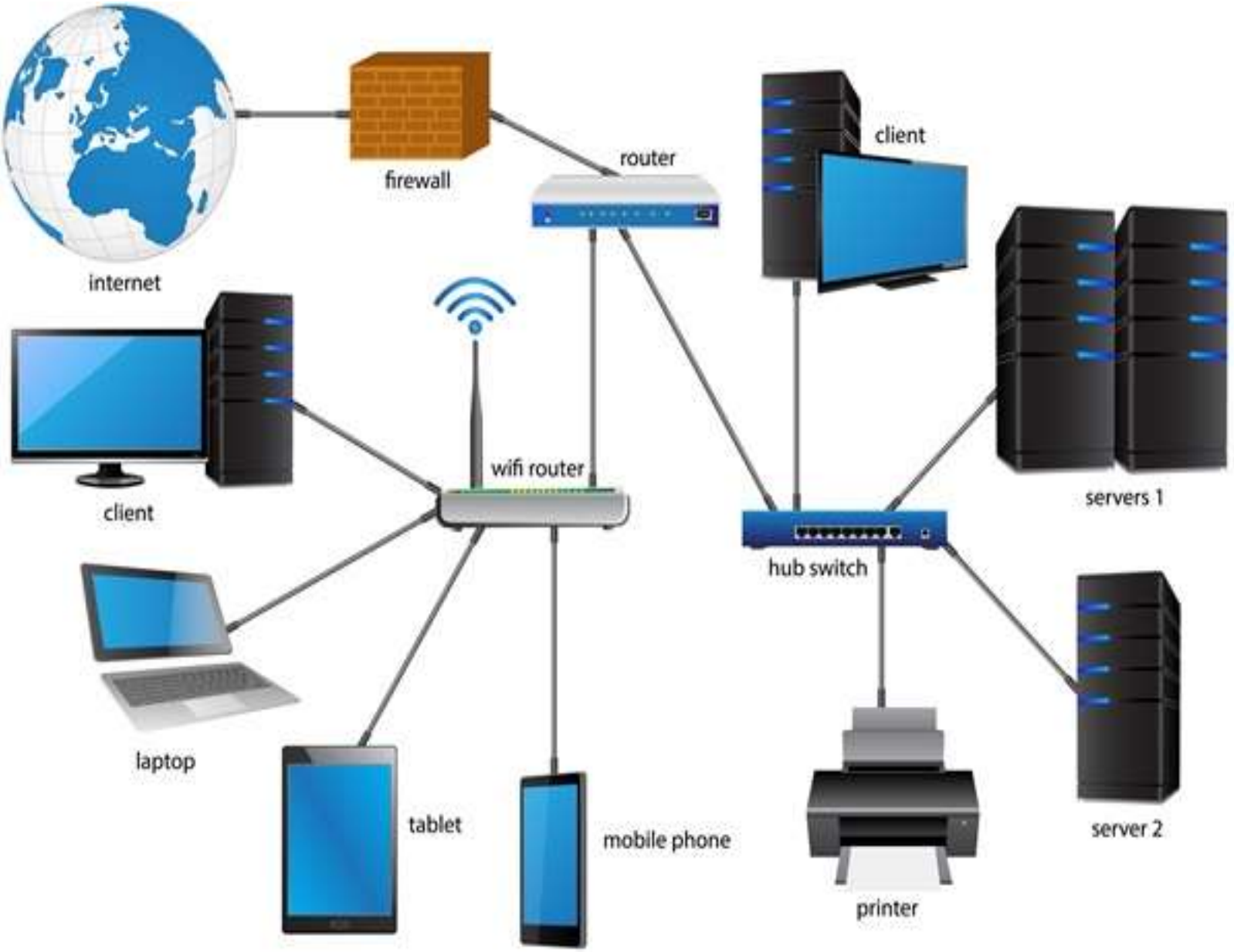
Personal Area Network (PAN)

- PAN is the interconnection between devices within the range of a person's private space, typically within a range of 10 meters.
- If you have transferred images or songs from your laptop to mobile or from mobile to your friend's mobile using Bluetooth, you have set up and used a personal area network.
- A person can connect his laptop, smart phone, personal digital assistant and portable printer in a network at home.
- This network could be fully Wi-Fi or a combination of wired and wireless.



Local Area Network (LAN)

- Local Area Network is a wired network spread over a single site like an office, building or manufacturing unit.
- LAN is set up to when team members need to share software and hardware resources with each other but not with the outside world.
- Typical software resources include official documents, user manuals, employee handbook, etc.
- Hardware resources that can be easily shared over the network include printer, fax machines, modems, memory space, etc. This decreases infrastructure costs for the organization drastically.
- A LAN may be set up using wired or wireless connections. A LAN that is completely wireless is called Wireless LAN or WLAN.


internet
firewall
router
client
servers 1
client
wifi router
hub switch
laptop
tablet
mobile phone
printer
server 2

Metropolitan Area Network (MAN)

- It is a network spread over a city, college campus or a small region.
- MAN is larger than a LAN and typically spread over several kilometers.
- Objective of MAN is to share hardware and software resources, thereby decreasing infrastructure costs.
- MAN can be built by connecting several LANs.
- The most common example of MAN is cable TV network.

Wide Area Network (WAN)

- Wide Area Network is spread over a country or many countries.
- WAN is typically a network of many LANs, MANs and WANs.
- Network is set up using wired or wireless connections, depending on availability and reliability.
- The most common example of WAN is the Internet.


CONNECTION

Differentiate between the types of Computer Networks

Different	LAN	MAN	WAN
Cost	Low optic	High	Higher
Network Size	Small	Larger	Largest
Speed	Fastest	Slower	Slowest
Transmission Media	Twisted-pair	Twisted-pair Fibre-optic cables	Fiber optic Radio wave Satellite
Number of Computers	Smallest	Large	Largest

Network Services

- Some basic services computer network can offer are:
- Directory Services
- File Services
- Communication Services
- Application Services

- **Directory Services**:-

i. Accounting

ii. Authentication and Authorization

iii. Domain Name Services

- **File Services**:-

i. File Sharing

ii. File Transfer

- **Communication Services:-**

i. Email
ii. Social Networking
iii. Internet Chat
iv. Discussion Boards
v. Remote Access

- **Application Services:-**

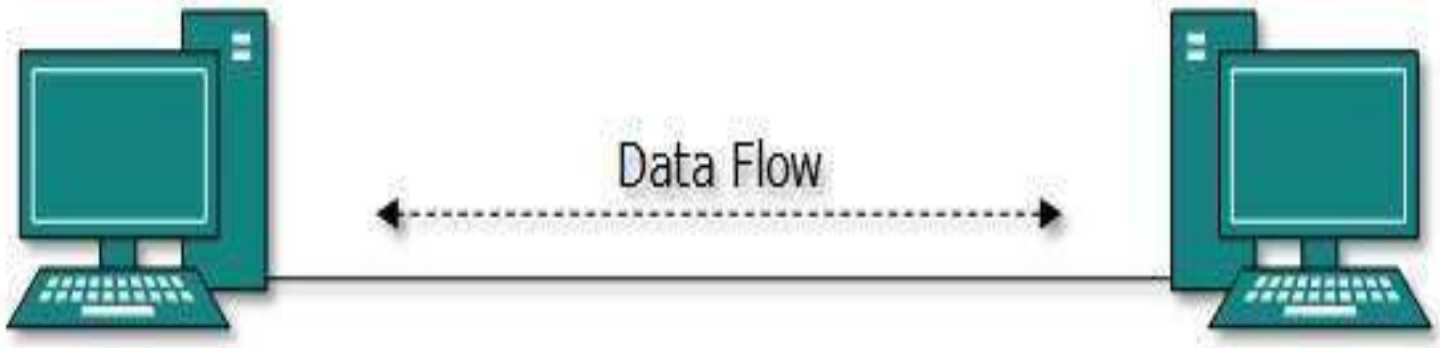
i. Resource Sharing
ii. Databases
iii. Web Services

Computer Network Topology

- 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. Both logical and physical topologies could be same or different in a same network.
- Point-to-Point
- Bus Topology
- Star Topology
- Ring Topology
- Tree Topology
- Daisy Chain
- Mesh Topology
- Hybrid Topology

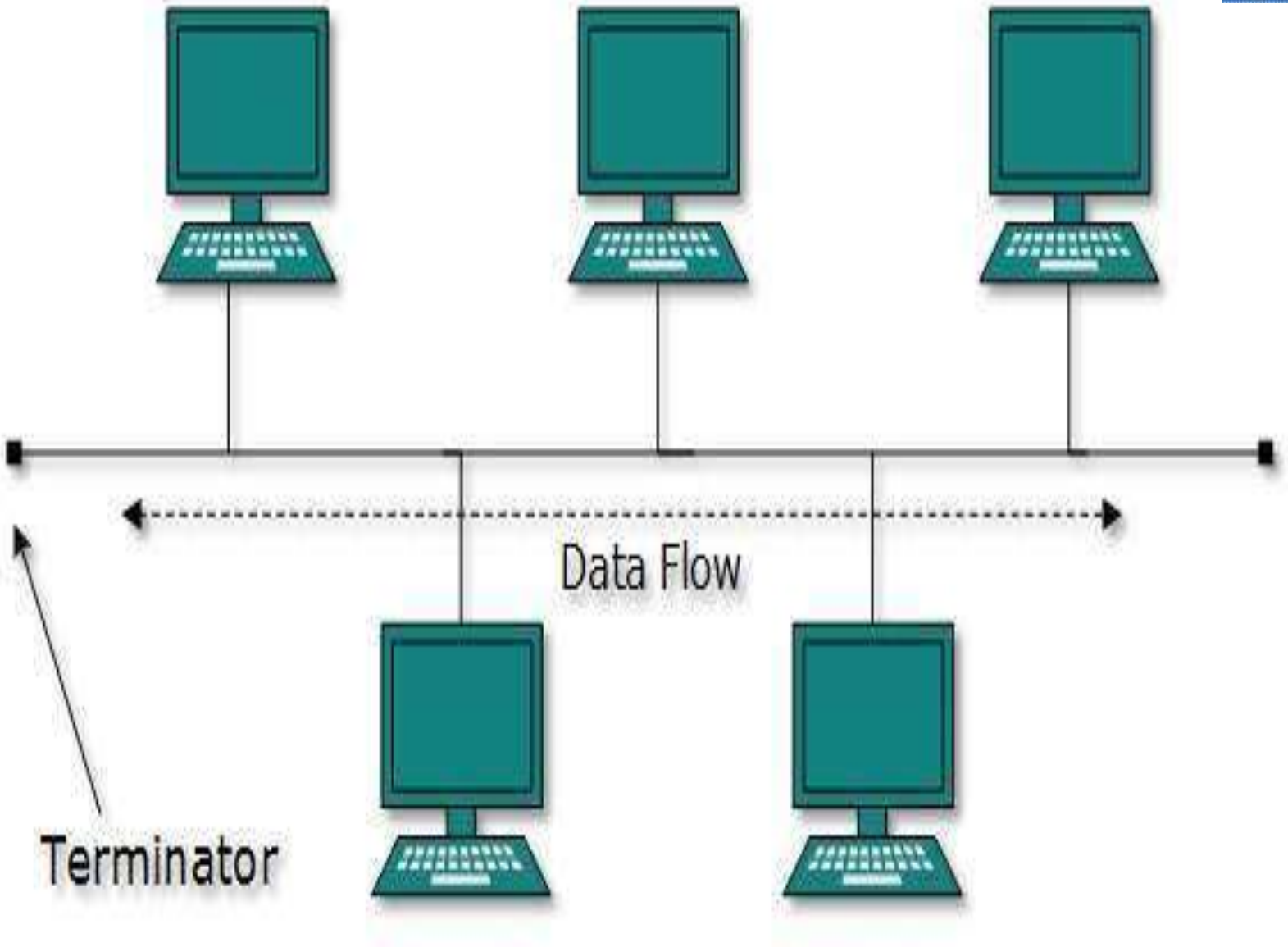
Point-to-Point

- 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.
- The receiving end of one host is connected to sending end of the other and vice-versa.
- If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.



Bus Topology

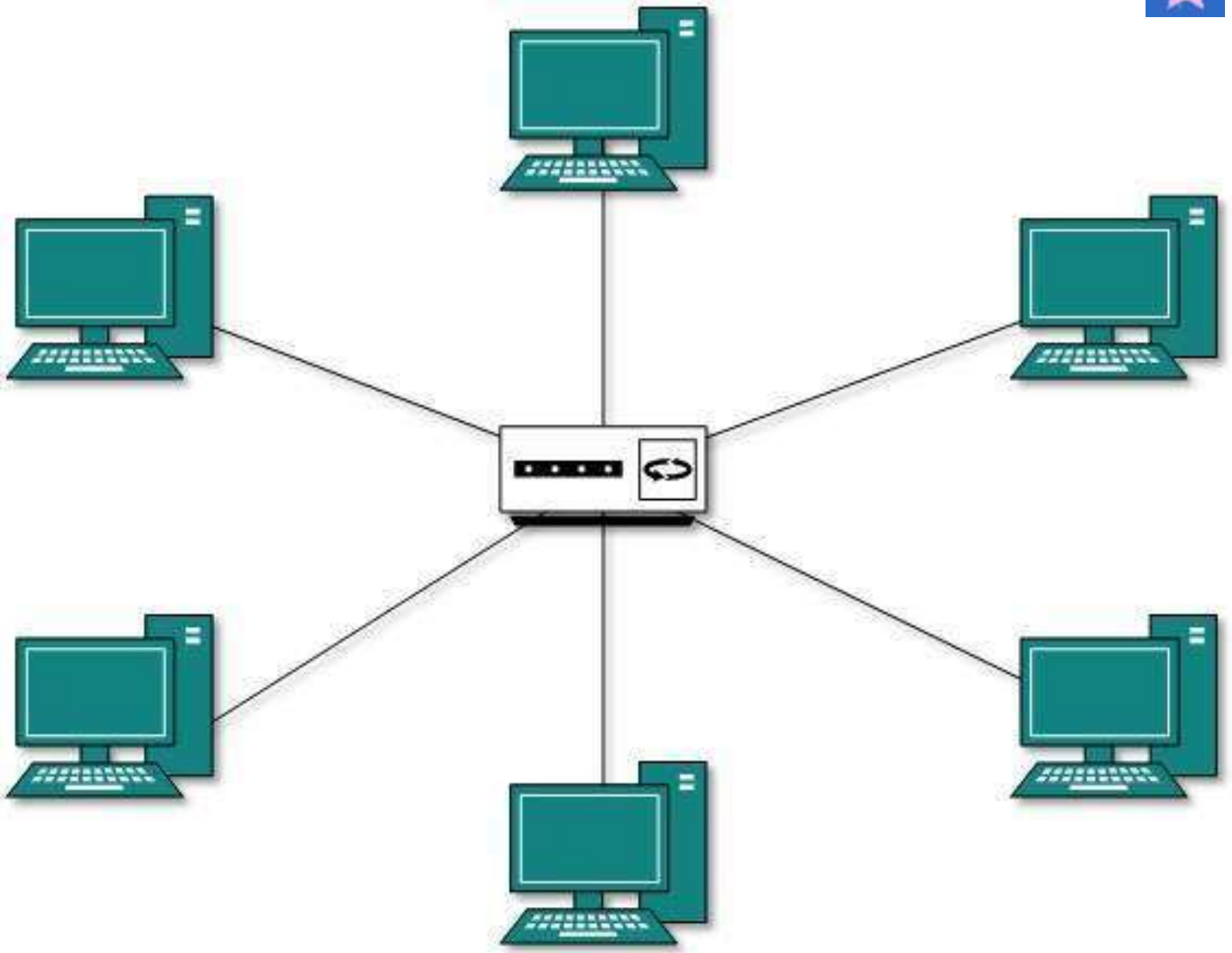
- All devices share single communication line or cable.
- This may have problem while multiple hosts sending data at the same time.
- Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue.
- It is one of the simple forms of networking where a failure of a device does not affect the other devices.
- But failure of the shared communication line can make all other devices stop functioning.
- Both ends of the shared channel have line terminator.
- The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.


Data Flow
Terminator

Star Topology

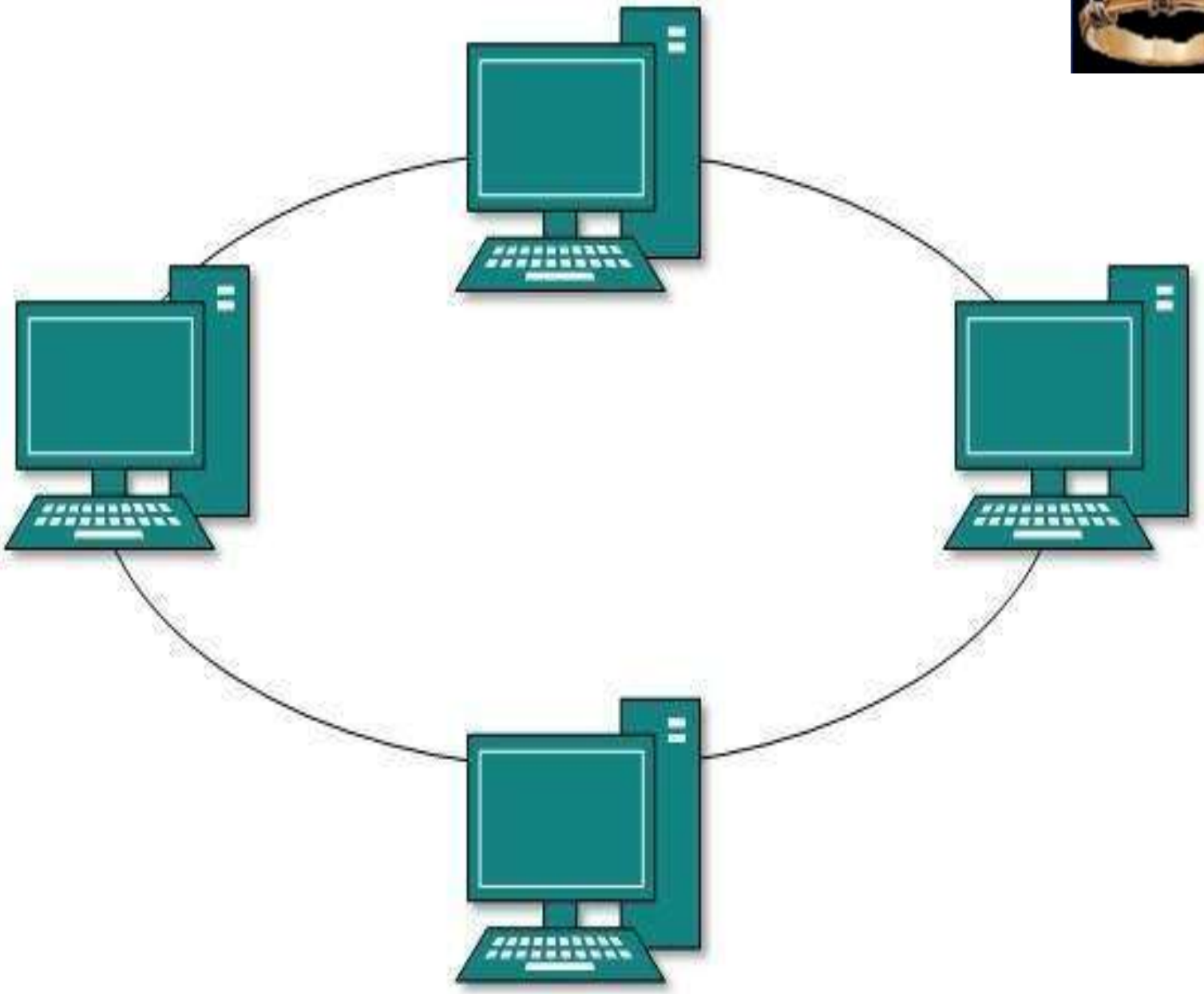
- All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:
- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway

- If hub fails, connectivity of all hosts to all other hosts fails.
- Every communication between hosts, takes place through only the hub.
- Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.



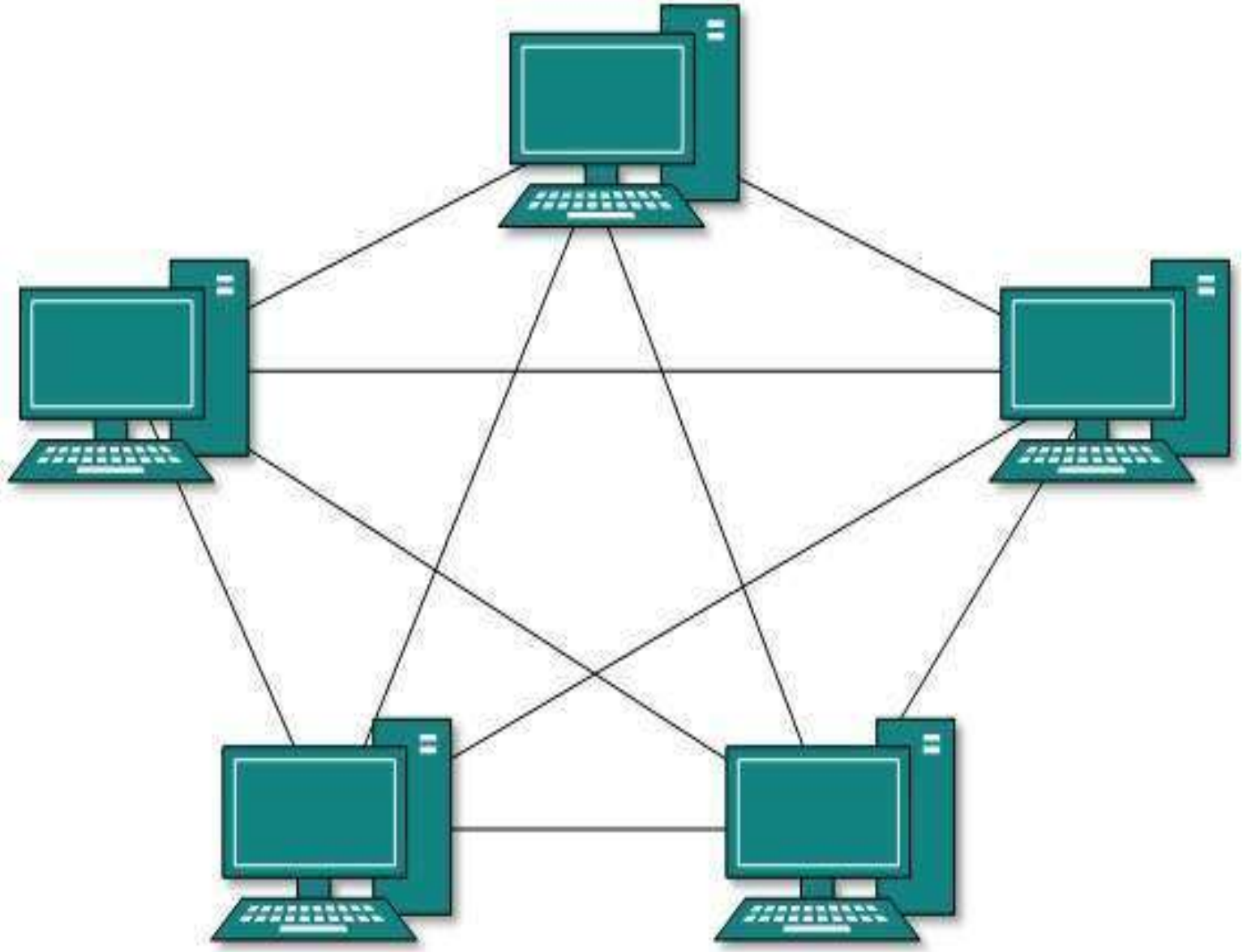
Ring Topology

- Each host machine connects to exactly two other machines, creating a circular network structure.
- When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts.
- To connect one more host in the existing structure, the administrator may need only one more extra cable.
- Failure of any host results in failure of the whole ring.
- Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.



Mesh Topology

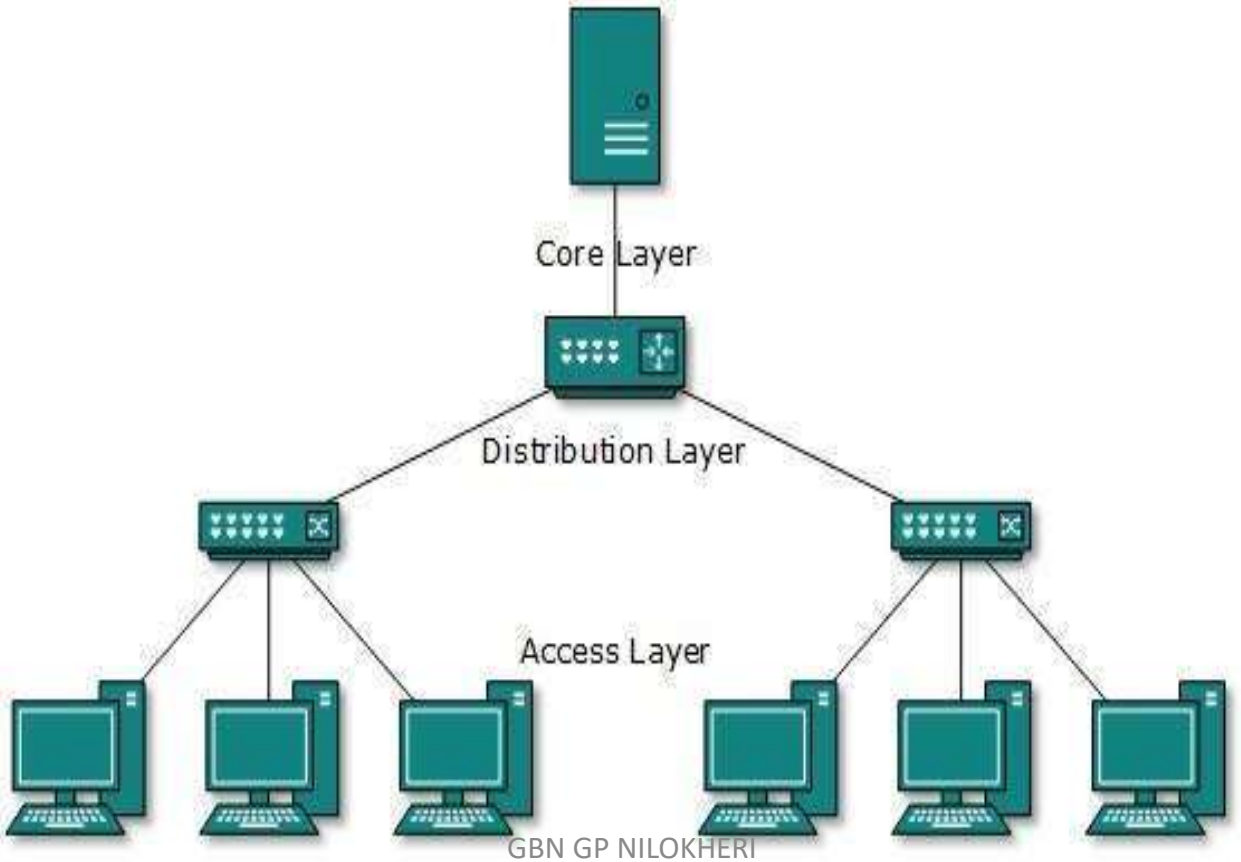
- A host is connected to one or multiple hosts.
- This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.
- Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:
- **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.
- **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.



Tree Topology

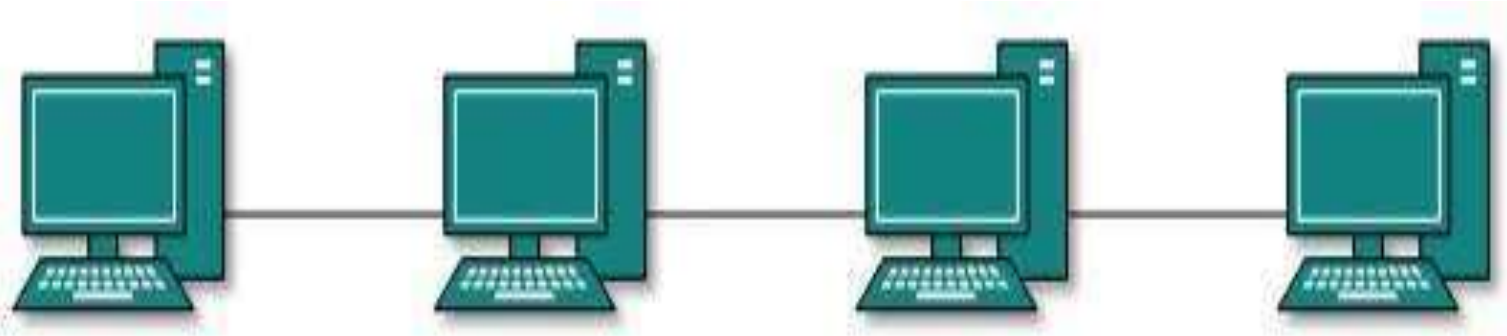
- Also known as Hierarchical Topology, this is the most common form of network topology in use presently.
- This topology imitates as extended Star topology and inherits properties of bus topology.
- This topology divides the network in to multiple levels/layers of network.
- Mainly in LANs, a network is bifurcated into three types of network devices.
- 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.

- All neighboring hosts have point-to-point connection between them.
- Similar to the Bus topology, if the root goes down, then the entire network suffers even though it is not the single point of failure.
- Every connection serves as point of failure, failing of which divides the network into unreachable segment.



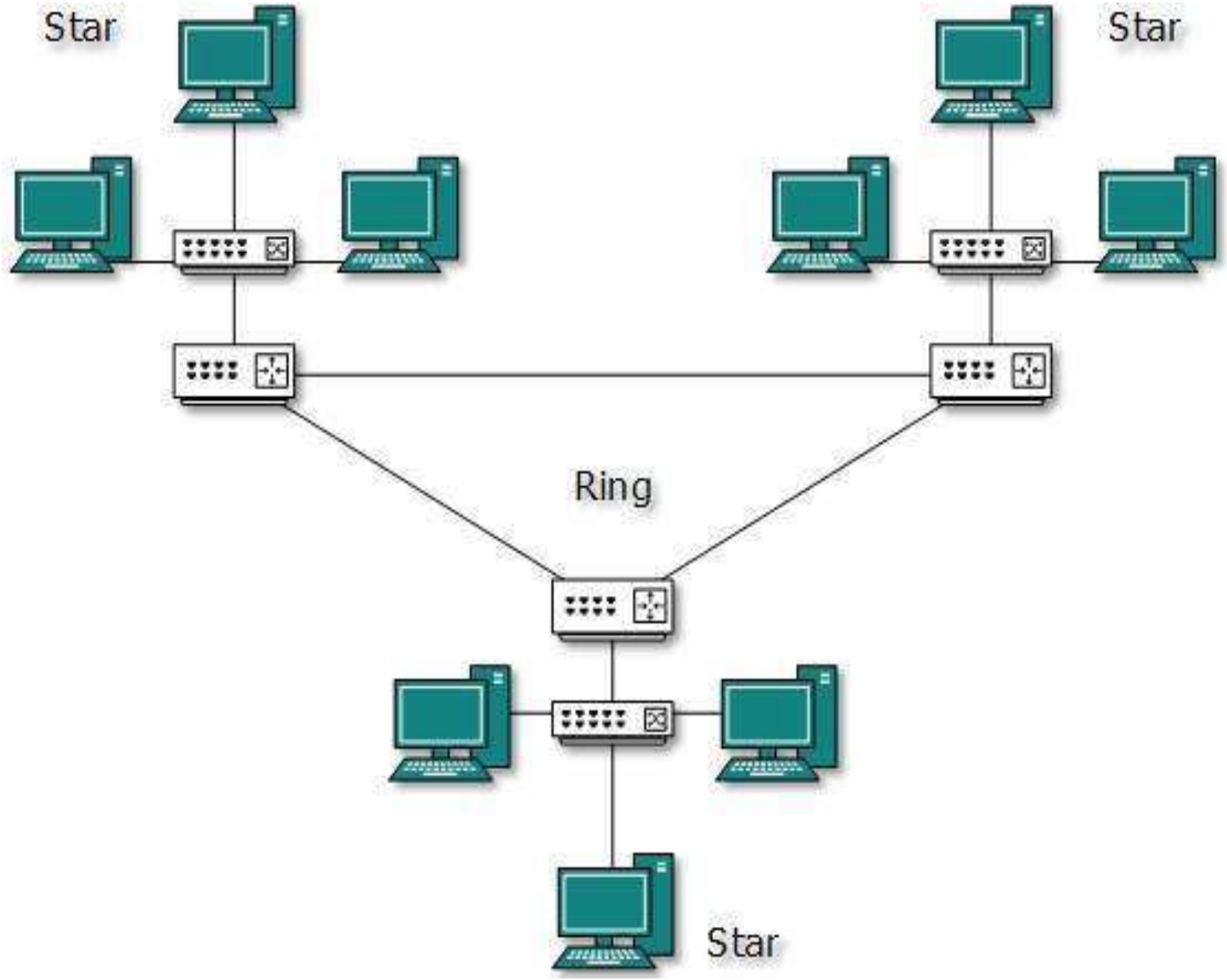
Daisy Chain

- This topology connects all the hosts in a linear fashion.
- Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts. i.e. if the end hosts in daisy chain are connected then it represents Ring topology.
- Each link in daisy chain topology represents single point of failure.
- Every link failure splits the network into two segments.
- Every intermediate host works as relay for its immediate hosts.



Hybrid Topology

- A network structure whose design contains more than one topology is said to be hybrid topology.
- Hybrid topology inherits merits and demerits of all the incorporating topologies.
- The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies.
- Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology


Star
Star
Ring
Star

Computer Network Switching

- Switching is process to forward packets coming in from one port to a port leading towards the destination.
- When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress.
- At broad level, switching can be divided into two major categories:
- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

Switching Techniques

- In large networks there might be multiple paths linking sender and receiver. Information may be switched as it travels through various communication channels. There are three typical switching techniques available for digital traffic.

  - Circuit Switching
  - Message Switching
  - Packet Switching

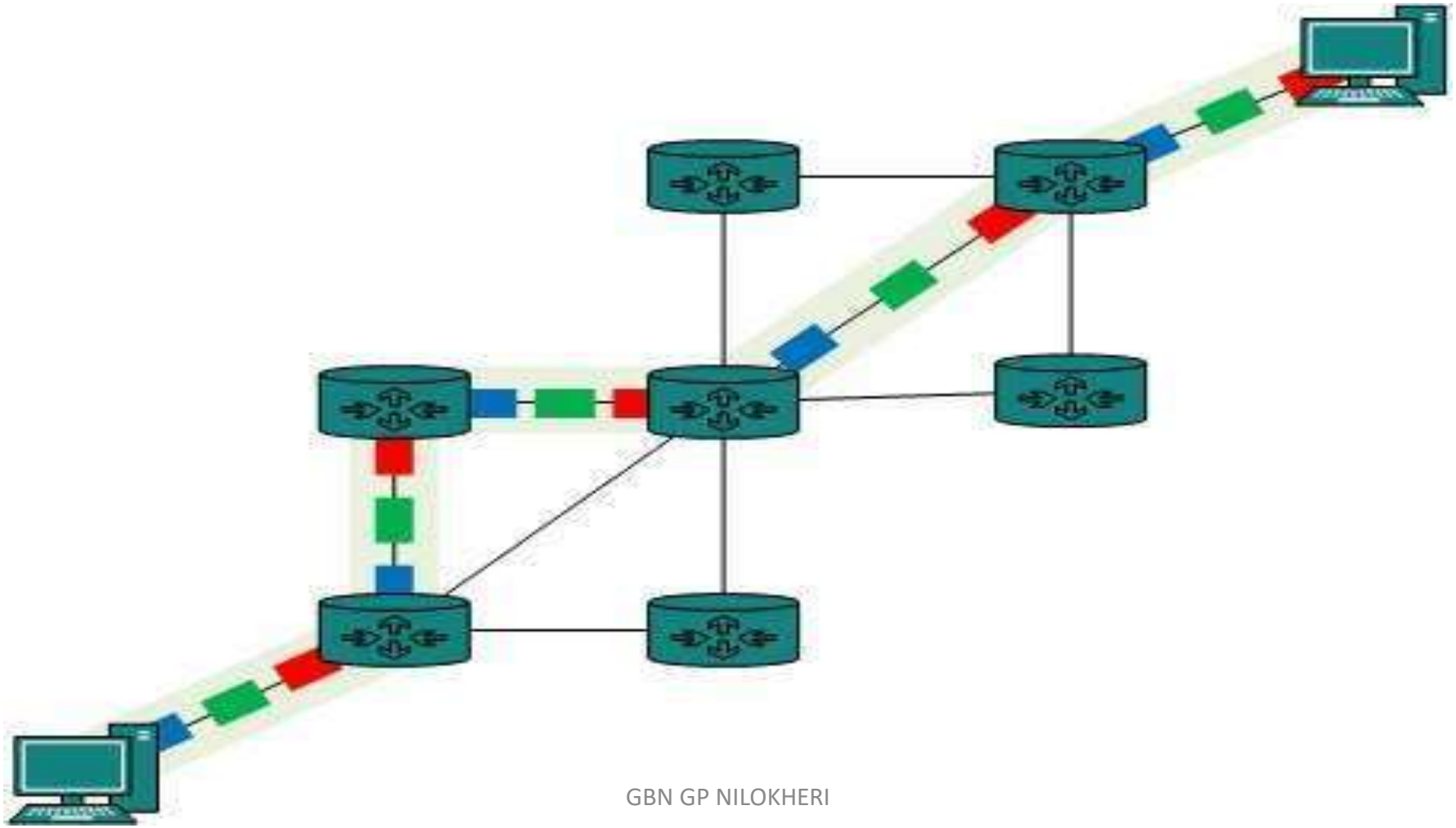
Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

- Establish a circuit
- Transfer the data
- Disconnect the circuit

- Circuit switching was designed for voice applications.
- Telephone is the best suitable example of circuit switching.
- Before a user can make a call, a virtual path between caller and callee is established over the network.



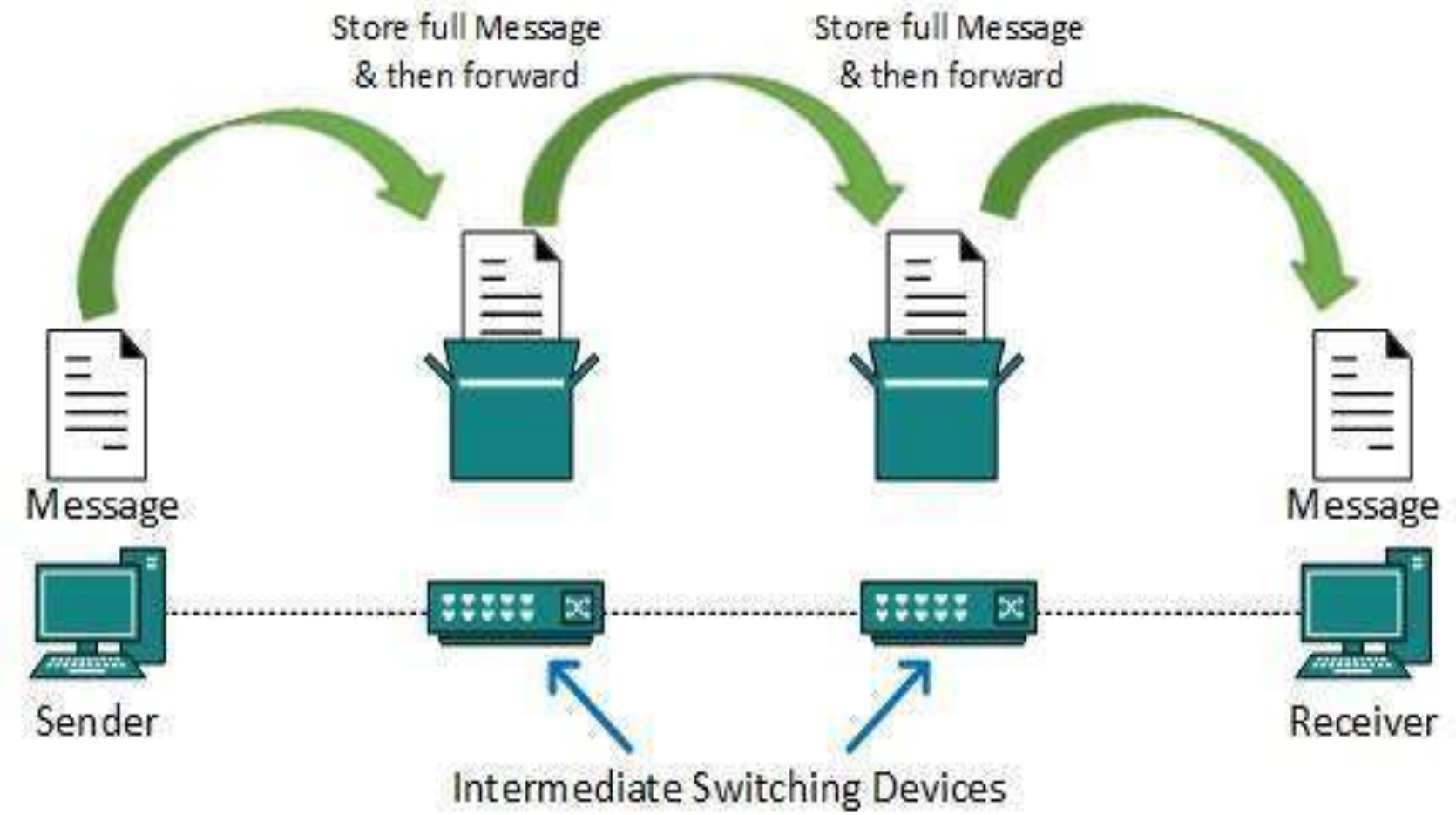
- **Advantages:**
  - The communication channel (once established) is dedicated.

- **Disadvantages:**
  - Possible long wait to establish a connection, (10 seconds, more on long- distance or international calls.) during which no data can be transmitted.
  - More expensive than any other switching techniques, because a dedicated path is required for each connection.
  - Inefficient use of the communication channel, because the channel is not used when the connected systems are not using it.

Message Switching

- This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.
- A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.
- Message switching is still used for electronic mail and telex transmission, it has largely been replaced by packet switching

- This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only.



Message Switching

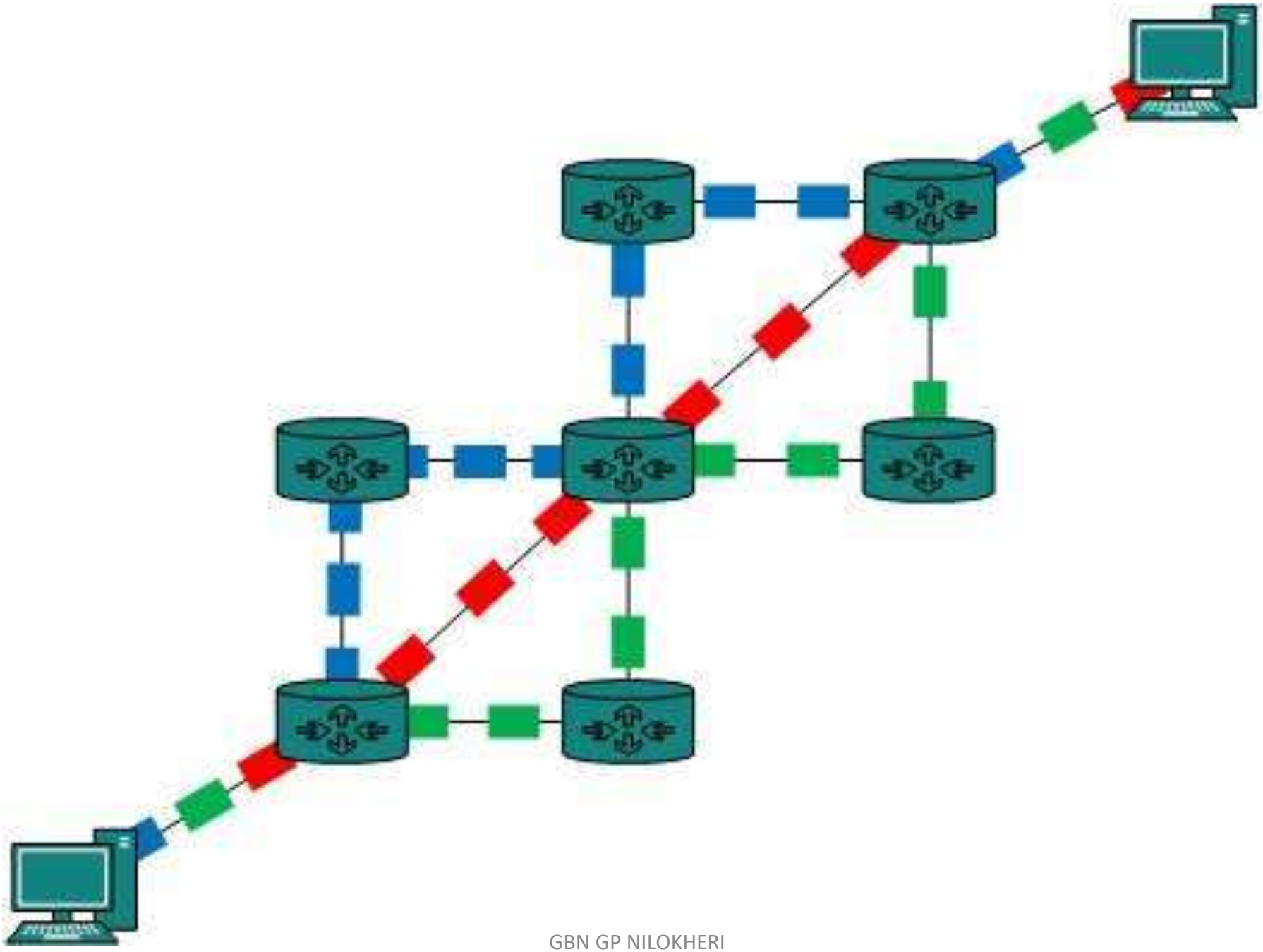
- **Advantages:**
  - Channel efficiency can be greater compared to circuit-switched systems, because more devices are sharing the channel.
  - Traffic congestion can be reduced, because messages may be temporarily stored in route.
  - Message priorities can be established due to store-and-forward technique.
  - Message broadcasting can be achieved with the use of broadcast address appended in the message.

Disadvantages

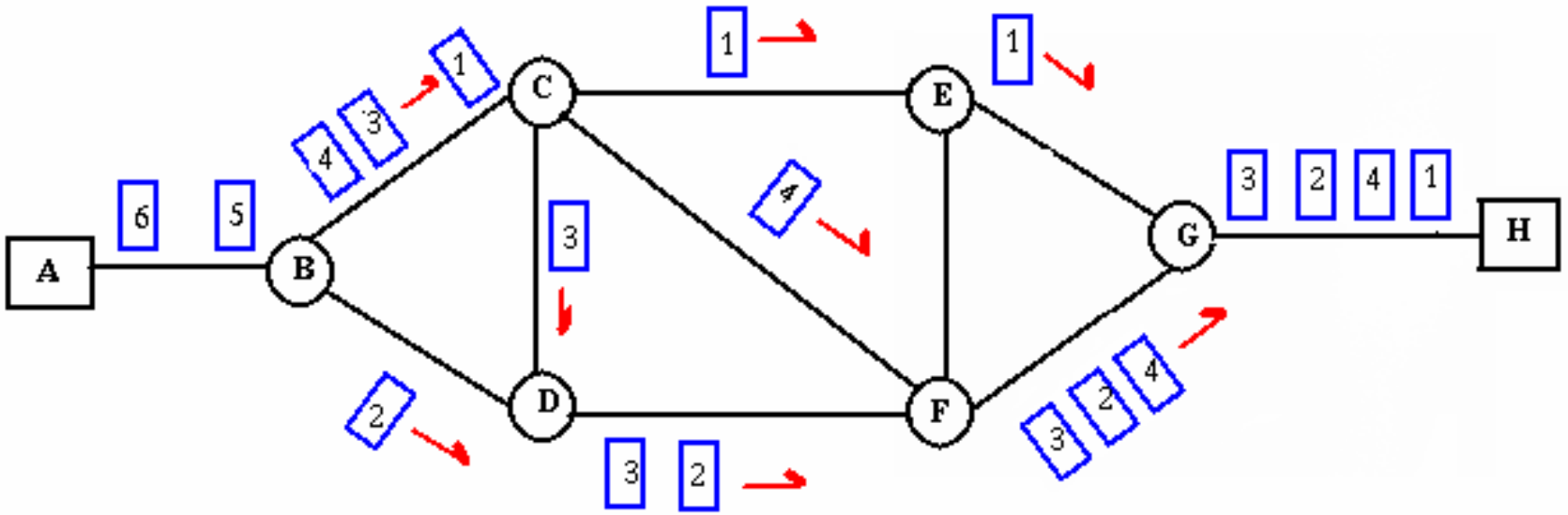
- Message switching is not compatible with interactive applications.
- Store-and-forward devices are expensive, because they must have large disks to hold potentially long messages.
- Message switching was not a solution for streaming media and real-time applications.

Packet Switching

- The entire message is broken down into smaller chunks called packets.
- The switching information is added in the header of each packet and transmitted independently.
- It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.
- **The internet uses packet switching technique.**



- *Packet switching* can be seen as a solution that tries to combine the advantages of message and circuit switching and to minimize the disadvantages of both.
- There are two methods of packet switching: Datagram and virtual circuit.



Packet Switching

Packet Switching: Datagram

- Datagram packet switching is similar to message switching in that each packet is a self-contained unit with complete addressing information attached.
- This fact allows packets to take a variety of possible paths through the network.
- So the packets, each with the same destination address, do not follow the same route, and they may arrive out of sequence at the exit point node (or the destination).
- Reordering is done at the destination point based on the sequence number of the packets.
- It is possible for a packet to be destroyed if one of the nodes on its way is crashed momentarily. Thus all its queued packets may be lost.

Packet Switching: Virtual Circuit

- In the virtual circuit approach, a preplanned route is established before any data packets are sent.
- A logical connection is established when
  - a sender send a "call request packet" to the receiver and
  - the receiver send back an acknowledge packet "call accepted packet" to the sender if the receiver agrees on conversational parameters.
- The conversational parameters can be maximum packet sizes, path to be taken, and other variables necessary to establish and maintain the conversation.
- Virtual circuits imply acknowledgements, flow control, and error control, so virtual circuits are reliable.

- In virtual circuit, the route between stations does not mean that this is a dedicated path, as in circuit switching.
- A packet is still buffered at each node and queued for output over a line.
- The difference between virtual circuit and datagram approaches:

➢ With virtual circuit, the node does not need to make a routing decision for each packet.

➢ It is made only once for all packets using that virtual circuit.

VC's offer guarantees that

- the packets sent arrive in the order sent
- with no duplicates or omissions
- with no errors (with high probability)

regardless of how they are implemented internally.

Advantages of packet switching

- Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.
- Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).
- Packet can be rerouted if there is any problem, such as, busy or disabled links.
- The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth.

Disadvantages of packet switching

- Protocols for packet switching are typically more complex.
- It can add some initial costs in implementation.
- If packet is lost, sender needs to retransmit the data.
- Another disadvantage is that packet-switched systems still can’t deliver the same quality as dedicated circuits in applications requiring very little delay - like voice conversations or moving images.