

CS - 21

Network Technology And Administration

Ch - 1

Basics of Network

Contents..

● Network Concept

- What is Network?
- Use of Network.

● Network Model

- Peer-to-Peer
- Client - Server

● Network Services

- File Service
- Print Service
- Communication Service
- Database Service
- Security Service
- Application Service

Contents..

● Network Access Methods

- CSMA/CD, CSMA/CA
- Token Passing
- Polling

● Network Topologies

- Bus, Star, Tree, Ring, Mesh, Hybrid

● Advanced Network Topologies

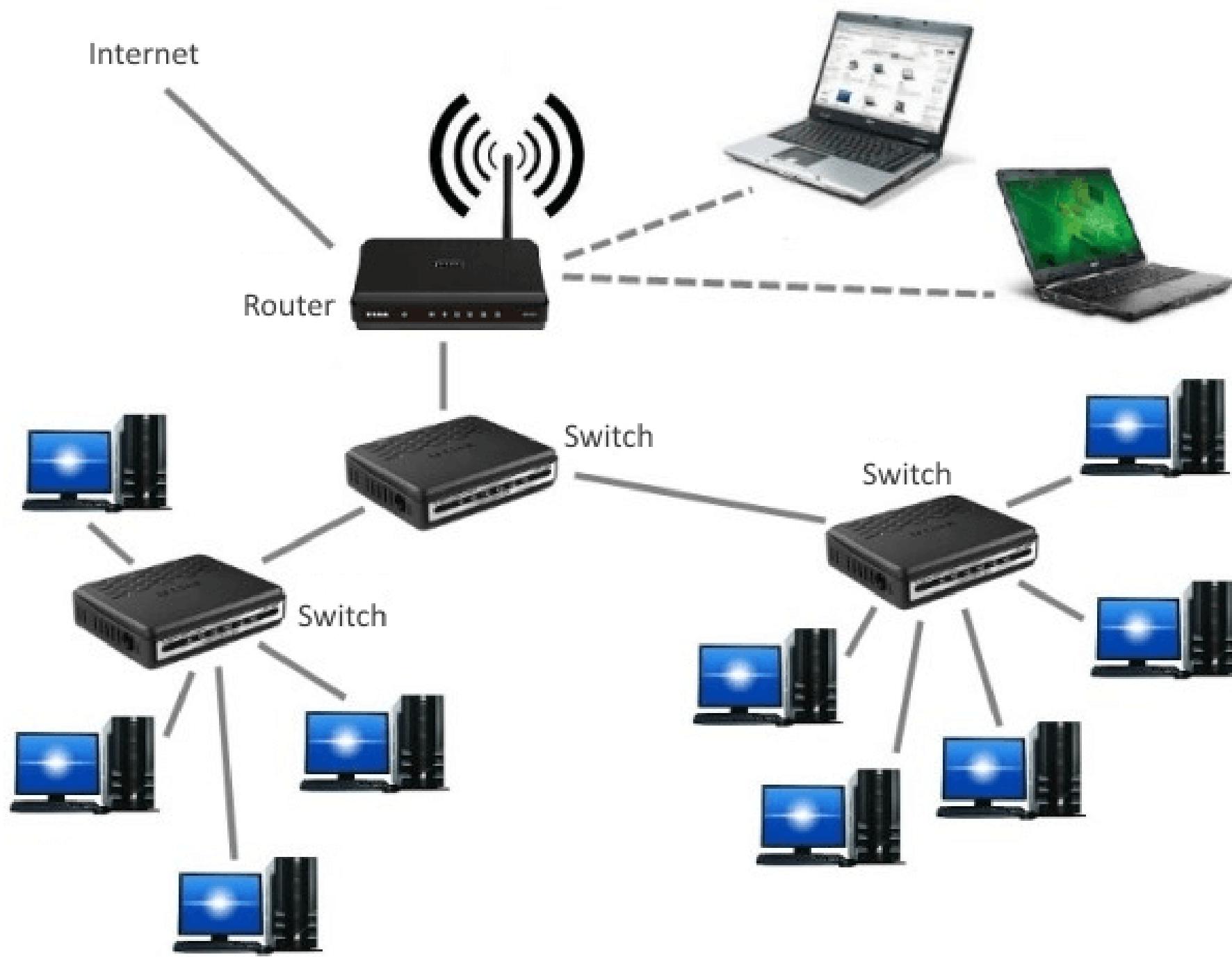
- Ethernet
- CDDI
- FDDI

● Communication Methods

- Unicasting
- Multicasting
- Broadcasting

● Computer Network :

- A computer network is a collection of two or more computer systems that are linked together.
- In other words, a computer network is a system that connects numerous independent computers in order to share information (data) and resources.
- The integration of computers and other different devices allows users to communicate more easily.
- A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.
- A computer network consists of various kinds of nodes. Servers, networking hardware, personal computers, and other specialized or general-purpose hosts can all be nodes in a computer network. Hostnames and network addresses are used to identify them.



➤ Use of Computer Network:

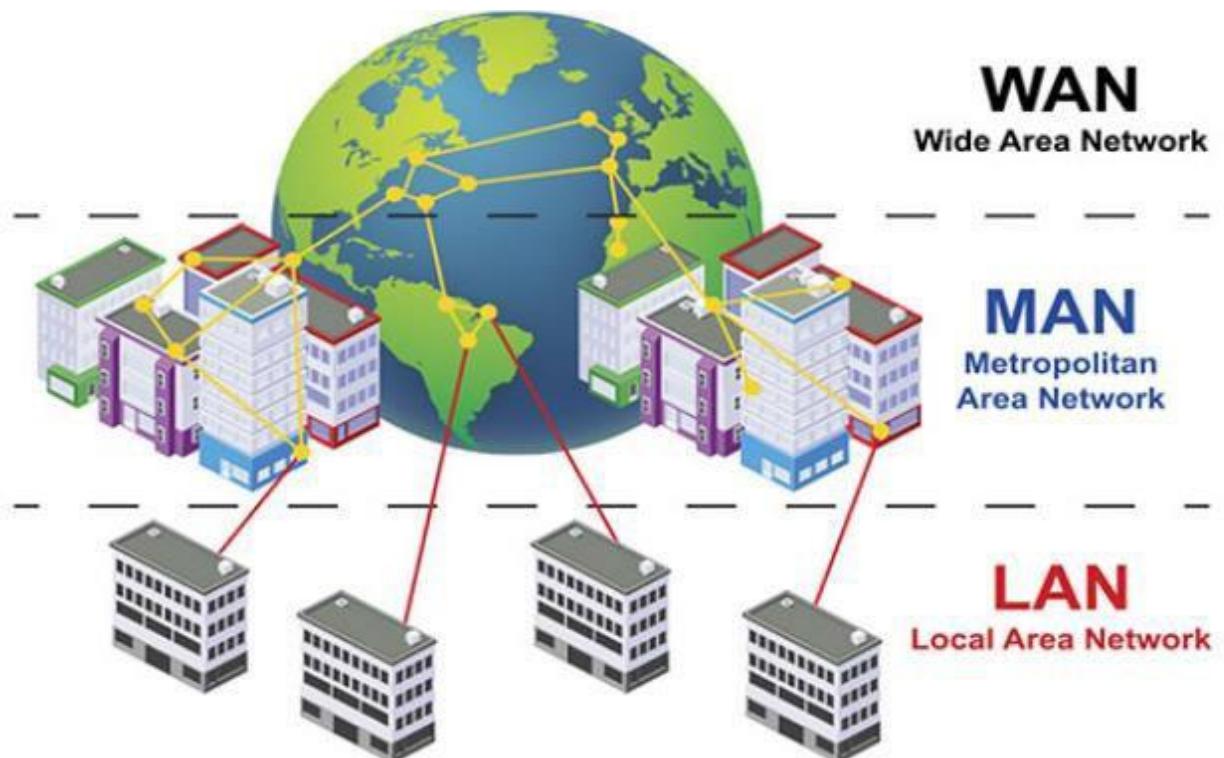
→ Computer networks have a variety of uses that many would see as essential today, including the following:

- **File sharing:** Which enables users to share data files through a network.
- **Application sharing:** Which enables users to share applications through a network.
- **Hardware sharing:** Which enables users in a network to share hardware devices, such as printers and hard drives.
- **Client-server model:** Which enables data to be stored on servers, where end-user devices or clients can access that data.
- **Voice Over IP (VoIP):** Which enables users to send voice data through internet protocols
- **Communication:** Which can include video, text and voice.
- **E-commerce:** Which enables users to sell and buy products over the internet.
- **Gaming:** Which enables multiple users to play together from various places.

○ Type of Computer Network:

→ A computer network can be categorized by their size. A **computer network** is mainly of **four types**:

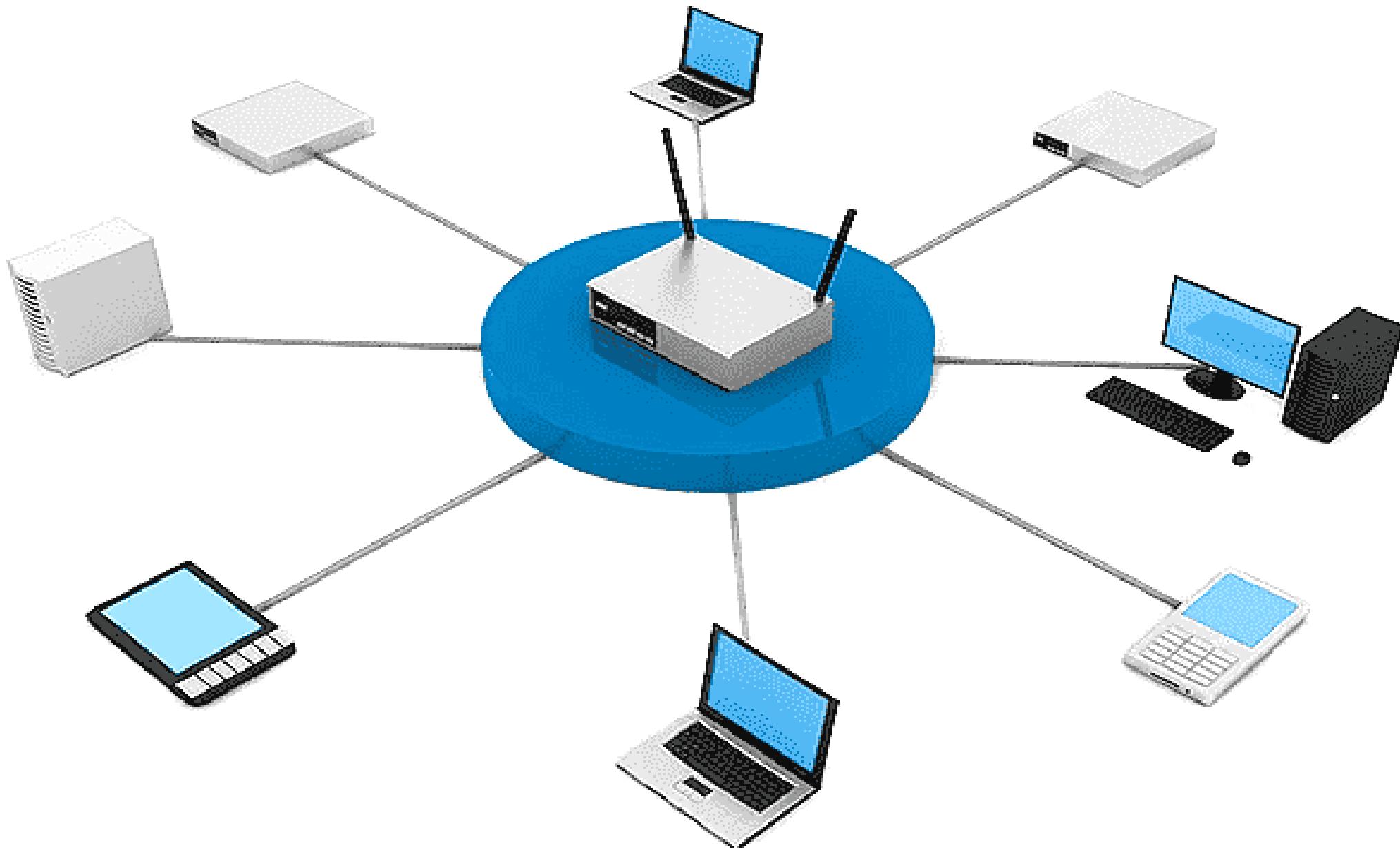
1. LAN(Local Area Network)
2. PAN(Personal Area Network)
3. MAN(Metropolitan Area Network)
4. WAN(Wide Area Network)



► LAN(Local Area Network):

- Local Area Network is a group of computers connected to each other in a small area such as building, office, compound etc.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.
- A LAN is a network that covers an area of around 10 kilometers. Depending upon the needs of the organization, a LAN can be a single office, building, or Campus. We can have two PCs and one printer in-home office or it can extend throughout a company and include audio and video devices.

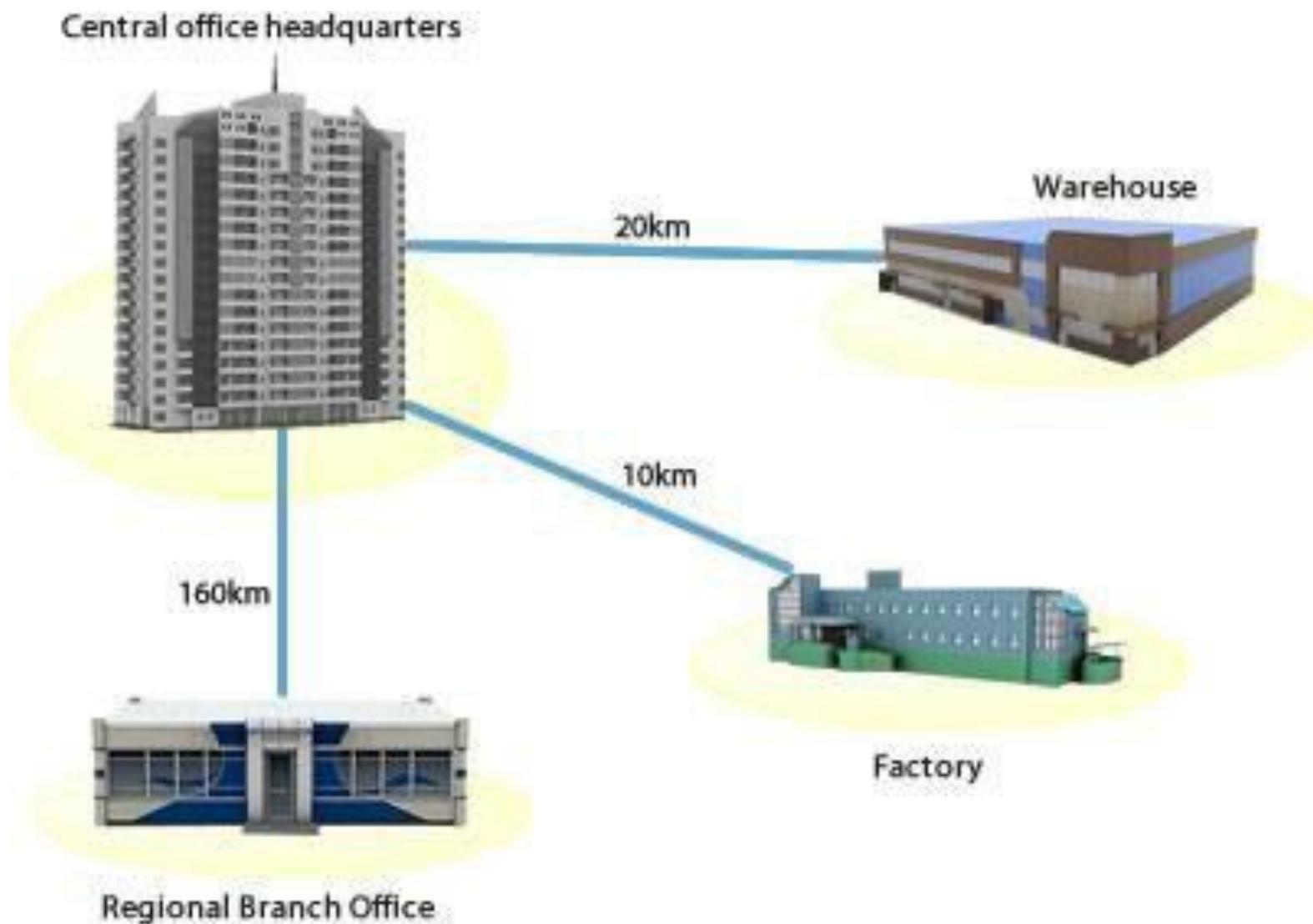
LAN(Local Area Network):



➤ MAN(Metropolitan Area Network):

- ➔ A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- ➔ MAN refers to a network that covers an entire city. For example: consider the cable television network.
- ➔ Government agencies use MAN to connect to the citizens and private industries.
- ➔ In MAN, various LANs are connected to each other through a telephone exchange line.
- ➔ It has a higher range than Local Area Network (LAN).

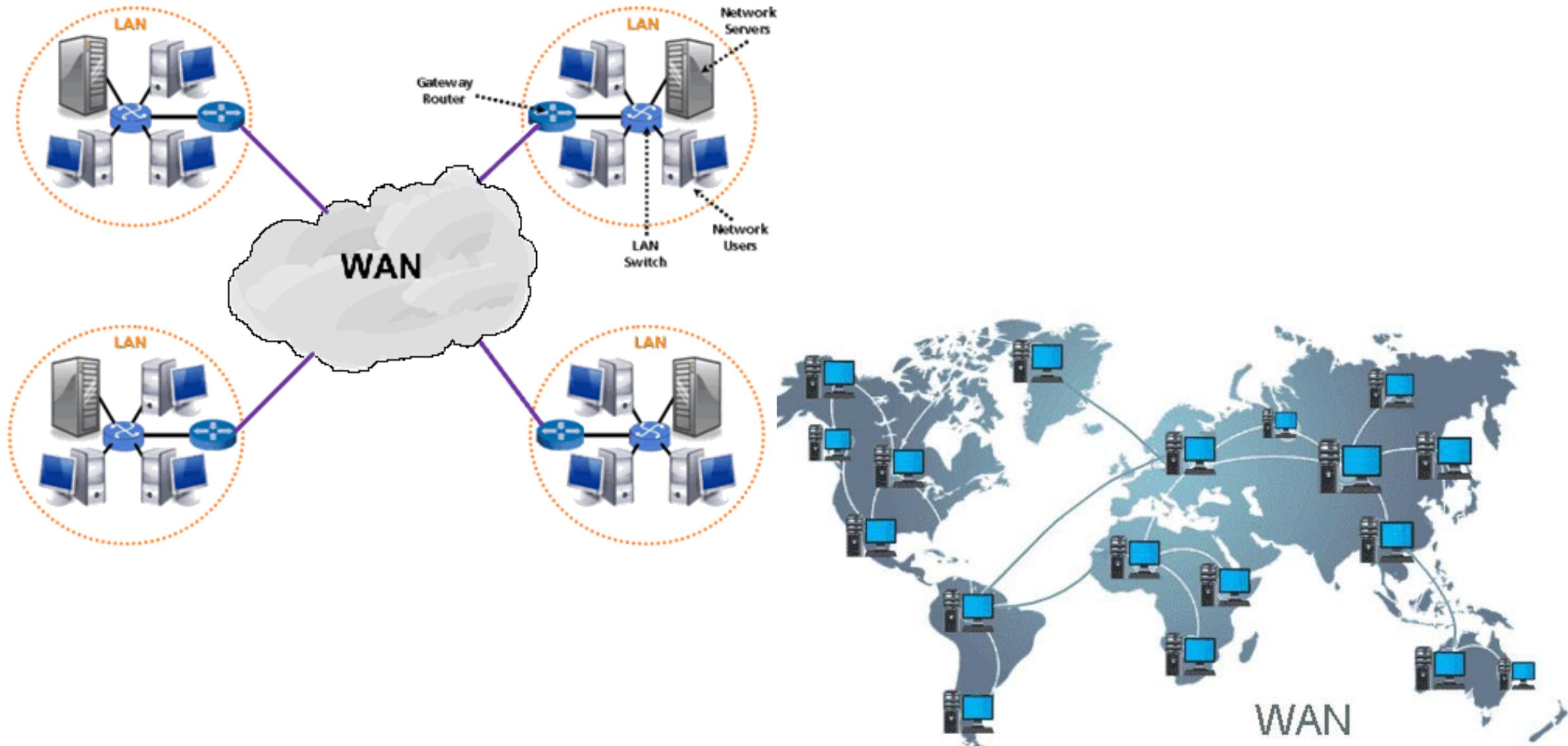
MAN(Metropolitan Area Network):



➤ WAN(Wide Area Network):

- ➔ WAN refers to a network that connects countries or continents. For example, the Internet allows users to access a distributed system called www from anywhere around the globe.
- ➔ A Wide Area Network is quite bigger network than the LAN and MAN.
- ➔ A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- ➔ The internet is one of the biggest WAN in the world.
- ➔ A Wide Area Network is widely used in the field of Business, government, and education.

WAN (Wide Area Network):



➤ PAN(Personal Area Network):

- ➔ Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- ➔ Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- ➔ *Thomas Zimmerman* was the first researcher scientist to bring the idea of the Personal Area Network.
- ➔ Personal Area Network covers an area of 30 feet.
- ➔ Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

PAN(Personal Area Network):

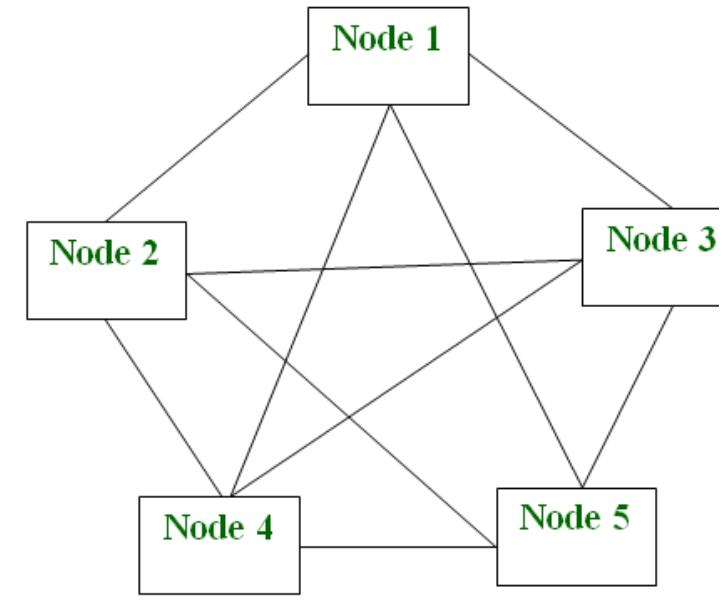


● Network Model:

- Peer-to-Peer (P2P) model: Here each computer acts as a node for file sharing within the formed network. Each node acts as a server and thus there is no central server in the network.
- ➔ This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes.
- ➔ Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.
- ➔ These networks do not involve a large number of nodes, usually less than 12. All the computers in the network store their own data but this data is accessible by the group.
- ➔ It requires specialized software. It allows resource sharing among the network.
- ➔ Since the nodes act as clients and servers, there is a constant threat of attack.
- ➔ Almost all OS today support P2P networks.

Network Model:

- P2P Network Architecture
 - Each computer in the network has the same set of responsibilities and capabilities.
 - Each device in the network serves both a client and server.
 - Each computer in the network has the ability to share data with other computers in the network.

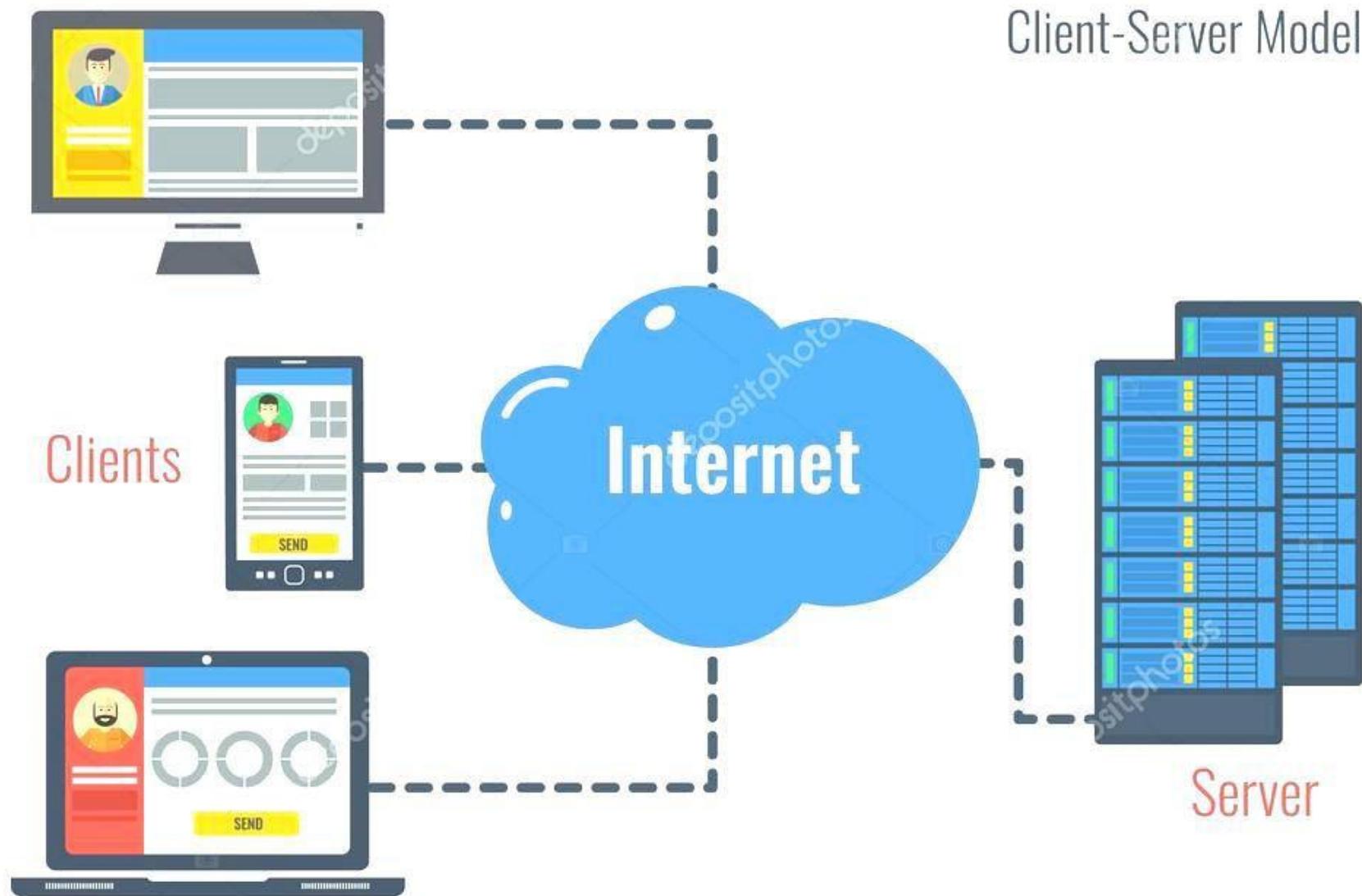


P2P Architecture

➤ Client – Server model:

- ➔ The Client-server model is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients.
- ➔ In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and deliver the data packets requested back to the client.
- ➔ Clients do not share any of their resources. Examples of Client-Server Model are Email, World Wide Web, etc.
- ➔ **Client:** In the digital world a client is a computer (Host) i.e., capable of receiving information or using a particular service from the service providers (Servers).
- ➔ **Server:** When we talk the word Servers, it means a person or medium that serves something. Similarly in this digital world a Server is a remote computer which provides information (data) or access to particular services.

► Client – Server model:



● Network Services:

➤ File Service:

→ File services include sharing and transferring files over the network.

➤ **File Sharing:**

→ One of the reasons which gave birth to networking was file sharing. File sharing enables its users to share their data with other users.

→ User can upload the file to a specific server, which is accessible by all intended users.

→ As an alternative, user can make its file shared on its own computer and provides access to intended users.

➤ **File Transfer:**

→ This is an activity to copy or move file from one computer to another computer or to multiple computers, with help of underlying network.

→ Network enables its user to locate other users in the network and transfers files.

Network Services:

> Communication Service:

- **Email:** When a user sends email to other user, it is actually transferred between users with help of email server.
- **Social Networking:** The computer savvy peoples, can find other known peoples or friends, can connect with them, and can share thoughts, pictures, and videos.
- **Remote Access:** This service enables user to access the data residing on the remote computer. This feature is known as Remote desktop.
- **Internet Chat:** Internet chat provides instant text transfer services between two hosts. Two or more people can communicate with each other using text-based Internet Relay Chat services. These days, voice chat and video chat are very common.

Network Services:

➤ Application Service:

- Any client computers send the request to statistics server. When the result becomes available, they are returned to the client.
- This way only one computer in an organization needs to have the expensive software and processing power required to calculate the statistics but all client computer can benefited.
- Through the help of specific applications / software, client which is less powerful computer, requests to the application server which is very powerful computer for specific task to accomplished. Server then take the request, process it and generates the result and return it to the client.

➤ Print Service:

Print services enable sharing of printer amongst many devices.

- Because of the printer is shared with multiple devices, through the print service anyone can save the additional cost in a network of office or organization.

Network Services:

➤ Security Service:

- Security service is critical because it prevents cybercriminals from gaining access to valuable data and sensitive information.
- When users share resources and data on a network, they should be able to control who can access the data or resource and what the user can do with it. Who is able to read and change the file also is a crucial consideration.
- Network security is enforced using a combination of hardware and software tools.
The primary goal of network security is to prevent unauthorized access into or between parts of a network.

➤ Database Service:

- Database stores data and information, processes it, and enables the users to retrieve it efficiently by using queries.
- Databases help organizations to make decisions based on statistics.

● Network access methods:

→ Network access methods are some techniques which specifies the way how can we access the network for storing and retrieving data from the any computer network. There are mainly three methods to access network as under:

➤ CSMA / CD:

- Carrier Sense Multiple Access / (with)Collision Detection is a method or protocol to accessing network which detects the clashes or accident (collision) of data.
- Whenever a frame in the CSMA is transferred, the station will sense the channel to verify if it's free or not. In case of a free channel, the station passes the frame.
- Sometimes, another station may also transfer the frame same time, thus resulting in a collision (clashes) of both.
- In this scenario, the station will cause a round-trip propagation delay (wait) for an acknowledgement post the transfer for CSMA. However, for CSMA/ CD, time taken for this can also be brought down.

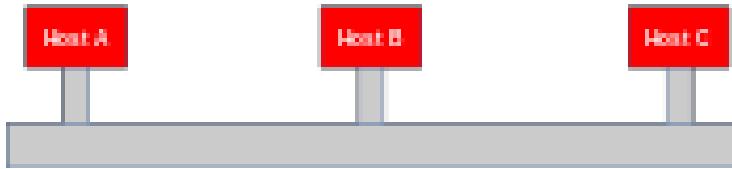
Network access methods:

How Does CSMA/CD Work?

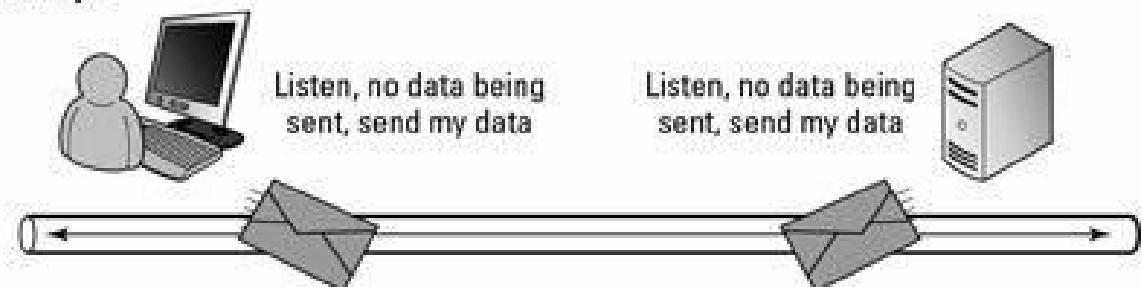
- Some nodes in CSMA/CD pass the frame first to confirm that there is a free link / channel.
 - If the channel is free then node can transfer information and listen again.
 - The node also observes the line for very high voltages, thus indicating a collision.
 - On detecting a collision, the node leaves the transfer, waiting until link is free.
 - The node from where the frame is transferred can also release a jam signal in order to reveal that a collision has taken place.
- ## Features:
- Upon identifying the collision, stations have to wait for sometime before transferring the frames.
 - Meanwhile, they can utilize a jam signal to indicate to the other stations that a collision has occurred, and so these stations have to wait.
 - Also, a priority mechanism is applied for a transmission priority that is high.

Network access methods:

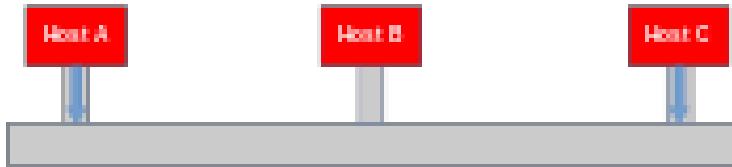
1) Carrier Sense



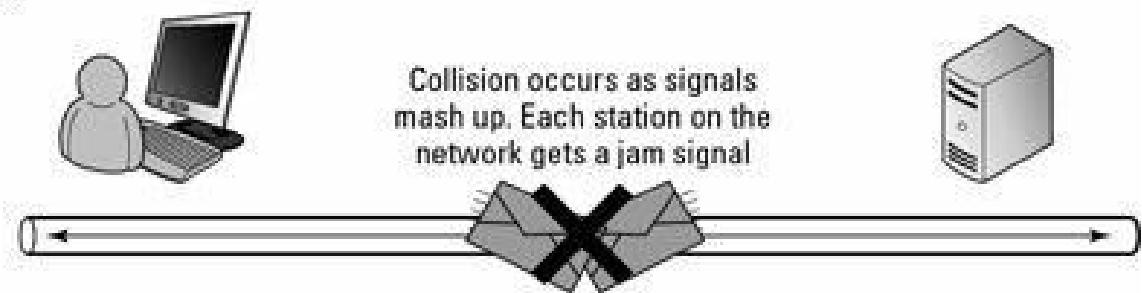
First attempt



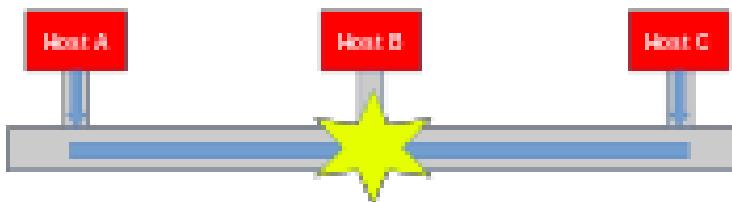
2) Multiple Access



Failure



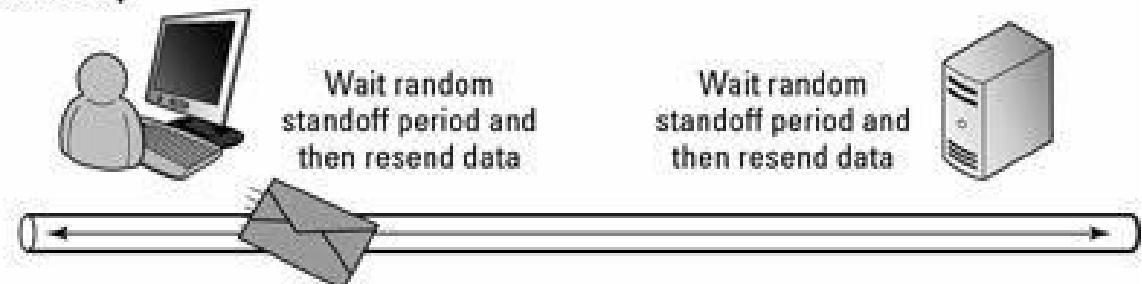
3) Collision



4) Collision Detection (Back off Algorithmus)



Second attempt



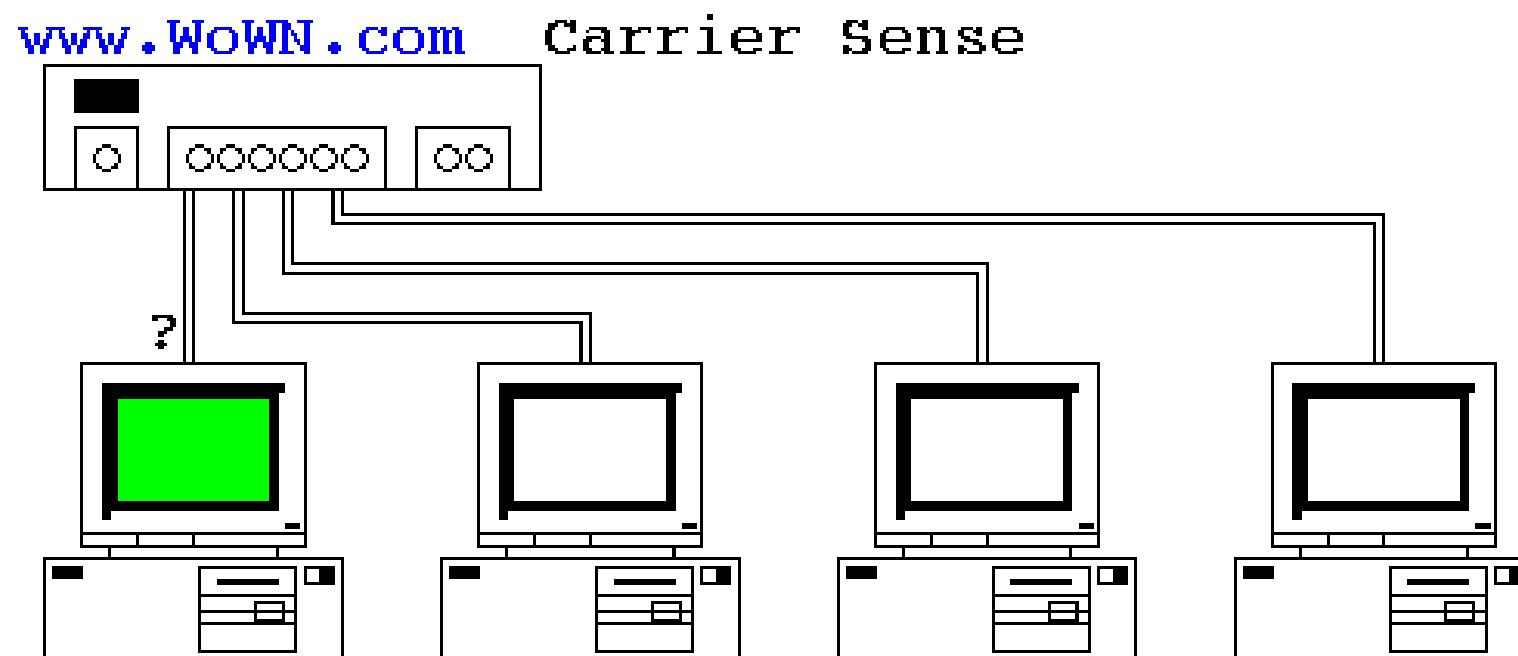
Network access methods:

➤ CSMA / CA:

- Carrier Sense Multiple Access / (with)Collision Avoidance is a method or protocol to accessing network which detects the clashes or accident (collision) of before the data is transferring and if clashes occur then avoids it.
- It was developed to minimize the potential of a collision occurring when two or more stations send their signals over a data link layer.
- In this scenario, CSMA requires each station to first check the state of the medium before initiating a transmission. This helps to avoid potential collisions by listening to the broadcasting nodes and then informing devices to transmit when the channel is free.
- For example, as soon as a node receives a packet to transmit across the network, it will check to ensure the channel is clear and no other node is transmitting at the same time. If the network channel is idle, the packet is sent.

Network access methods:

- If the channel is not clear, the node waits for a randomly chosen period of time in microseconds and then checks again to see if the channel is clear. This is called the backoff factor and is counted down using a backoff counter.
- If the channel is idle when the backoff counter reaches zero, the node transmits the packet. If the channel is not clear when the backoff counter reaches zero, the backoff factor will reset itself and repeat the process.



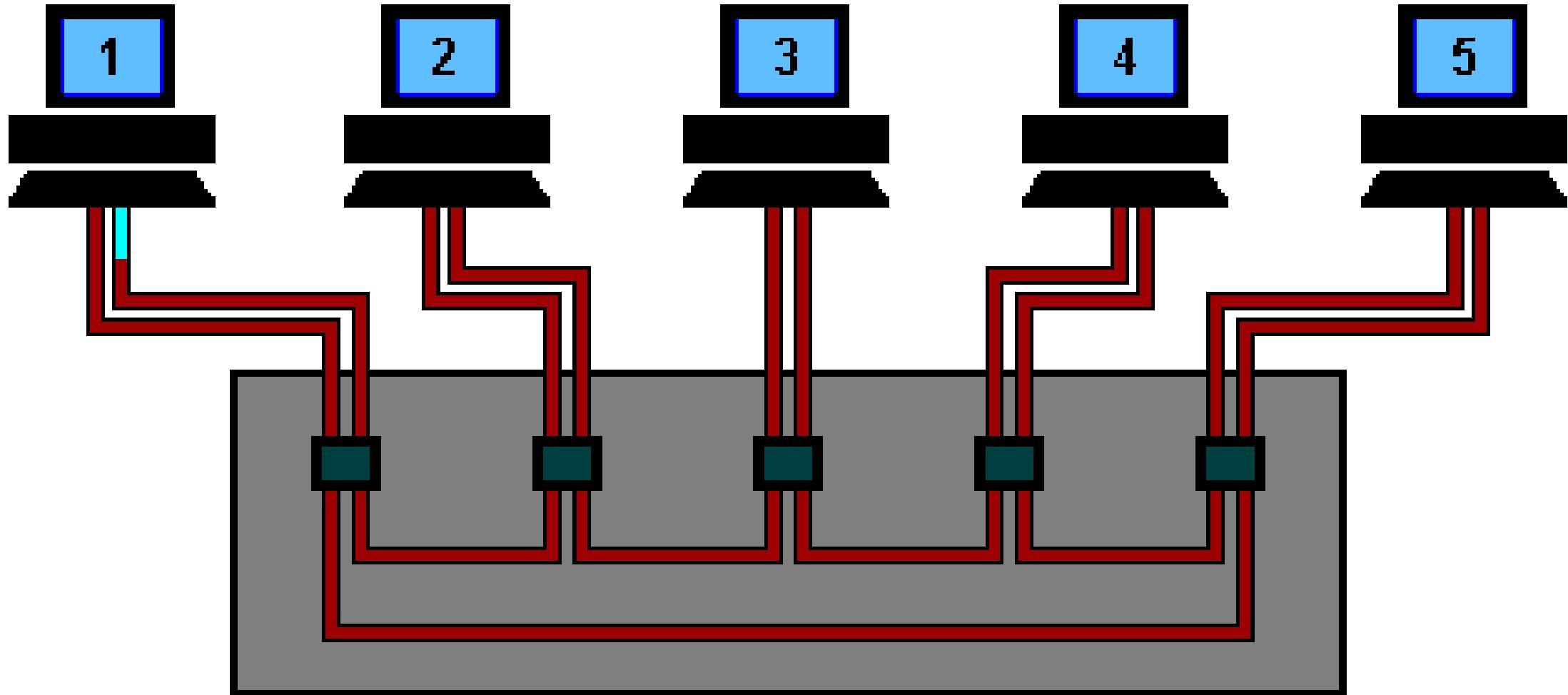
Network access methods:

➤ Token Passing:

- The token ring topology uses an access method called token passing. For any station on the ring to transmit, it must first have a token.
- The Token-Passing is a protocol depends on a control signal called the token.
- A token is a 24-bit packet that circulates throughout the network from NIC to NIC in an orderly fashion.
- If a workstation wants to transmit a message, first it must seize the token. At that point, the workstation has complete control over the communications channel.
- The existence of only one token eliminates the possibility of signal collisions. This means that only one station can speak at a time.
- Token rings reduce the chances of data collision.
- Token passing performs better than bus topology under heavy traffic.
- A server is not needed to control connectivity among the nodes.

Network access methods:

➤ Token Passing:



Network access methods:

➤ Polling:

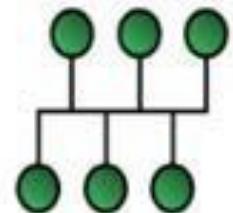
- In electronic communication, 'polling' is the continuous checking of other programs or devices by one program or device to see what state they are in, usually to see whether they are still connected or want to communicate.
- Specifically, in multipoint or multidrop communication (a controlling device with multiple devices attached that share the same line), the controlling device sends a message to each device, one at a time, asking each whether it has anything to communicate (in other words, whether it wants to use the line).
- Polling activity gives a chance to those devices who wants to share something into shared transmission line. The device who elected by poll to transfer the data, the only device can transfer their data on into the transmission line.

● Network Topology:

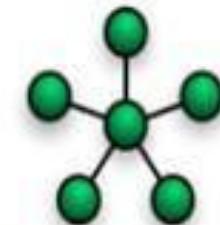
→ Topology defines the structure of the network of how all the components are interconnected to each other.

→ There are mainly five types of Network topology:

1. Bus Topology
2. Star Topology
3. Ring Topology
 - Single Ring
 - Double Ring
4. Tree Topology
5. Mesh Topology
 - Full Mesh
 - Partial Mesh

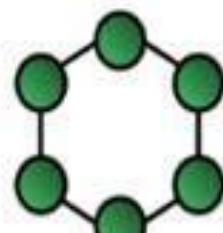


BUS Topology

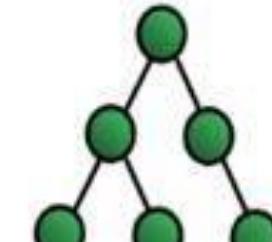


STAR Topology

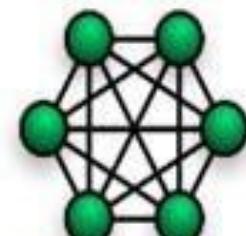
**Network
Topology**



RING Topology



TREE Topology



MESH Topology

➤ Bus Topology:

- ➔ Bus topology is simplest way of organizes network. In bus topology all computer are connected to the same transmission line by using coaxial cable.
- ➔ The word bus means all devices / nodes joint in single straight cable call backbone.
- ➔ In bus topology both end of the main cable needs to be terminated, if there is no terminator the signal will bounce from the end and hence collision of signal and noise generates.

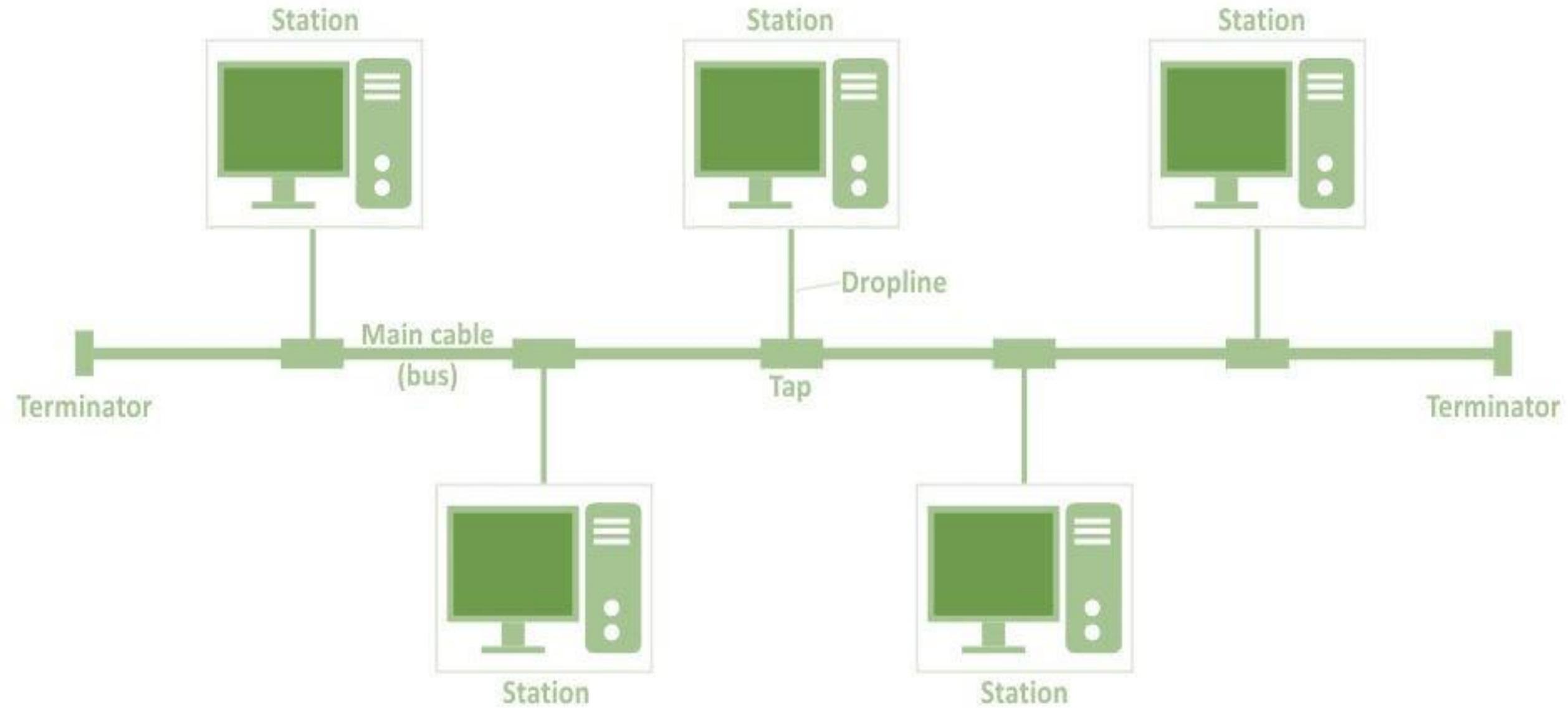
• Advantages:

- ➔ Easy to connect a computer to the single linear cable.
- ➔ Required less cable compare to star topology.
- ➔ Cost effective compared to other topologies.

• Disadvantages:

- ➔ The entire network will fail if backbone fail.
- ➔ Terminator required at the both end of the cable.

Bus Topology



➤ Star Topology:

- ➔ Star topology mostly use in LAN. Star topology can be implemented at home, offices and small organization.
- ➔ All computer in star topology is connected to central device like hub, switch or connector.
- ➔ Computer in network is connected with hub or switch through STP or UTP cable.

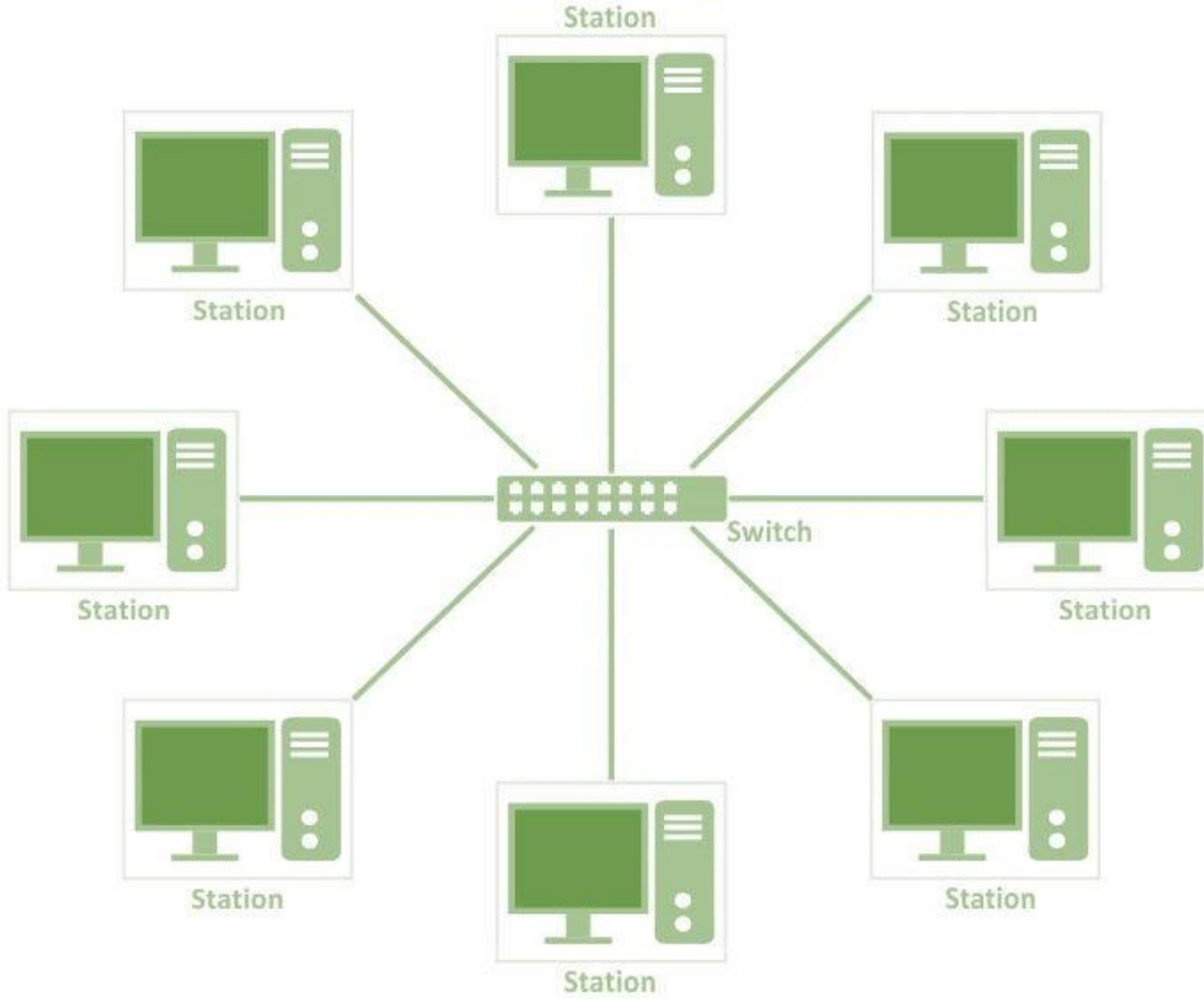
- **Advantages:**

- ➔ Easy to install and removing device from network.
- ➔ If one of the cable or wire fail then entire network will not affected.
- ➔ Easy to detect fault.

- **Disadvantages:**

- ➔ Required more cable compare to linear/bus topology.
- ➔ If hub switch connector fail then entire network will fail.
- ➔ More expensive than linear bus because of cost of hub and switch.

Star Topology



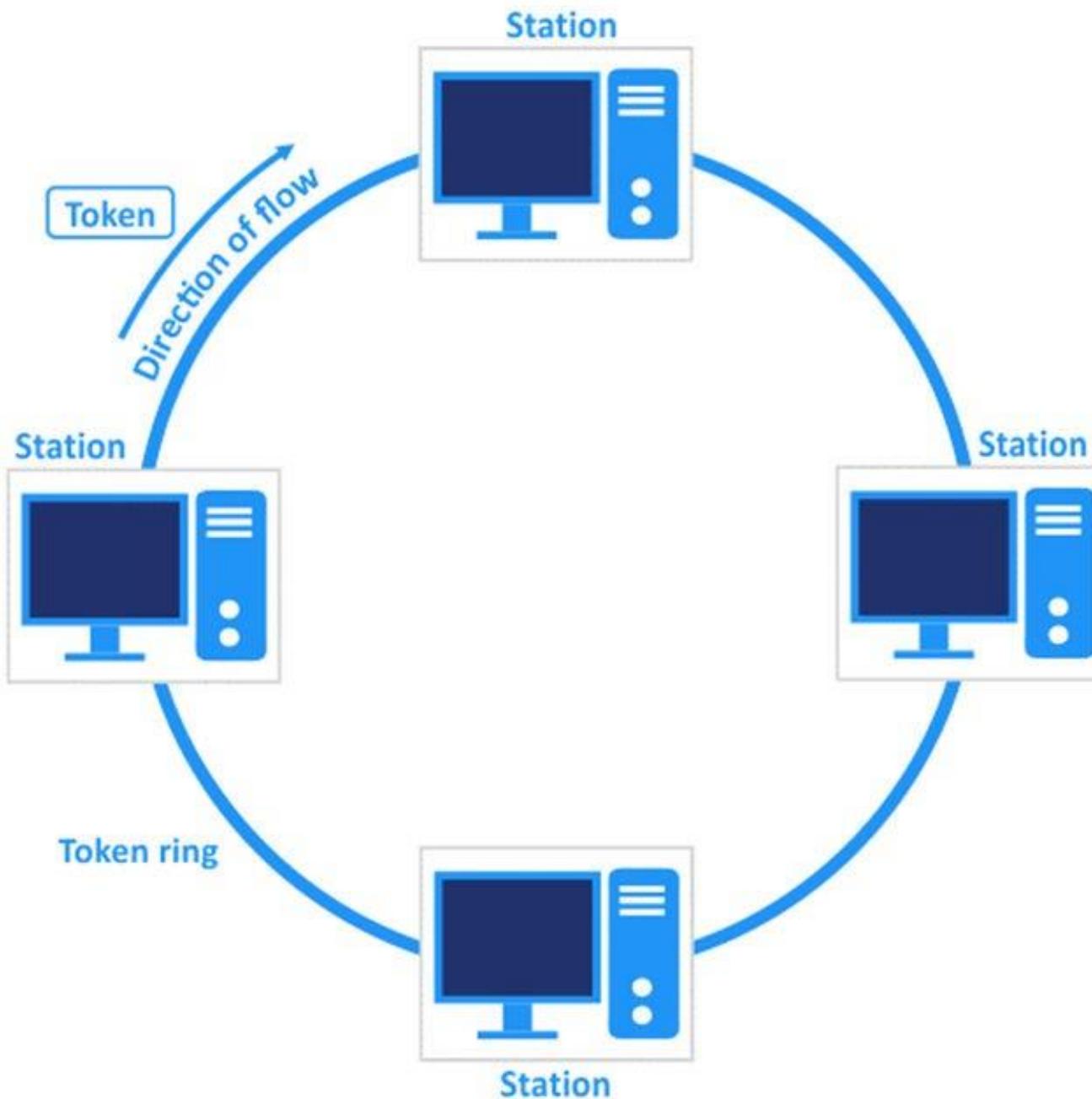
➤ **Ring Topology:**

- ➔ In Ring Topology all the devices are connected in ring manner.
- ➔ In ring topology every device has neighbor for communication purpose.
- ➔ There are two types of Ring topologies:

➤ **Single Ring:**

- ➔ In single ring topology, Message travel throw a ring in the same direction only it may be either clockwise or anti-clockwise.
- ➔ Single Ring Topologies are referred to as one-way or unidirectional ring networks.
- ➔ If any of the computer fails, the entire network will be disturbed. As Single Ring Topology transmits data in one-way or half-duplex manner.

Single Ring Topology

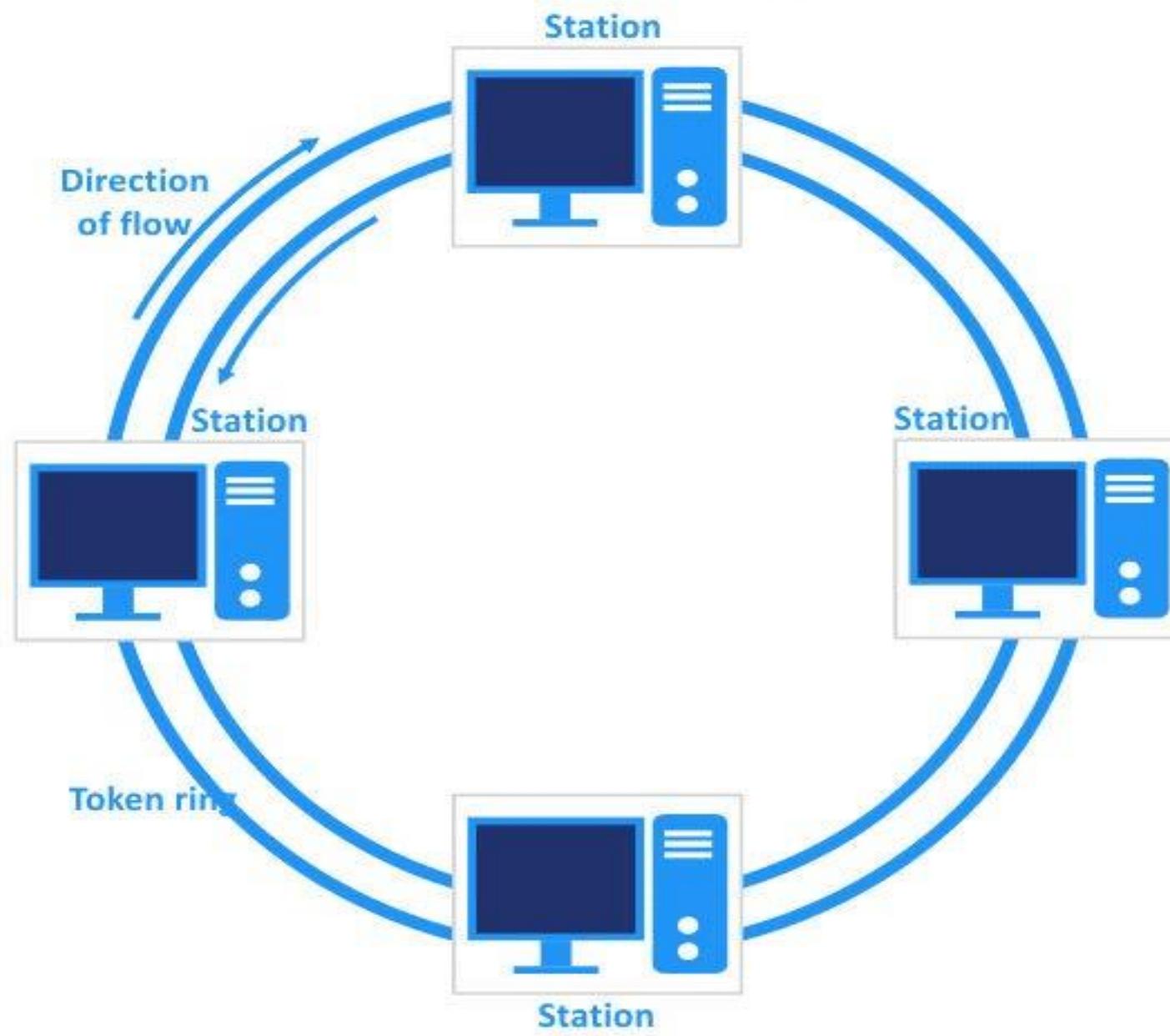


Ring Topology:

➤ Double / Dual Ring:

- ➔ In double ring topology we use two rings instead of single ring.
- ➔ If one of the rings is fail than another ring will transfer message.
- ➔ Here, first ring is works as clockwise data transfer and another ring is works as an anti-clockwise data transfer.
- ➔ If any of the computer fails, the entire network will not be disturbed. As double Ring Topology transmits data in two-way or full-duplex manner.
- ➔ It is also known as bi-directional ring topology.

Dual Ring Topology



Ring Topology:

- **Advantages:**

- Equal access to the resources.
- There is no need of server to control the connectivity among the nodes in the topology.
- It is cheap to install and expand.
- Minimum collision.
- Speed to transfer the data is very high in this type of topology.

- **Disadvantages:**

- It is slower in performance as compared to the bus topology
- It is Expensive.
- Difficult to troubleshoot the ring.

➤ Tree Topology:

- ➔ As the name suggests, tree topology forms a tree like structure of devices.
- ➔ Tree topology is a combination of two topology linear/ Bus topology and Star topology.
- ➔ Sometimes it is also called hierarchical topology as in this topology, all elements are arranged like the branches of a tree.
- ➔ When you have a multi-floor / multi-departmental building and wish to establish clusters at each section of the network, you can utilize tree topology.

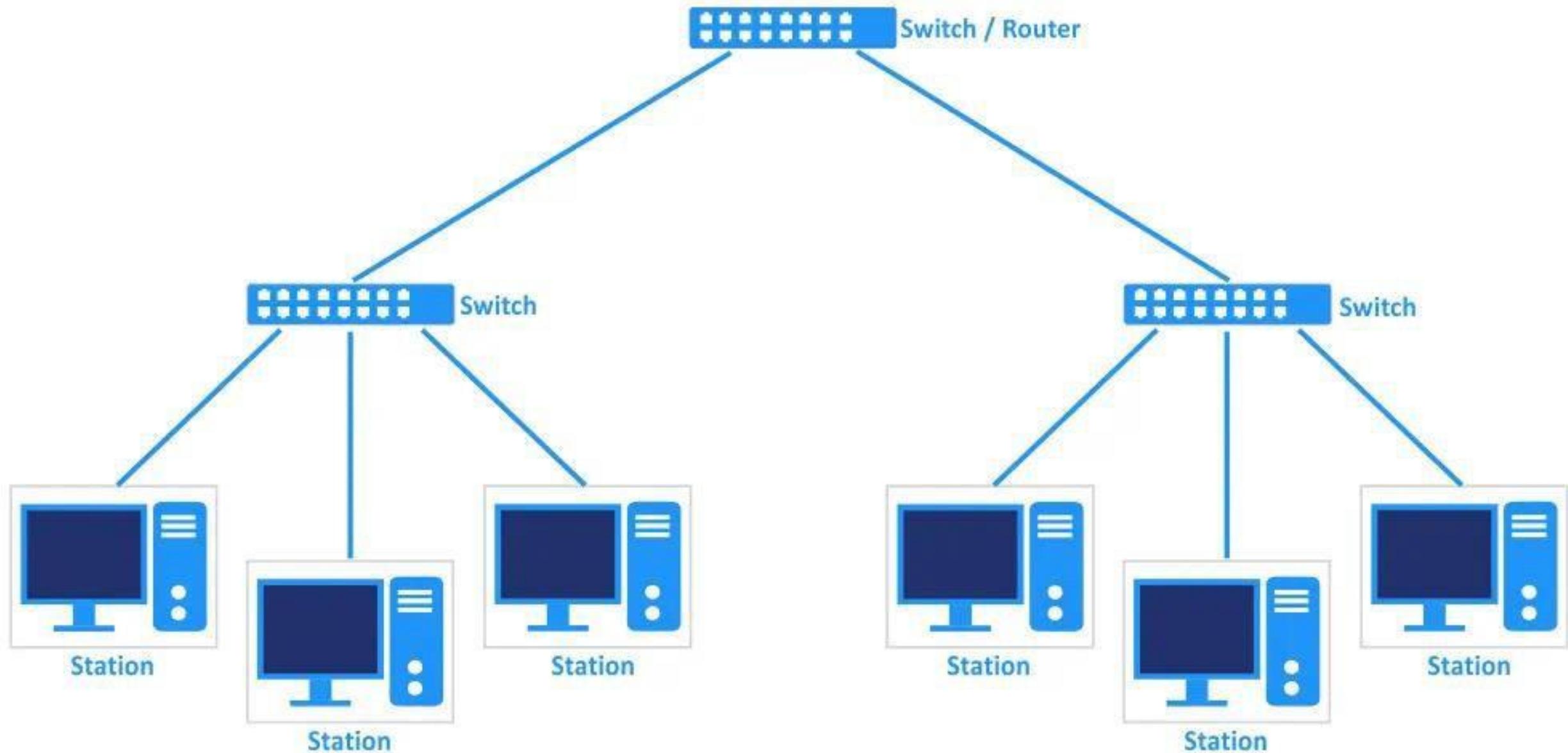
- **Advantages:**

- ➔ Point to point wiring for individual segment.
- ➔ A tree topology network can be managed and maintained easily.
- ➔ In this topology, Node expansion is easy and fast.

- **Disadvantages:**

- ➔ If the central hub gets fails the entire system fails due to hierarchy of devices.
- ➔ The cost is high because of cabling.

Tree Topology



➤ Mesh Topology:

- ➔ Mesh topology is a type of networking in which all the computers are inter-connected to each other.
- ➔ In Mesh Topology, the connections between devices take place randomly.
- ➔ The connected nodes can be computers, switches, hubs, or any other devices.
- ➔ Internet is the best example of mesh topology. Assume the internet network among 4 – 5 cities, each city connected with other remaining cities.
- ➔ Mesh Topology further divided into two categories:
 - **Full Mesh:**
 - ➔ In a full mesh topology, all the devices are connected with all other devices.
 - ➔ Full Mesh is a network where every node will have an $n-1$ number of connections if there are n number of nodes available in the network.
 - ➔ It provides a benefit that if one of the nodes goes down, the traffic load of the network is redistributed to other nodes.

Mesh Topology:

➤ Partial Mesh:

- In a full mesh topology, only a few nodes are attached with all the other nodes.
- It means that in this network, it is not necessary to connect all the devices are attached with other.
- As compared to full mesh topology, it is less costly, and it provides basic redundancy to control the failure of any nodes.

• Advantages:

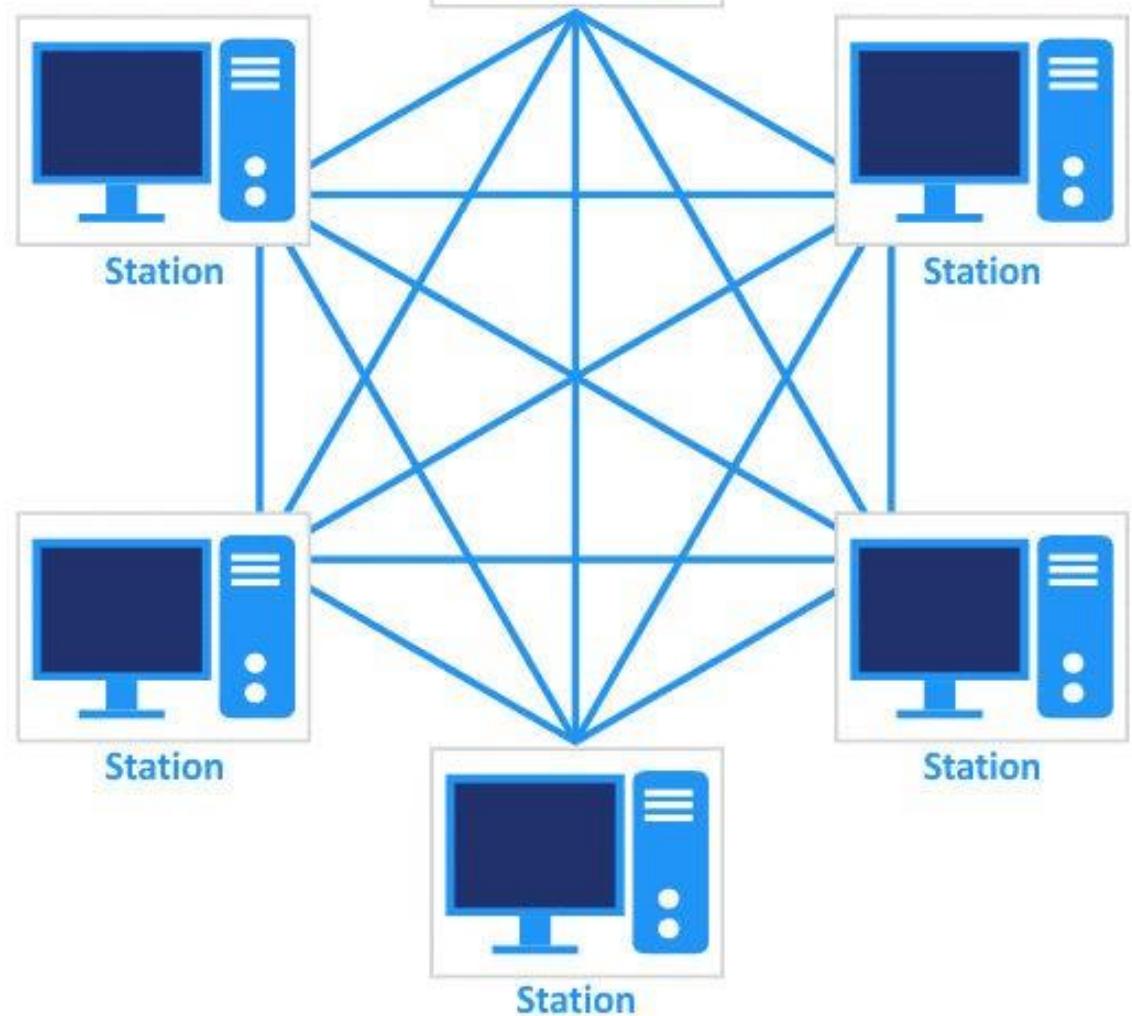
- Data can be transmitted to another node in any situation.
- If any single node fails, will not affect to entire network.

• Disadvantages:

- In this topology, each node works as a router that increases complexity.
- The installation is much hard.
- As compared to other topologies the cost of mesh topology is high.

Full Mesh

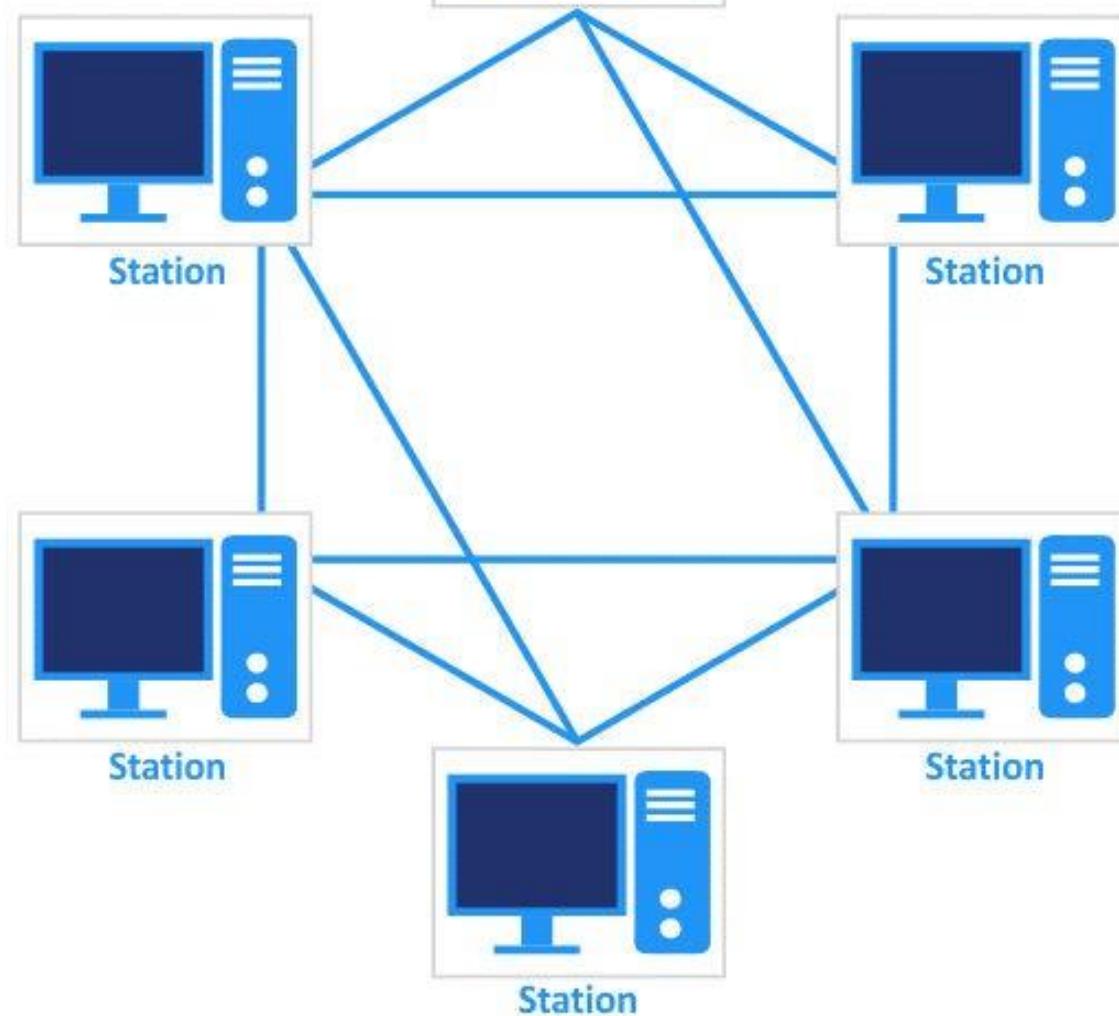
Station



Mesh Topology

Partial Mesh

Station



➤ Hybrid Topology:

- A hybrid topology is a kind of network topology that is a combination of two or more network topologies, such as mesh 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.

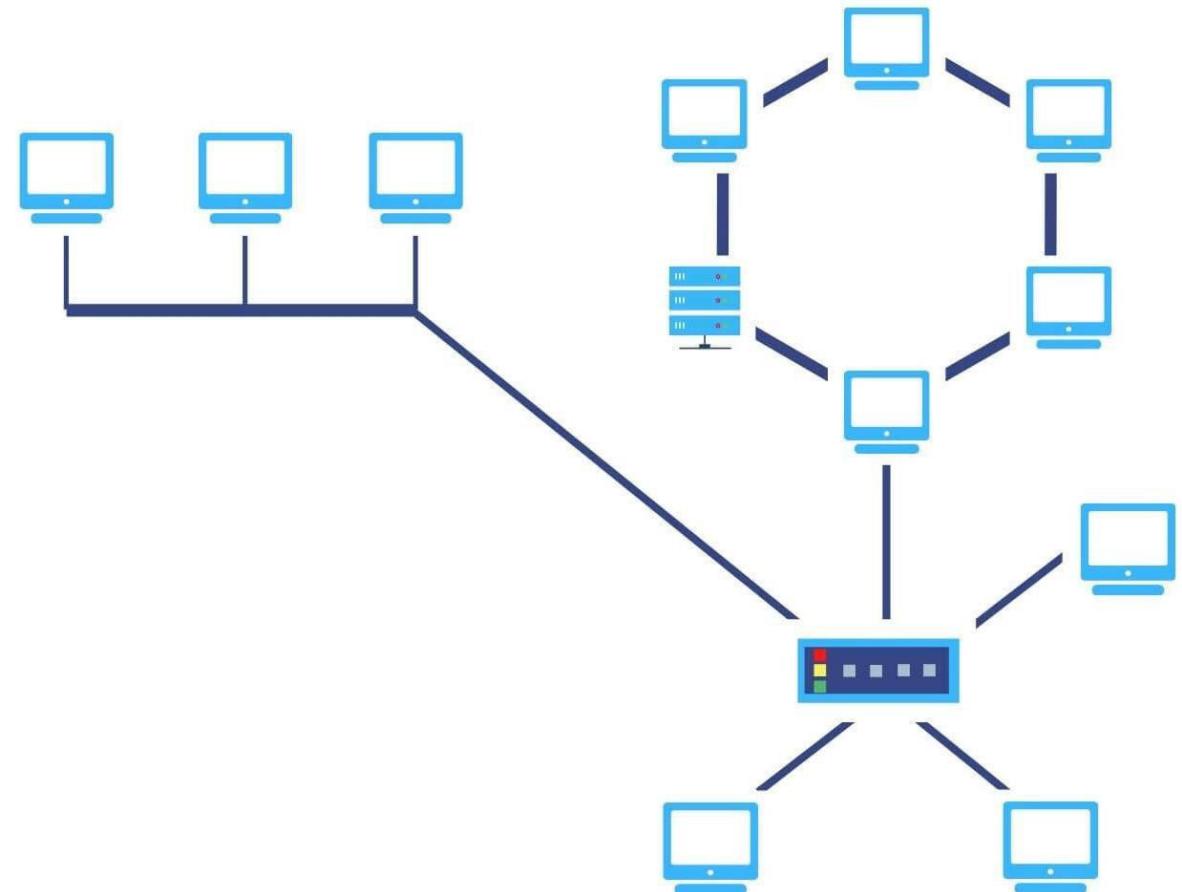
□Advantages:

- This type of topology combines the benefits of different types of topologies in one topology and it can be modified as per requirement.
- It is extremely flexible and reliable as well.
- Error detecting and troubleshooting are easy.
- It Handles a large volume of traffic and it is used to create large networks.

Hybrid Topology:

□ Dis-advantages:

- It is expensive and the design of a hybrid network is very complex.
- There is a change in the hardware to connect one topology with another topology for that purpose specialized software required as well.
- Installation is difficult.

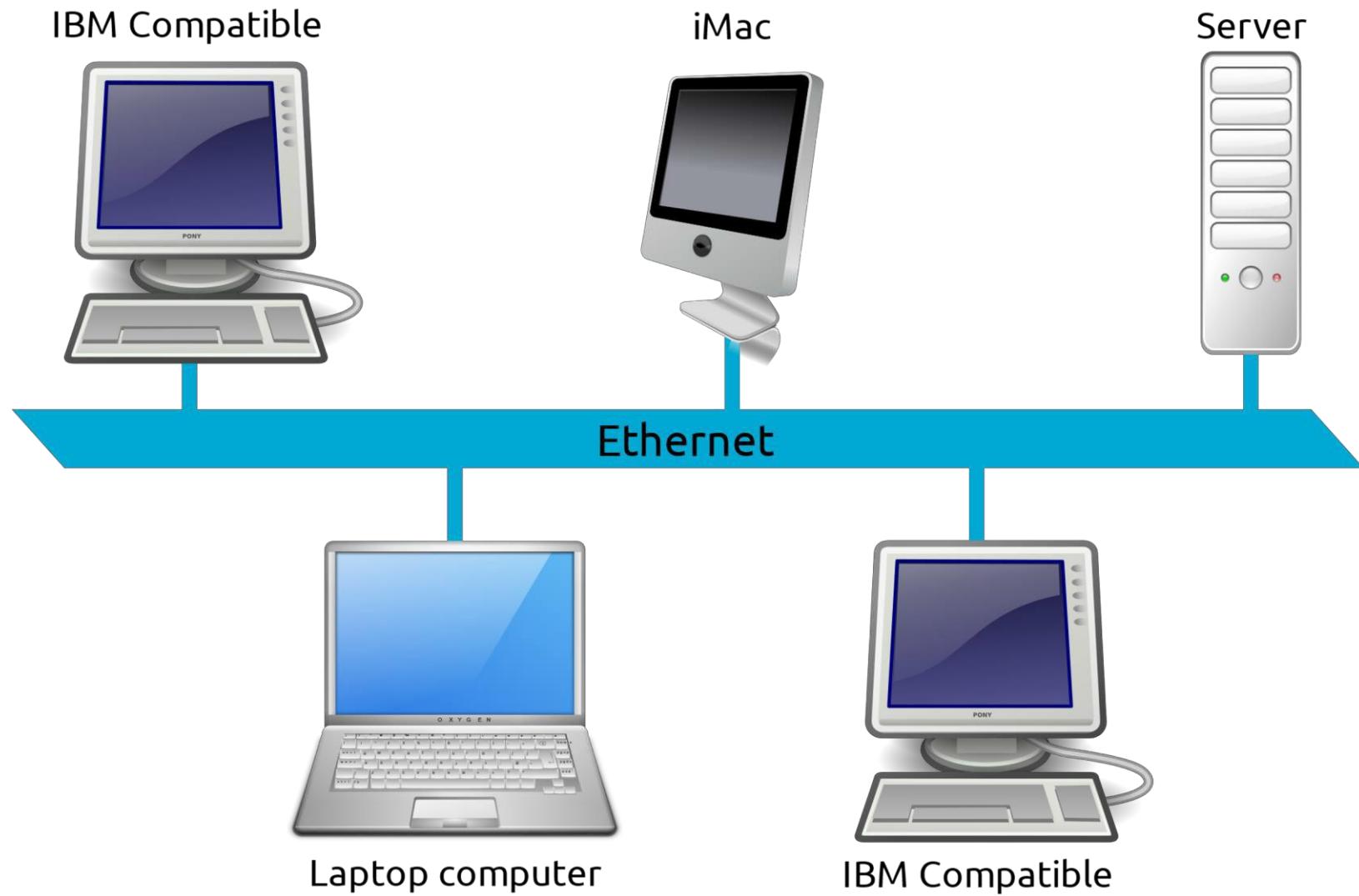


● Advanced Network Topologies:

➤ Ethernet :

- Ethernet is the traditional technology for connecting devices in a wired LAN or WAN. It enables devices to communicate with each other via a protocol, which is a set of rules or a networking program.
- Ethernet describes how network devices format and transmit data so other devices on the same LAN or campus network can recognize, receive and process the information. An Ethernet cable is the physical, coated wiring over which the data travels.
- Compared to wireless LAN technology, Ethernet is less vulnerable to disruptions.
- It can also offer a higher network security and control than wireless technology because devices must connect using physical cabling. This makes it difficult for outsiders to access network data or hijack bandwidth for unsanctioned devices.
- Current versions of Ethernet can support operations up to 400 Gbps.

Advanced Network Topologies:



● Advanced Network Topologies:

➤ FDDI (Fiber Distributed Data Interface):

- FDDI (Fiber Distributed Data Interface) is a network standard that uses fiber optic connections in a LAN that can extend in range up to 200 kilometers.
- The FDDI protocol is based on the token ring protocol. A FDDI LAN can support thousands of users. While FDDI is frequently used on the backbone for a WAN or CAN, it has been largely replaced by other networking technologies.
- A FDDI network contains two token rings: a primary ring and a secondary ring that is used as a redundant backup.
- The primary ring offers up to 100 Mbps capacity, while the secondary ring can also be used to carry data, increasing capacity to 200 Mbps.

Advanced Network Topologies:

➤ CDDI (Copper Distributed Data Interface):

- CDDI (Copper Distributed Data Interface) is a network standard that uses copper wire connections in a LAN that can extend in range up to 100 meters.
- CDDI uses cabling, which is unshielded twisted pair cables (UTP) made of copper. CDDI also uses the same protocols and constructs as FDDI, but uses copper wire as the medium.
- A CDDI network also contains two token rings: a primary ring and a secondary ring that is used as a redundant backup.
- The primary ring offers up to 100 Mbps capacity, while the secondary ring can be used for redundant backup.
- This term is also known as twisted-pair distributed data interface (TP-DDI).

● Communication Methods:

➤ Unicasting (One-to-One):

- This type of information transfer is useful when there is a participation of a single sender and a single recipient.
- So, in short, you can term it as a one-to-one transmission. For example, if a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets) to the device with IP address 20.12.4.2 in the other network, then unicast comes into the picture.
- This is the most common form of data transfer over the networks.

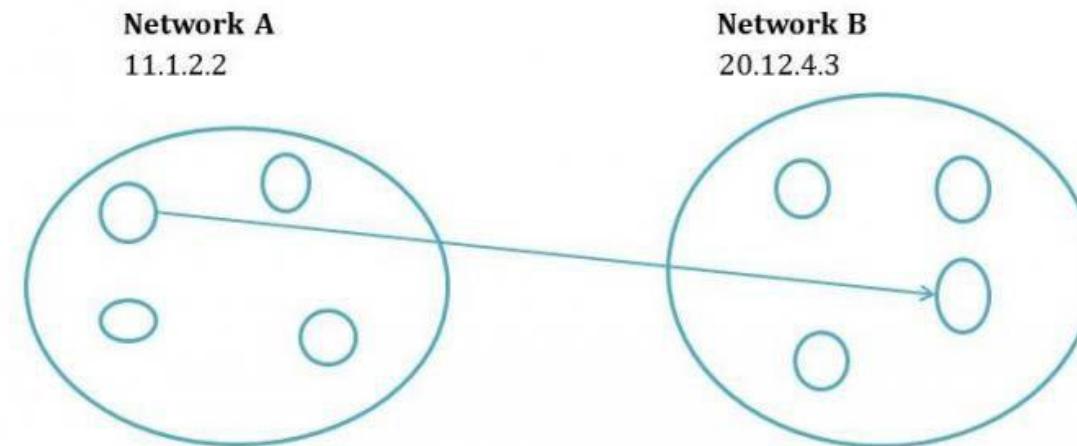


Figure: Unicast

Communication Methods:

➤ Multicasting (One-to-Many):

- In multicasting, one/more senders and one/more recipients participate in data transfer traffic.
- In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets servers direct single copies of data streams that are then simulated and routed to hosts that request it.

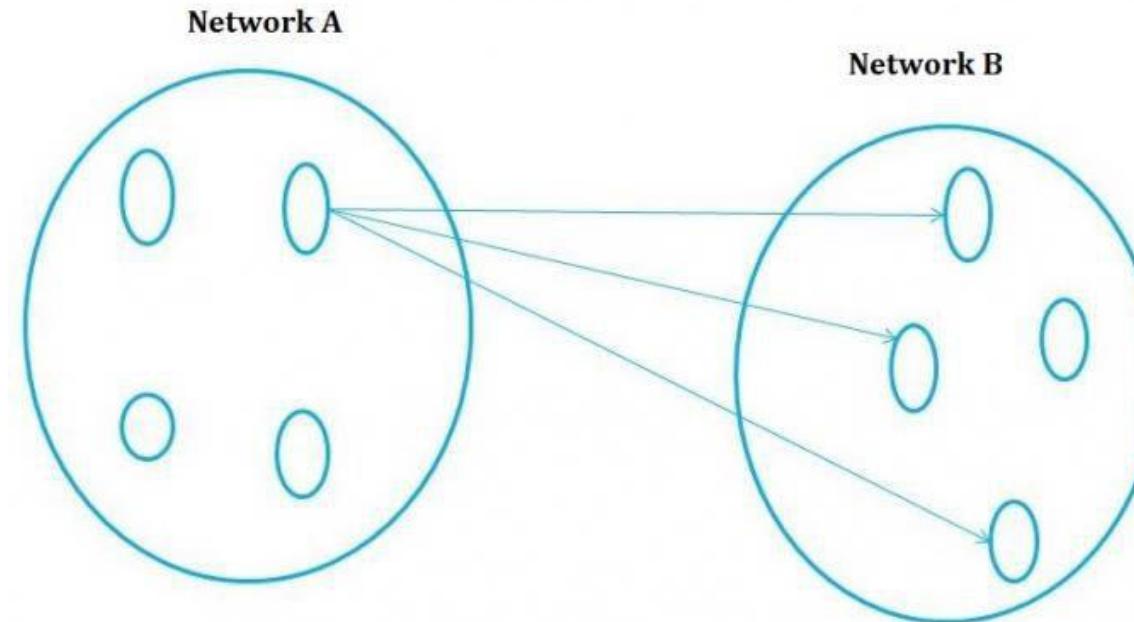


Figure: Multicast

Communication Methods:

➤ Broadcasting (One-to-all):

- This is useful when a device in one network wants to transfer packet stream to all the devices over the other network.
- This is achieved by translating all the Host ID part bits of the destination address to 1, referred to as Direct Broadcast Address in the datagram header for information transfer.

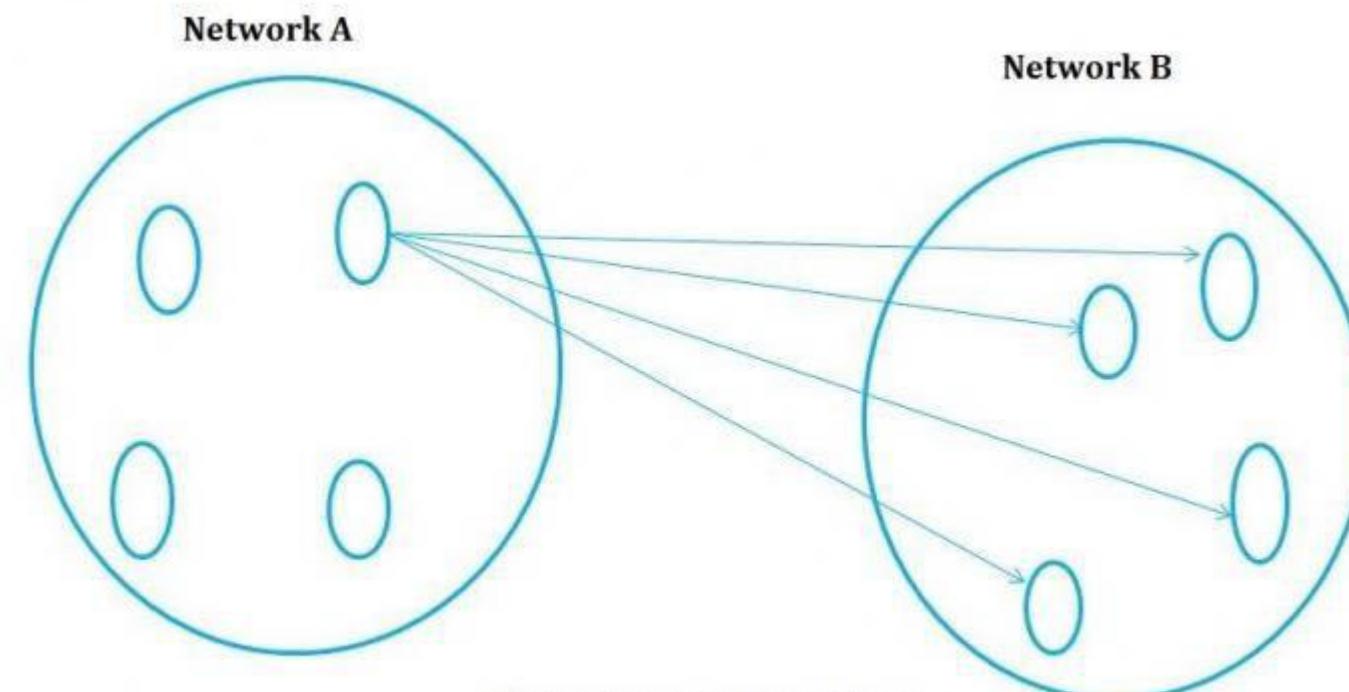


Figure: Directed Broadcast

○ Assignments:

1. What is Network? What are the se of network?
2. Explain network model: Peer-to-Peer and Client-Server in details.
3. Explain all network services in brief.
4. Describe following:
 - CSMA/CD
 - CSMA/CA
 - Token Passing
 - Polling
5. What is Network topology? Explain all types of topology in detail.
6. Explain all advanced network topologies in details.
7. List and explain all communication methods available in computer network.

CS - 21

NETWORK TECHNOLOGY AND ADMINISTRATION

Ch - 2

Network Model and

LAN Sharing

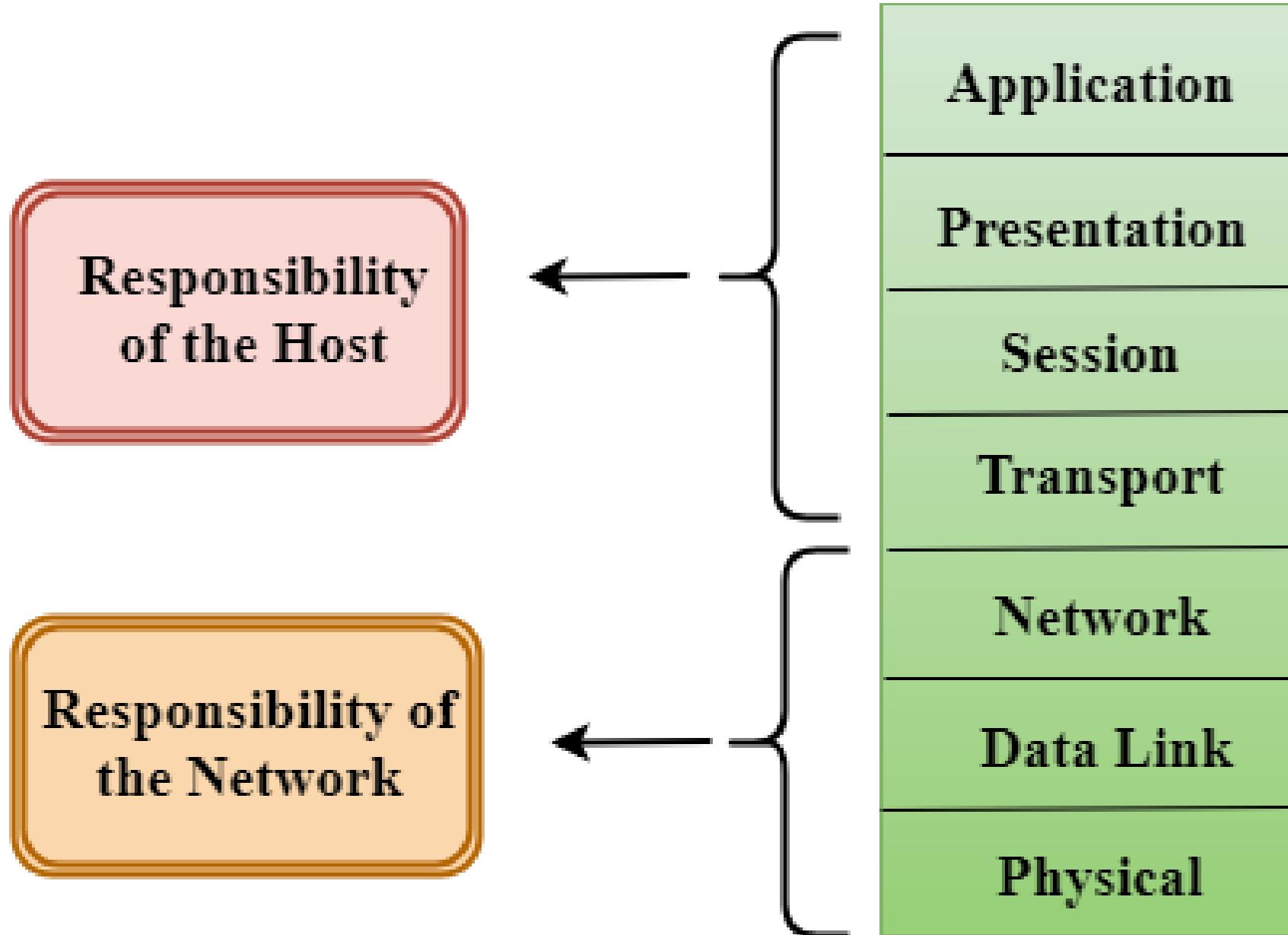
Contents..

- OSI reference model with 7 layers.
- TCP/IP network model with 4 layers.
- File and Print Sharing in LAN. Network drive.
- Disk quota.
- Encryption.
- Compression. Net
- Meeting

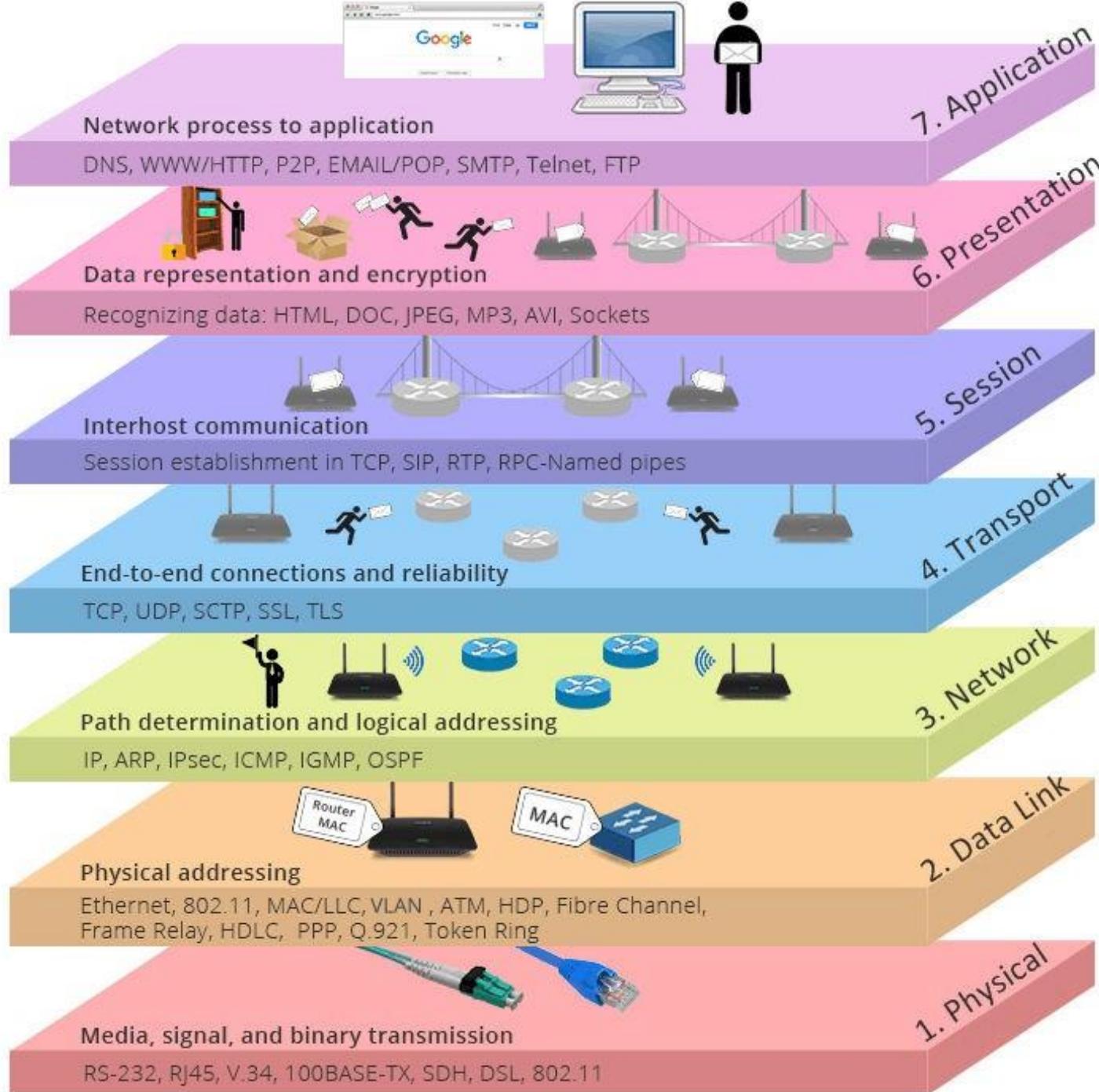
● OSI Reference Model:

- OSI stands for Open System Interconnection.
- The OSI model is just a model / structure that represents how any open system like Computer, Mobile, Tablets or any computing devices can able to connect to the network and how they send their data to other devices via computer networks.
- in other words, is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter- computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

→ There are 7 layers in an OSI reference model:



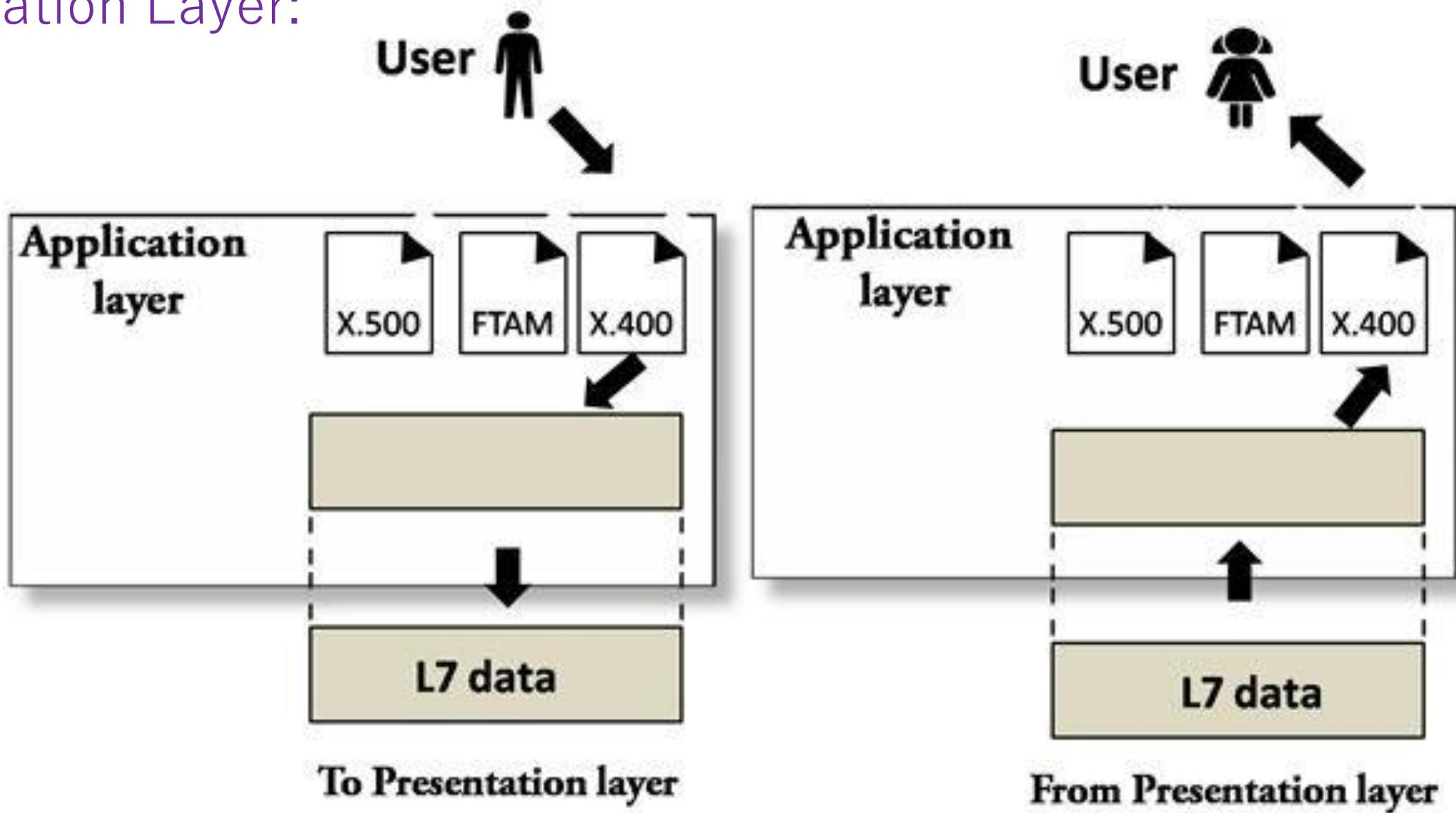
- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.
- Upper three layers: Application Layer, Presentation layer and Session Layer are the software-based layers.
- The lower four layers: Transport Layer, Data Link Layer, Network Layer and Physical Layers are the hardware-based layers.



➤ Application Layer:

- ➔ At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications.
- ➔ These applications produce the data, which has to be transferred over the network.
- ➔ This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
- ➔ An application layer is not an application, but it performs the application layer functions.
- ➔ An application layer allows a user to access the files in a remote computer.
- ➔ An application layer provides the facility for email forwarding and storage.
- ➔ For Example: Gmail, using Gmail we can prepare and forward the mail to another device.

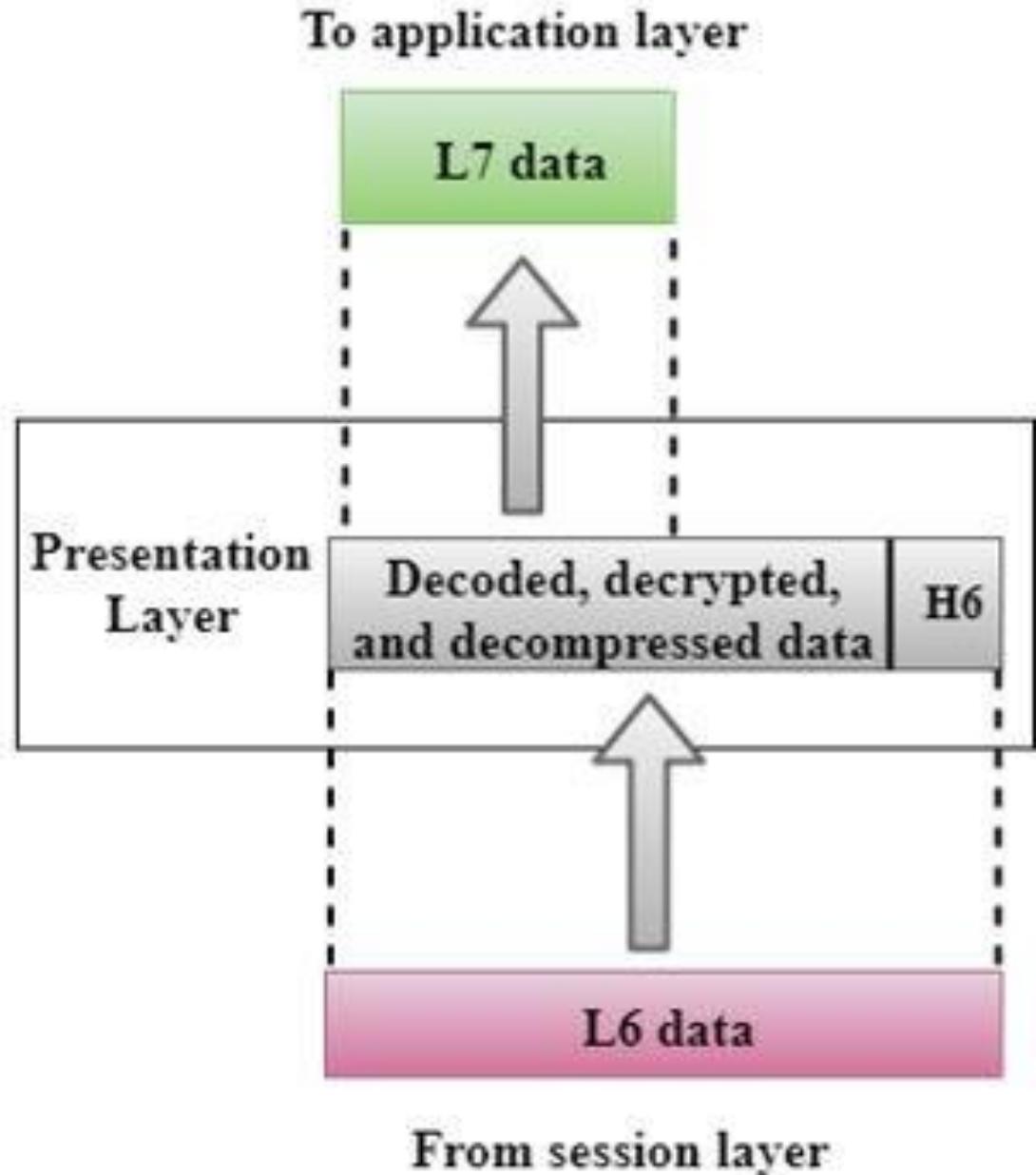
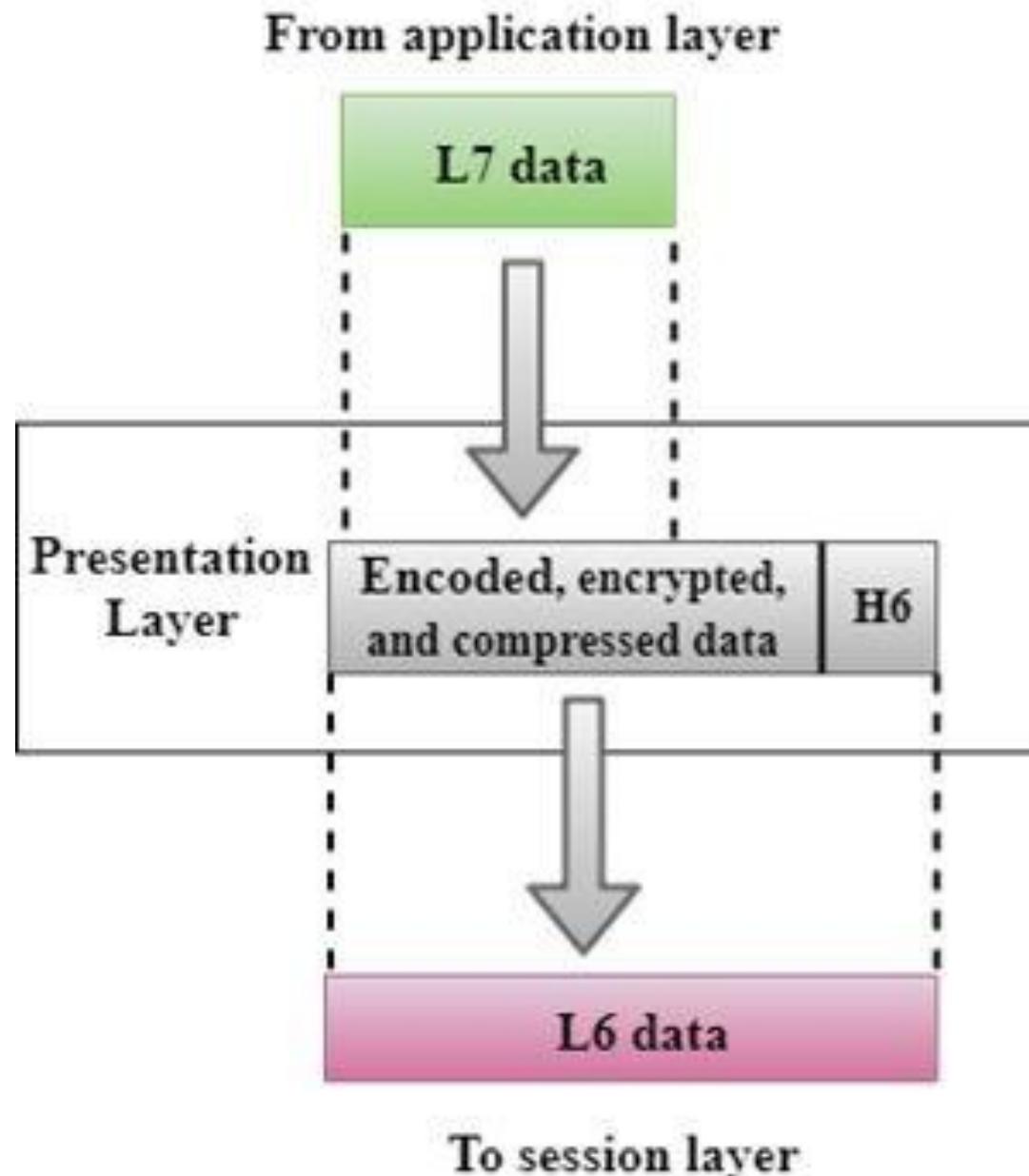
Application Layer:



➤ Presentation Layer:

- ➔ The presentation layer ensures that the message is presented to the upper layer in a standardized format. It deals with the syntax and the semantics of the messages.
- ➔ This layer is also known as Translation layer, as this layer serves as a data translator for the network.
- It performs following functions:
 - ➔ **Translation:** For example, ASCII to EBCDIC.
 - ➔ **Encryption/ Decryption:** Data encryption translates the data into form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
 - ➔ **Compression:** Reduces the number of bits that need to be transmitted on the network.

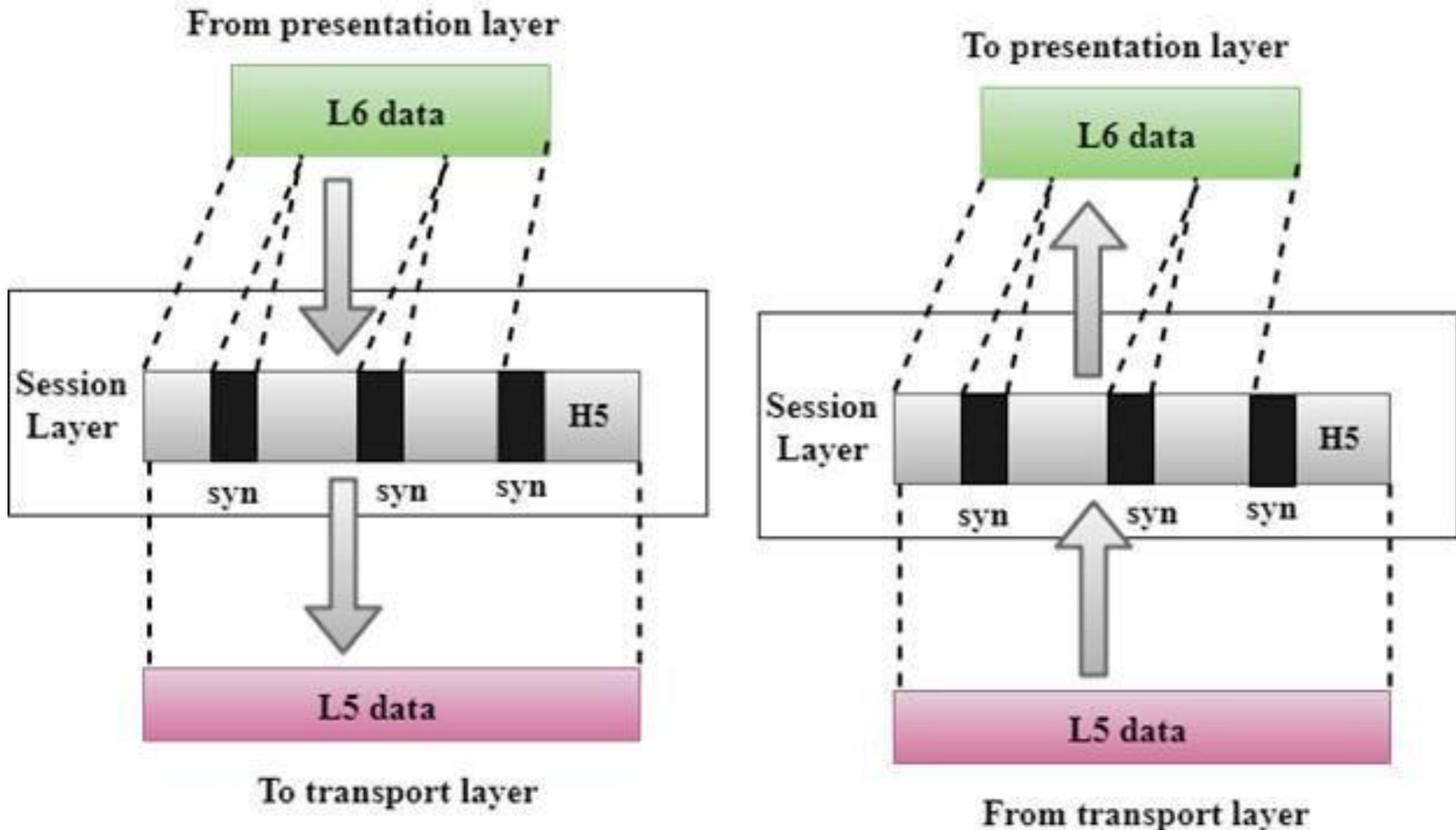
Presentation Layer:



➤ Session Layer:

- ➔ This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.
- ➔ The layer allows the two processes to establish, use and terminate a connection.
- ➔ This layer also controls single or multiple connections for each-end user application and directly communicates with both Presentation and transport layers.
- ➔ Synchronization: This layer allows a process to add synchronization points into the data. These points help to identify the error so that the data is resynchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- ➔ Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex or simplex manner.

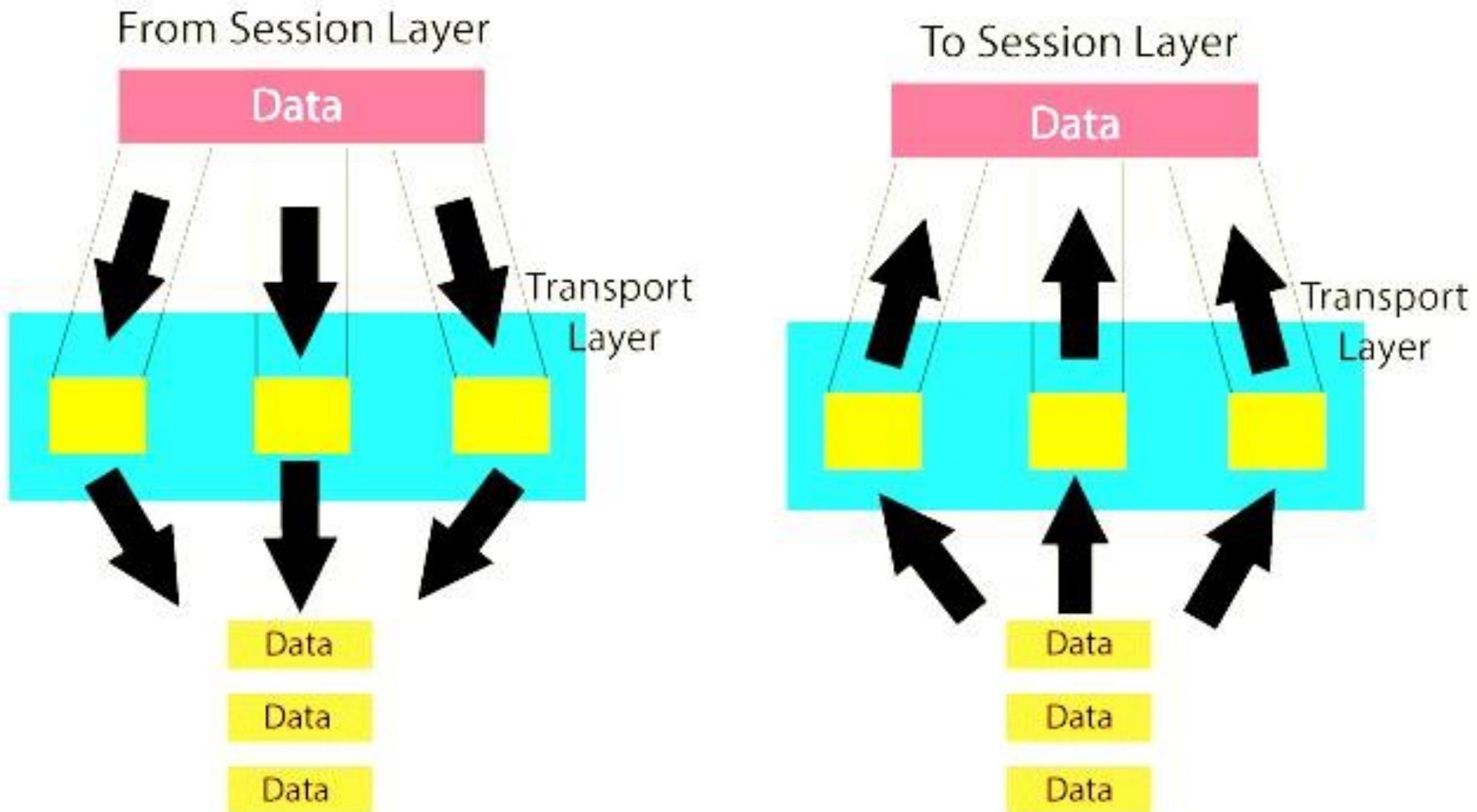
Session Layer:



➤ Transport Layer:

- ➔ The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
 - ➔ The main responsibility of the transport layer is to transfer the data completely.
 - ➔ It receives the data from the upper layer and converts them into smaller units known as segments.
 - ➔ It provides two protocols to transfer a data: TCP/IP protocol and User Datagram Protocol (UDP).
 - ➔ The data in the transport layer is referred to as Segments.
 - ➔ This layer assigns a port number and segment number to each segment of data.
 - ➔ Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
- Transport Layer is called as Heart of OSI model.

Transport Layer:



> Network Layer:

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- The network layer works for the transmission of data from one host to the other located in different networks.
- The sender & receiver's IP addresses are placed in the header by the network layer.

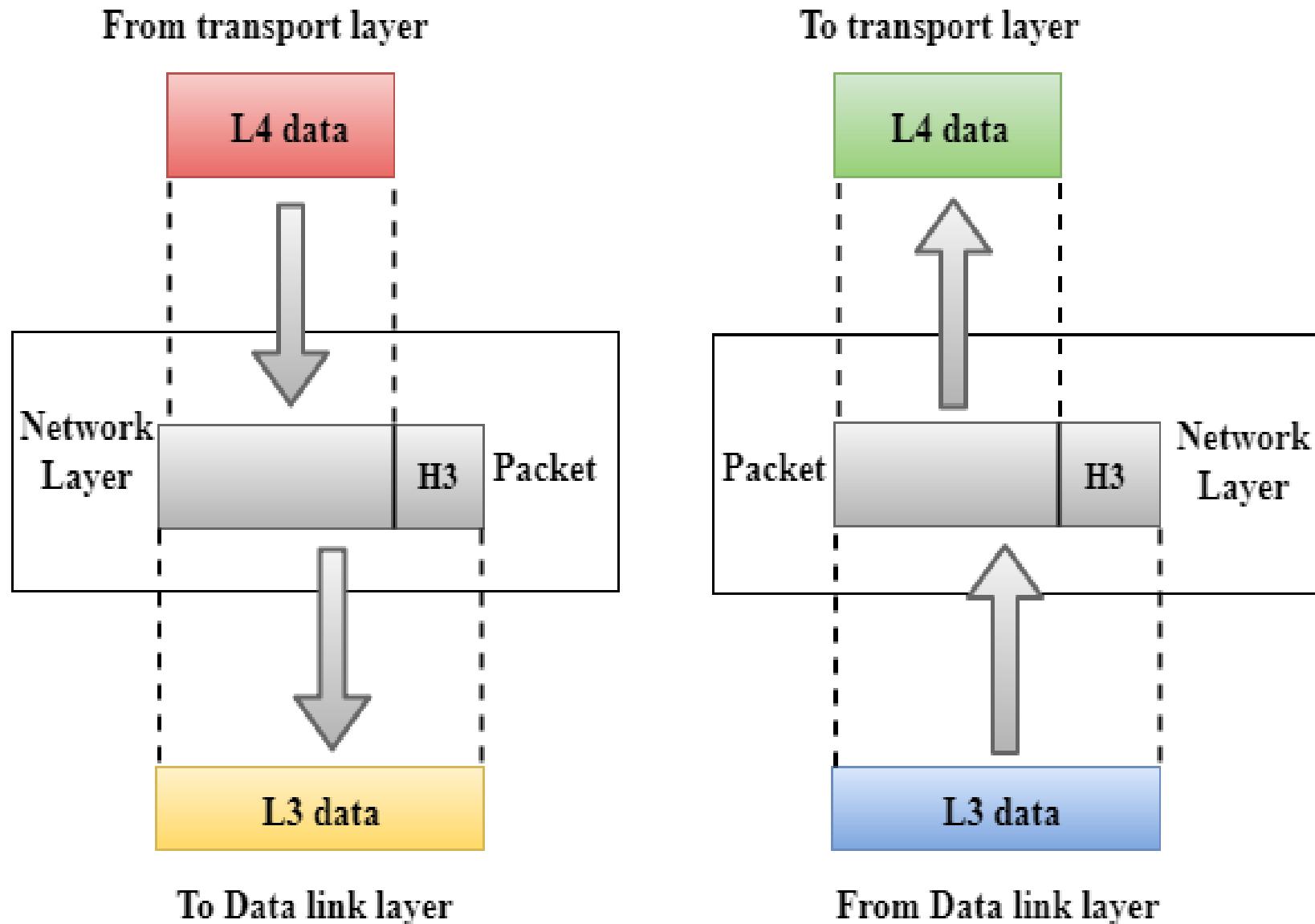
The functions of the Network layer are:

- 1. Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- 2. Logical Addressing:** In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme.
- 3. Packetizing:** A Network Layer receives the data as segments from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Network Layer:

Network Layer Devices:

- 1.Router
- 2.Layer 3 Switch
- 3.Brouter 4.Gateway



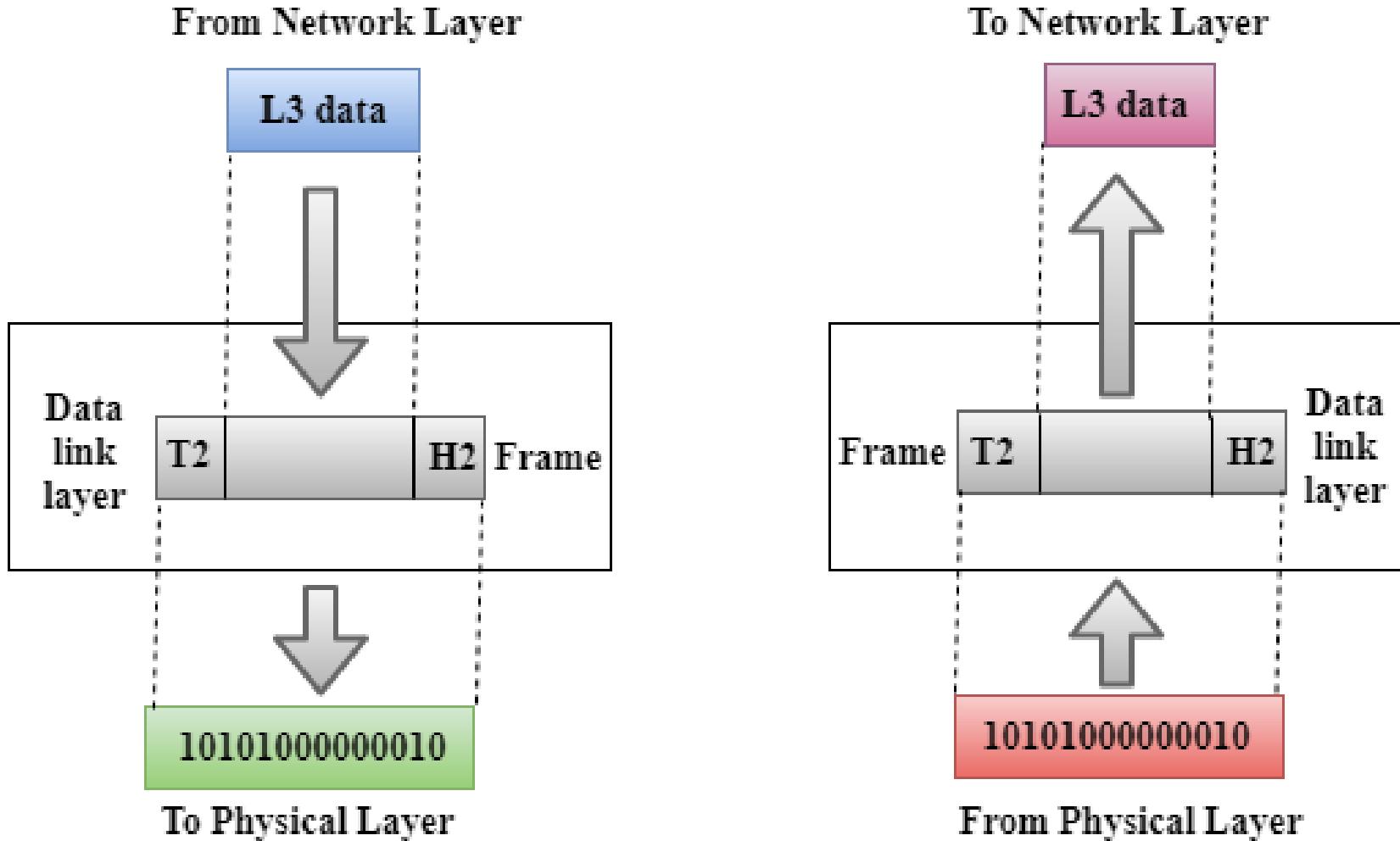
➤ Data-Link Layer:

- The data link layer is responsible for the node-to-node delivery of the message.
- The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- Data Link Layer is divided into two sub layers:
 - Logical Link Control (LLC)
 - Media Access Control (MAC)
- The packet received from the Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also writes Sender and Receiver's MAC address in the header.
- *Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
Switch & Bridge are Data Link Layer devices.

Data-Link Layer:

- Data Link Layer Devices

1. Switch
2. Bridge



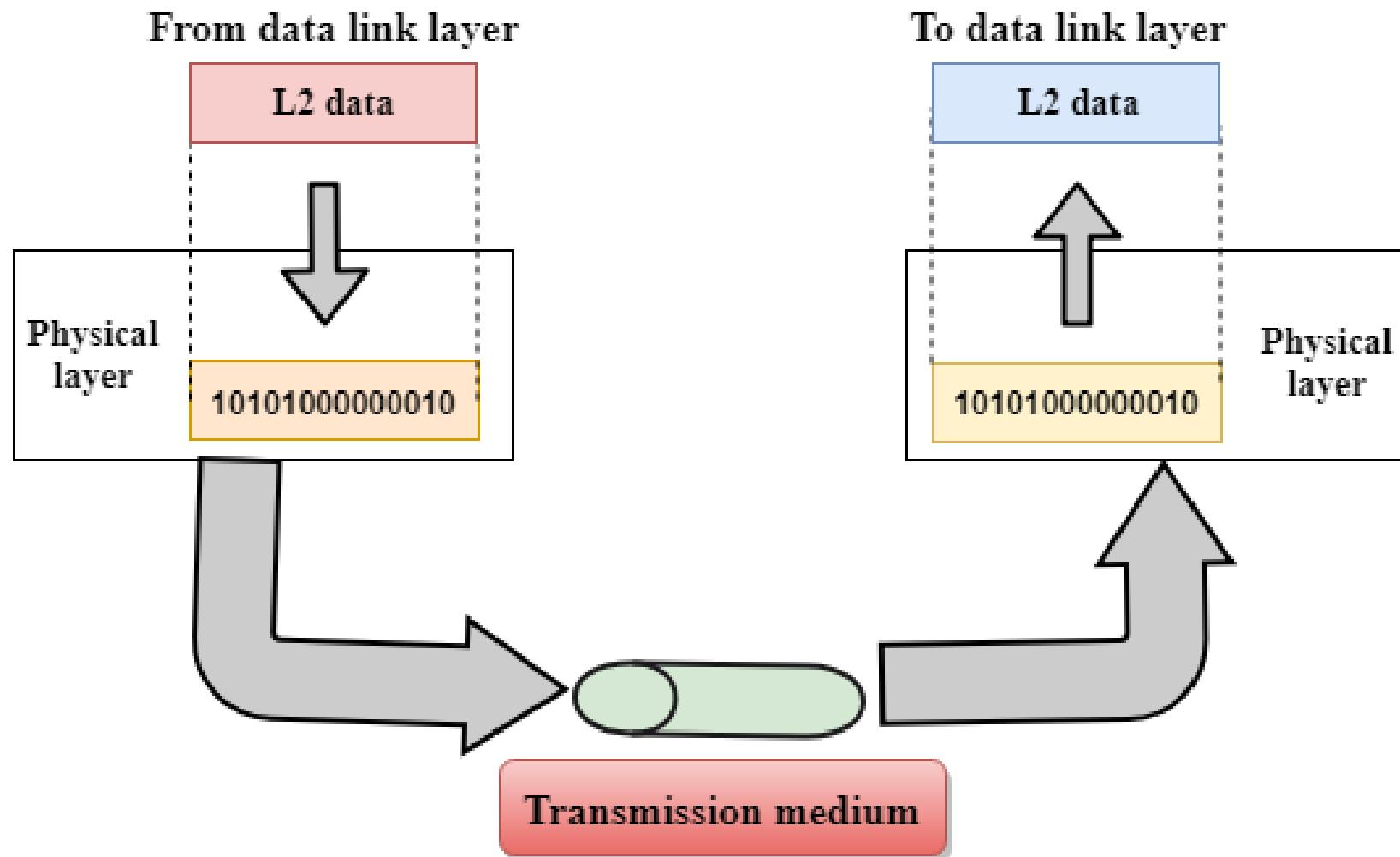
➤ Physical Layer:

- The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices.
- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- The physical layer contains information in the form of bits. (10101010)
- It is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer.
- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half- duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

Physical Layer:

■ Physical Layer Devices

1. NIC (Network Interface Card) / LAN Card
2. Modem
3. HUB (Active, Passive, Smart Hub)
4. Repeater





Transceiver



Cable Modem



Sockets/Connectors



Wired Media Cables



Wireless Media Antennas



Intermediate devices –
Hubs, Repeaters

○ **TCP/IP Model:**

- The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- Whereas TCP/IP model was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol.
- The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.
- There are four Layers included into TCP/IP model are as under:
 - Application Layer
 - Transport Layer
 - Internet Layer
 - Network Access Layer

TCP/IP Model:

➤ Process/Application Layer:

- An application layer is the topmost layer in the TCP/IP model.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- Following are the main protocols used in the application layer:
 - ✓ HTTP, SNMP, SMTP, DNS, TELNET, FTP.

➤ Host-to-Host / Transport Layer:

- It is responsible for end-to-end communication and error-free delivery of data.
- It shields the upper-layer applications from the complexities of data.
- The two main protocols present in this layer are :
- Transmission Control Protocol (TCP) – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data.
- User Datagram Protocol (UDP) – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

➤ Internet Layer:

- This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- The main protocols residing at this layer are :
 - IP (Internet Protocol)
 - ICMP(Internet Control Message Protocol)
 - ARP (Address Resolution Protocol)

➤ Network Access Layer:

- This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model.
- It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

● File and Printer Sharing:

- File and printer sharing is the part of Microsoft networking that enables you to share files and local printers with other user on small networks.
- If this services is enabled on your windows computer and you are connected to a LAN you are allowing others to connect to your computer and access your files and printers.
- While you can setup passwords to protect your files and printers when using this service.

● Aping Network Drive:

- Ping is the name of a standard software utility (tool) used to test network connections. It can be used to determine if a remote device (such as Web or game server) can be reached across the network and, if so, the connection's latency.
- Ping tools are part of Windows, Mac OS X and Linux as well as some routers and game consoles.
- Most ping tools use Internet Control Message Protocol (ICMP). They send request messages to a target network address at periodic intervals and measure the time it takes for a response message to arrive.

● Disk Quota:

- A disk quota is a limit set by a system administrator that restricts certain aspects of file system usage on modern operating system.
- There are two basic types of disk quotas.
- The first , known as a usage quota or block quota , limits the amount of disk space that can be used.
- The second , known as a file quota or inode quota limits the number of files and directories that can be created.

○ Encryption:

- Encryption is the conversion of data into form called a ciphertext that cannot be easily understood by unauthorized people.
- Decryption is the process of converting encrypted data back into its original form so it can be understood.
- Network encryption is a network security process that applies crypto services at the network transfer layer above the data link layer.
- Data is encrypted only while in transit existing as plaintext on the originating and receiving hosts.
- Network encryption is implemented through internet protocol security a set of open Internet Engineering Task Force (IETF) standards that used in conjunction created a framework for private communication over IP networks.

○ Compression:

- Compression is the reduction in size of data in order to save space or transmission time.
- For data transmission , compression can be performed on just the data content or on the entire transmission unit.
- Graphic image file formats are usually designed to compress information as much as possible.
- Graphic image compression can be either lossy or lossless.
- When you send or receive information on the internet large text files , either singly or with other as part of an archive file , may be transmitted in zip , gzip or other compressed format.

○ Net Meeting:

- Microsoft introduced the NetMeeting application to allow for IP communications and video conferencing .
- It also allowed for application and desktop sharing , remote desktop sharing and transfer of files between client computer.
- NetMeeting was available for use starting with later version of Internet Explorer 3 and windows 95 and continued Windows XP.

○ Assignments:

1. Describe OSI model with all the layers in brief.
2. Define TCP/IP in detail.
3. Explain following in details:
 - File and Print Sharing in LAN.
 - Network drive.
 - Disk quota.
 - Encryption.
 - Compression.
 - Net Meeting

□Ch – 3 _ Transmission Media:

Ch-3

Transmission Media

■ **Transmission Media**

1. **Guided Media**

➤ **Twisted Pair Cable**

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)

➤ **Co-Axial Cable**

- Thinnet
- Thicknet

- Fiber Optic Cable

2. **Unguided Media**

- Radio wave
- Microwave
- Infrared

Transmission Media :

- A transmission medium is a material substance/stuff (solid, liquid, or gas) which can propagate energy waves.
- For example : The transmission medium for sound received by the ears is usually air but solid and liquids may also act as transmission media for sound.
- Transmission media are the physical pathways that connect computer to other device.
- Transmission medias can be of two types :
 - Guided Media (Wired)

- Unguided Media (Wireless)

Transmission media

Guided media

Coaxial

Fibre
Optics

Twisted

Baseband

Broadband

Unshielded

Shielded

Unguided media

Radiowaves

Microwaves

infrared

Bluetooth

Laser

❖ Guided Media:

- **Guided Media:**

It is also referred to as Wired or Limited transmission media. Signals being transmitted are directed and restricted in a narrow pathway by using physical links.

- **Features:**

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

- **(i) Twisted Pair Cable –**

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective cover. They are the most widely used Transmission Media. Twisted Pair is of two types:

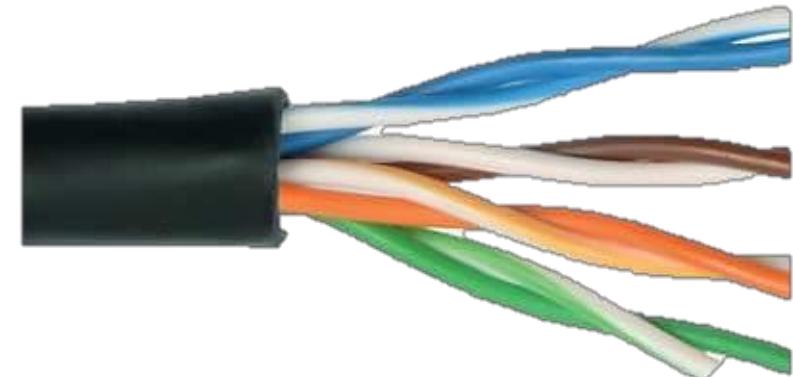
1. Twisted Pair Cable:

■ **Unshielded Twisted Pair (UTP):**

UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Features:

- Least expensive
- Easy to install
- High-speed capacity
- At risk to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to weakening of signals.



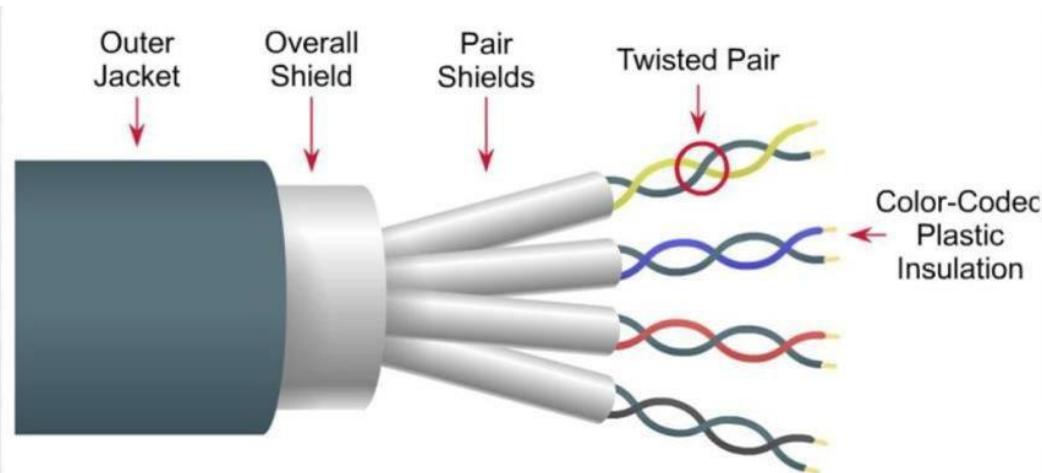
Twisted Pair Cable:

■ **Shielded Twisted Pair (STP):**

This type of cable consists of a special jacket (a copper thread covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

Features:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster
- Comparatively difficult to install and manufacture
- More expensive



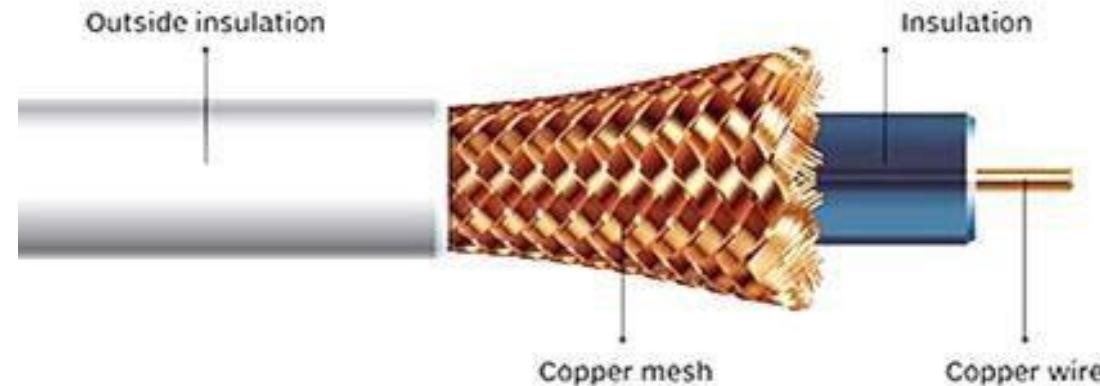
→ Bulky

2. Coaxial Cable:

■ (ii) **Coaxial Cable –**

It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Coaxial cable



Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Types of Coaxial Cable:

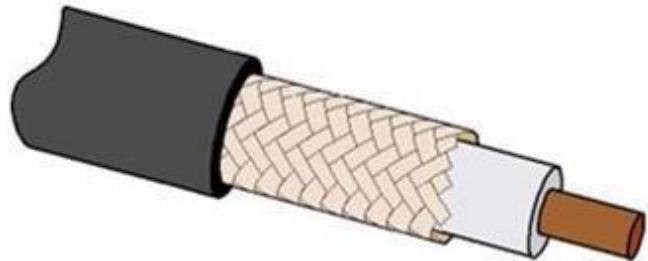
- Coaxial cable further divided into two categories

1. Thinnet Cable: Thinnet cable is light , flexible & less expensive cable medium.

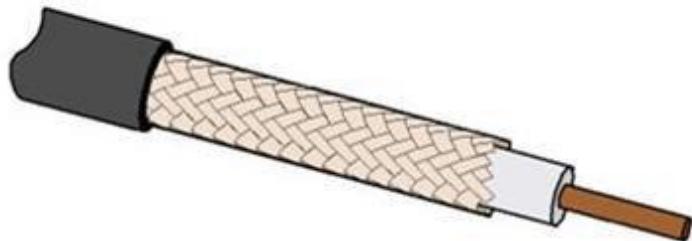
- It is easy to install.

2. Thicknet cable: Thicknet is thicker than thinnet.

- It can carry more signals at longer distance than thinnet.



ThickNet core



ThinNet core

3. Fiber Optic Cable:

- **3. Optical Fiber Cable:** It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.
- The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

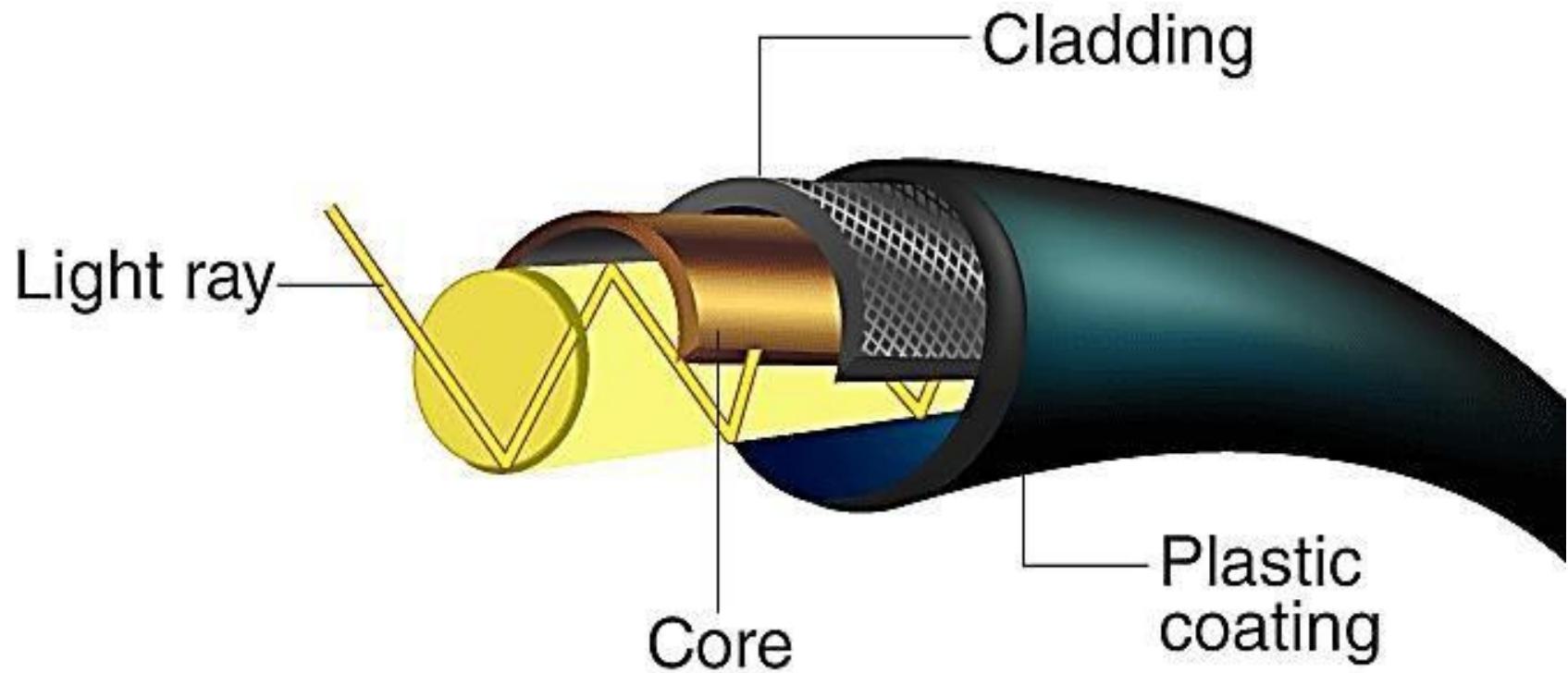
Advantages:

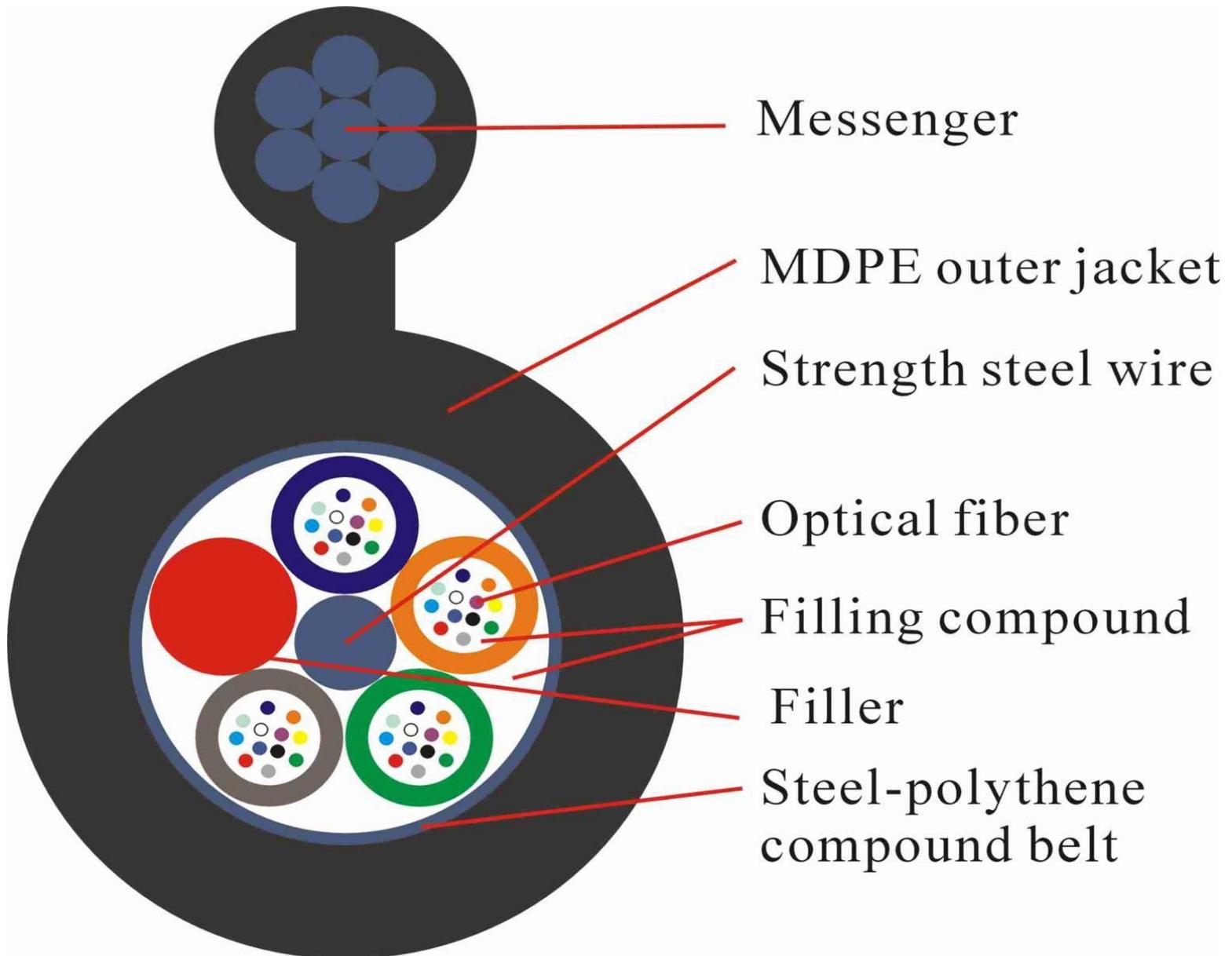
- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation (reduction)
- Protection from electromagnetic interference
- Protection from acidic materials

Fiber Optic Cable:

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile (Breakable)





❖ Unguided Media :

- Media that do not use any physical pathway or physical transmission medium is called wireless transmission media.
- Network with no physical pathway or without any cabling uses wireless media.
- Earth atmosphere provides the physical data path for transmissions.
- There are mainly five types of wireless transmission method are followed :
 1. Infrared
 2. Laser
 3. Radiowave
 4. Microwave

5. Bluetooth Technology

Various Frequency Ranges:

Frequency Band Name	Acronym m	Frequency Range	Wavelength (Meters)
Extremely Low Frequency	ELF	3 to 30 Hz	10,000 to 100,000 km
Super Low Frequency	SLF	30 to 300 Hz	1,000 to 10,000 km
Ultra Low Frequency	ULF	300 to 3000 Hz	100 to 1,000 km
Very Low Frequency	VLF	3 to 30 kHz	10 to 100 km
Low Frequency	LF	30 to 300 kHz	1 to 10 km
Medium Frequency	MF	300 to 3000 kHz	100 to 1,000 m
High Frequency	HF	3 to 30 MHz	10 to 100 m
Very High Frequency	VHF	30 to 300 MHz	1 to 10 m (FM, TV, Radio)
Ultra High Frequency	UHF	300 to 3000 MHz	10 to 100 cm (TV, Cellphone, Bluetooth, GPS)
Super High Frequency	SHF	3 to 30 GHz	1 to 10 cm (Radars, Satellite)
Extremely High Frequency	EHF	30 to 300 GHz	1 to 10 mm (LAN, Remote access)

1. Infrared Transmissions:

- Infrared technology uses the invisible portion of the light range with wave length just a little less than those of red light.
- These frequency are very high offering nice data transfer rates.
- We are used to seeing Infrared technology utilization for our television or VCR remote.



Television



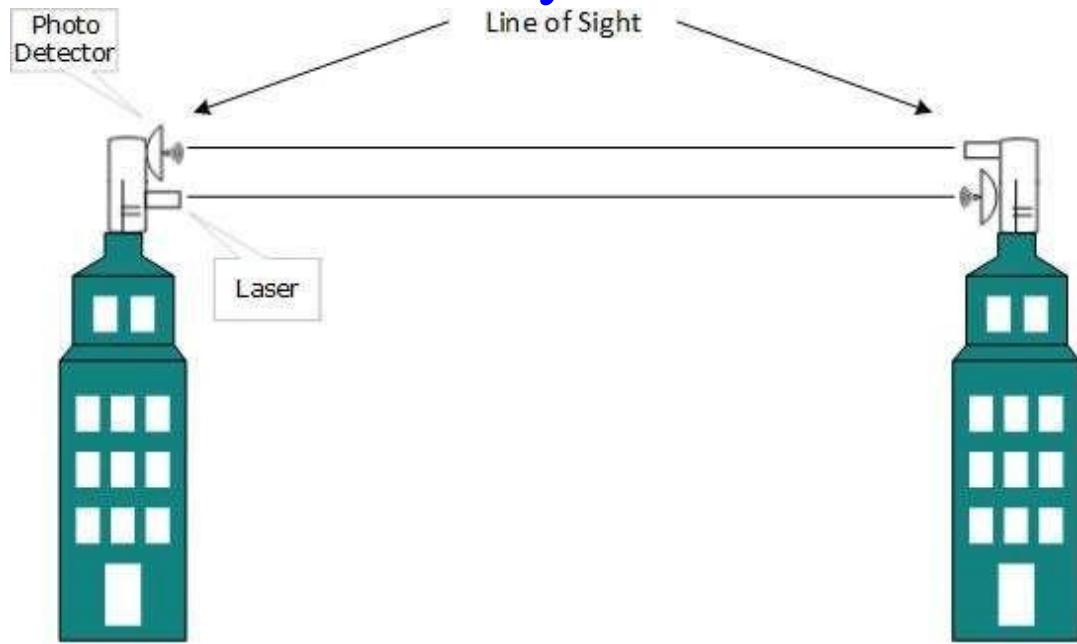
Infrared Radiations



Remote

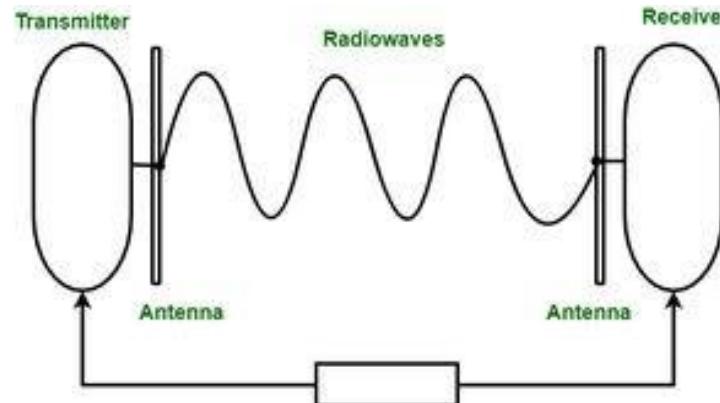
2. Laser Transmission:

- The word laser is an acronym for Light Amplification by Simulation Emission of Radiation.
- High-powered laser transmitters can transmit data for several thousand yards or meters when line-of-sight communication is possible.
- Laser light technology is employed in with LAN & WAN transmission , though it is more commonly used in WAN transmission.



3. Narrow Band Radio Transmission:

- Narrow band radio communication also called single frequency radio.
- The range of narrow band radio is higher than infrared. Effectively enabling mobile computing over a limited area.
- Neither the receiver nor the transmitter must be placed along a direct line of sight; the signal can bounce off walls, buildings, and even the atmosphere, but heavy walls, such as steel or concrete walls, can block the signal.
- Higher power frequency hence less attenuation (weakening of signals).



4. Microwave Communication :

- In the electromagnetic spectrum, waves within the frequencies 1GHz to 300GHz are called microwaves
- Microwave communication can take two forms :

1 Terrestrial Links [ground]

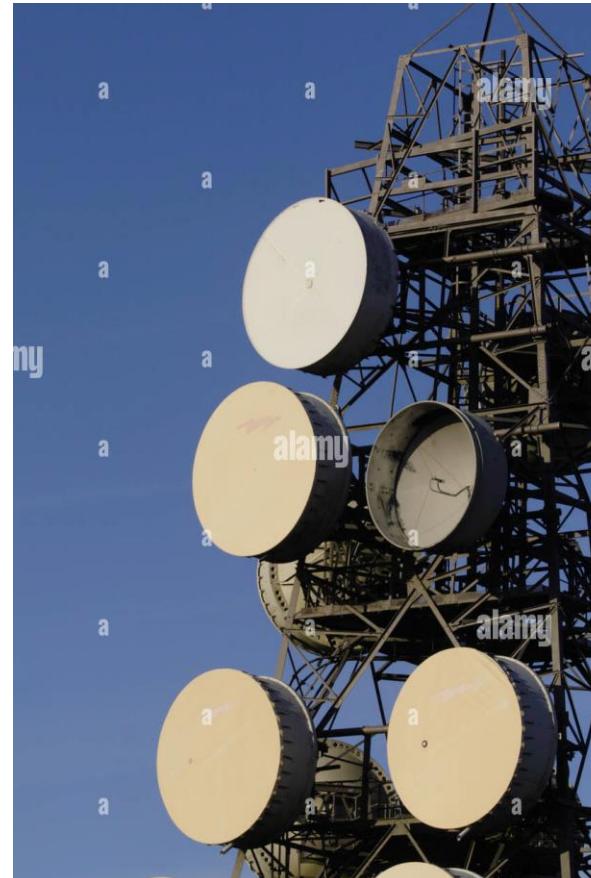
2 Satellite Links

1. Terrestrial or Ground links :

- Terrestrial microwave communication use earth based transmitter & receivers.
- Terrestrial microwave equipment in the form of telephone link towers.
- in such a case a microwave link is an ideal solution.

4. Microwave communication :

- In these systems, the signals are extremely focused and the physical route must be line of sight. Terrestrial Microwave Systems need directional parabolic antennas to broadcast and receive signals in the lower gigahertz range.



4. Microwave Communication:

2. Satellite Microwave: Satellite microwave system relay transmission through communication Satellite.

- These Satellite operate in geographically synchronize orbits 22,300 miles (36,000 Km) above the earth.
- Earth station use parabolic antennas to communicate with Satellite.



Bluetooth Technology :...

- Bluetooth :
- Bluetooth is a radio-based wireless technology.
- It allows device to share information over a maximum range of 10 meters.
- Bluetooth technology enables computers, phones, and peripherals to communicate with one another without cables.
- Bluetooth enables devices give the user more flexibility, security, reduced power consumption.
- As long as two Bluetooth devices are close enough to each other, it's possible to make a connection.

Advantages

- **Advantages**
- Enhance user experience.
- Connecting devices without the need for cables.
- Becoming more integrated within laptops, mobile phones, and many other devices.
- Reduced power consumption.

Ch-4

Multiplexing & Switching Concepts

Content:

1. Multiplexing & De-multiplexing

Multiplexing Types

- FDM (Frequency Division Multiplexing)
- TDM (Time Division Multiplexing)
- CDM (Code Division Multiplexing)
- WDM (Wavelength Division Multiplexing)

2. Different Frequency Ranges

3. Switching Techniques :

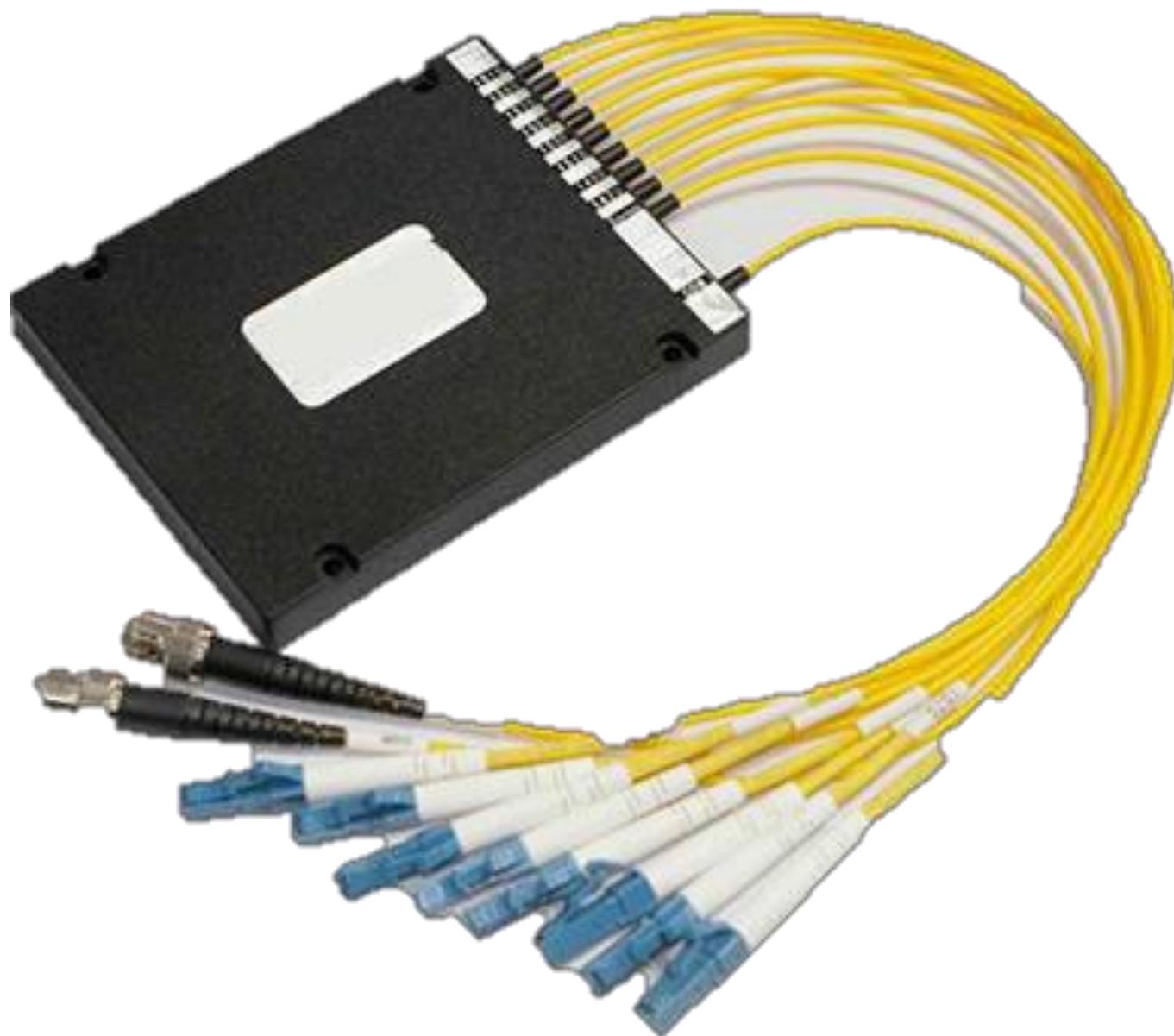
- - Circuit Switching
- - Message switching

- - Packet Switching

Multiplexing & Demultiplexing:

- **Multiplexing** is a technique used to combine and send the multiple data streams over a single medium.
- Multiplexing is achieved by using a device called **Multiplexer (MUX)** that combines multiple input lines to generate a single output line. Multiplexing follows many-to-one, i.e., multiple input lines and one output line.
- **Demultiplexing:** The separation of combined single data stream to multiple inputs is called demultiplexing. It is achieved by using a device called **Demultiplexer (DEMUX)** available at the receiving end. DEMUX separates a signal into its component signals (one input and multiple outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

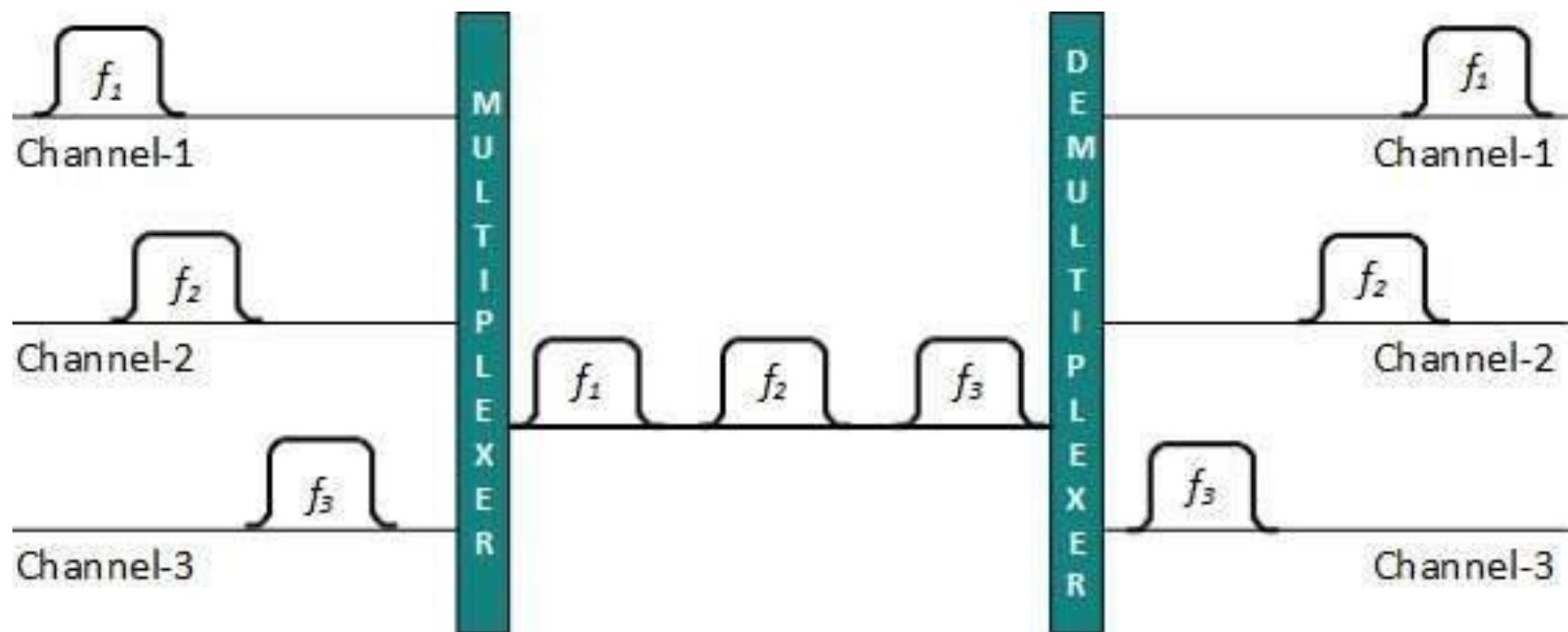
Multiplexing/De-multiplexing Device:



1 FDM (Frequency Division Multiplexing):

- When the carrier is frequency, FDM is used. FDM is an analog technology.
- FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel.
- Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other.
- One advantage of FDM is that, it supports bidirectional signaling on the same time i.e. transmission of data can be done from both side of cable at the same time.

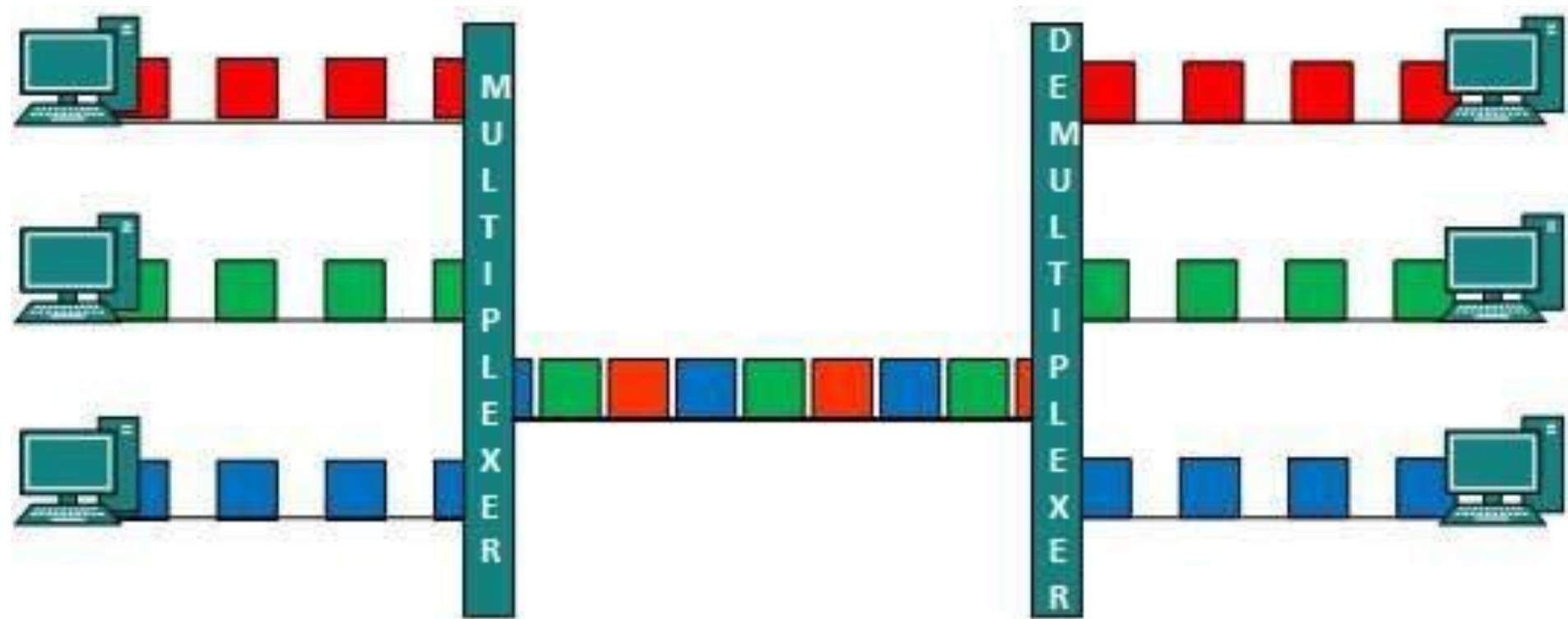
FDM:



2 TDM (Time Division Multiplexing) :

- It divides a channel into time slots that are allocated to data streams to be transmitted.
- TDM is applied primarily on digital signals but can be applied on analog signals as well.
- In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

TDM:



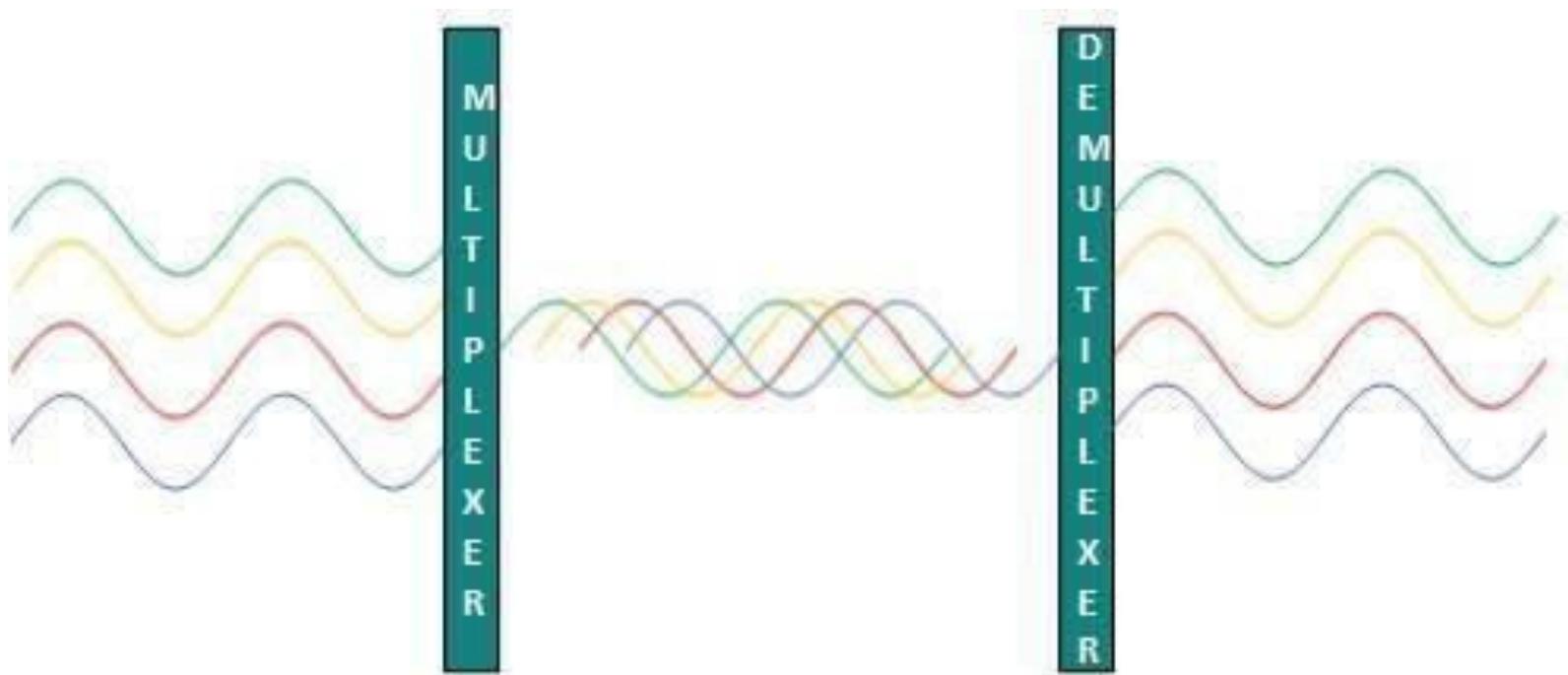
TDM

3 CDM (Code division multiplexing) :

- It is a networking technique in which multiple data signals are combined for simultaneous transmission over a common frequency band.
- When CDM is used to allow multiple users to share a single communications channel, the technology is called code division multiple access (CDMA).

4 WDM (Wavelength-Division Multiplexing):

- Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths.
- This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.



❖ Switching Techniques :

- Switching Techniques is similar to when you drive from your house to work. You can probably take a variety of routes, depending upon the events on the roadways, such as road work or traffic jams. Based on these conditions, you choose the route to take. This type of decision-making is what is done at the network level.
- Switching techniques are mechanism for moving data from one network segment to another. Switching technique is of three types:
 - Circuit switching
 - Message switching
 - Packet switching

Circuit Switching:

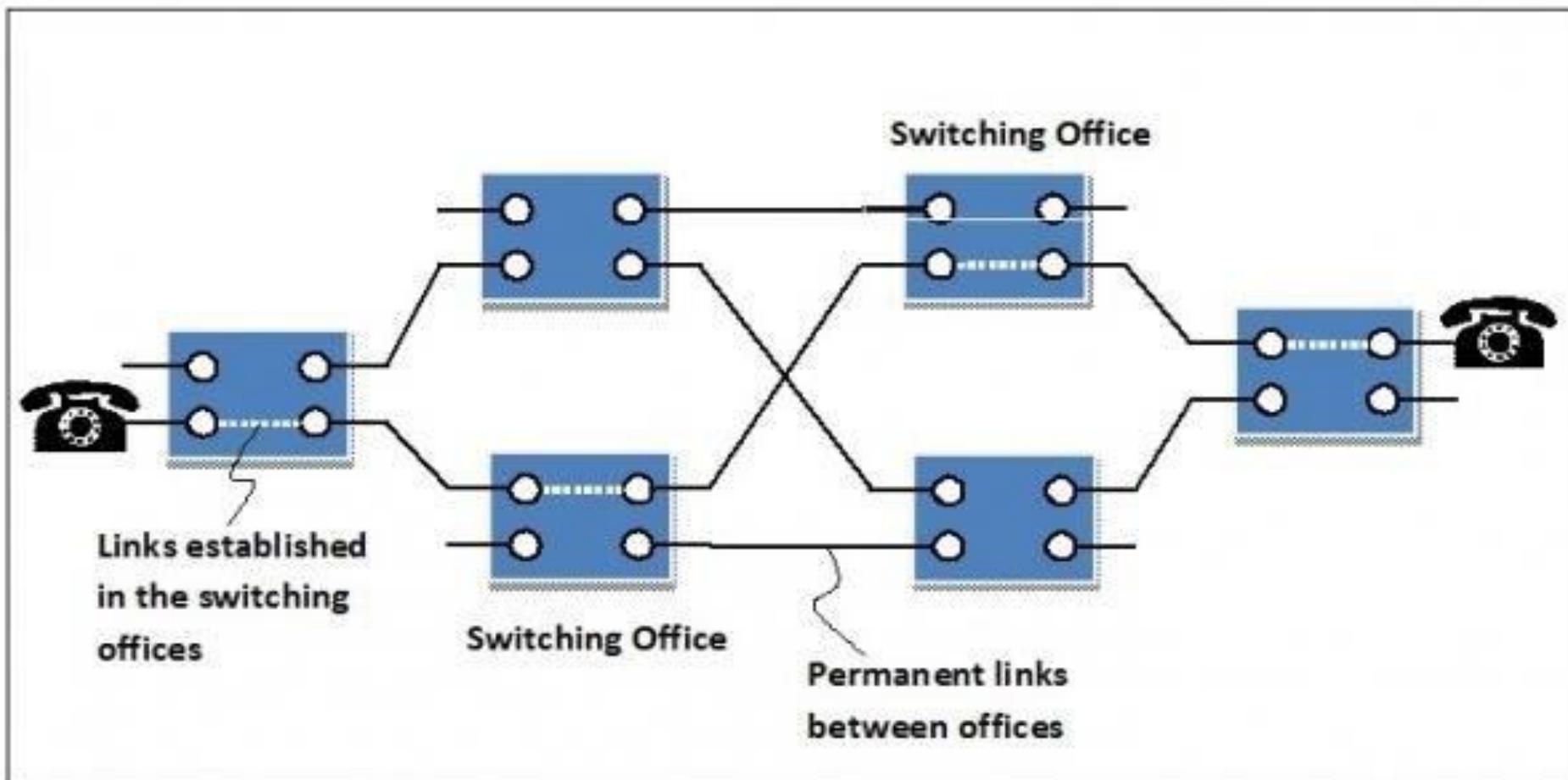
1) **Circuit Switching:** Circuit switching is a connection-oriented network switching technique. Here, a dedicated route is established between the source and the destination and the entire message is transferred through it.

■ **Phases of Circuit Switch Connection:**

- Circuit Establishment:** In this phase, a dedicated circuit is established from the source to the destination through a number of intermediate switching centers. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.
- Data Transfer :** Once the circuit has been established, data and voice are transferred from the source to the destination. The dedicated connection remains as long as the end parties communicate.

Circuit Switching:

- **Circuit Disconnection** : When data transfer is complete, the connection is relinquished. The disconnection is initiated by any one of the user. Disconnection involves removal of all intermediate links from the sender to the receiver.



Circuit Switching:

- The blue boxes represent the switching offices and their connection with other switching offices. The black lines connecting the switching offices represents the permanent link between the offices.
- When a connection is requested, links are established within the switching offices as denoted by white dotted lines, in a manner so that a dedicated circuit is established between the communicating parties. The links remains as long as communication continues.

Advantages:

- It is suitable for long continuous transmission, since a continuous transmission route is established, that remains throughout the conversation.
- The dedicated path ensures a steady data rate of communication.

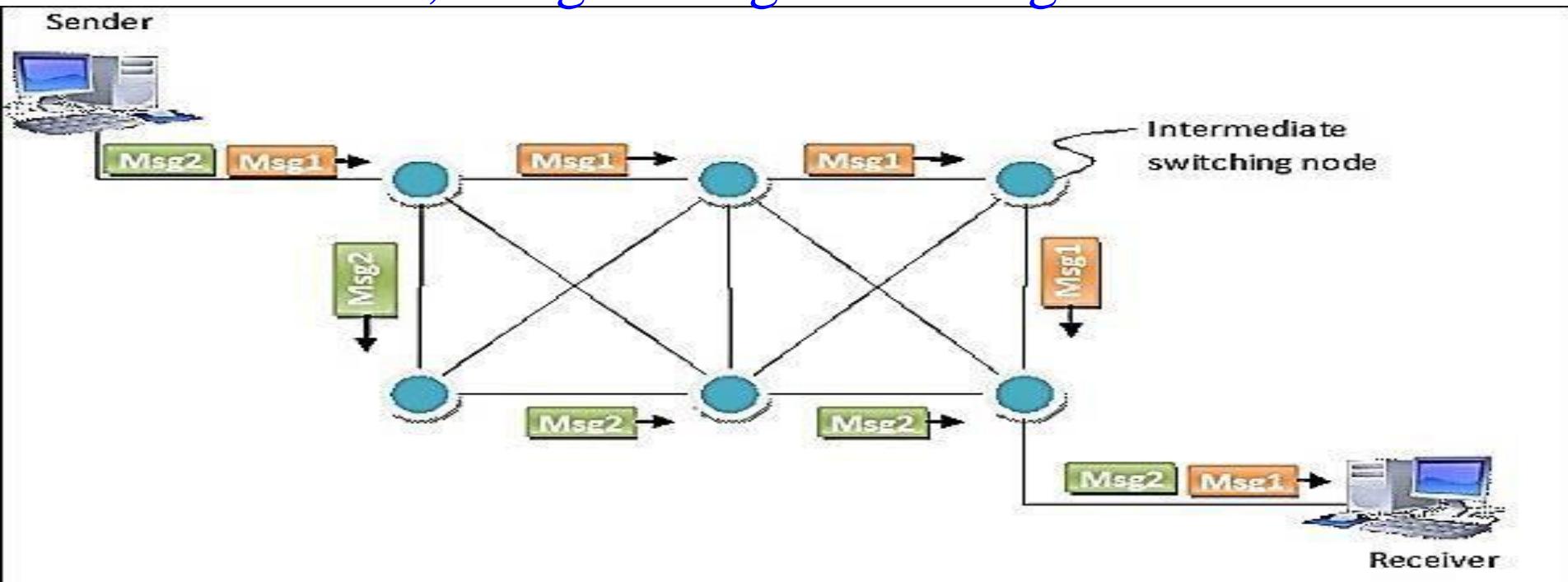
Circuit Switching:

- **Disadvantages**
 - Circuit switching establishes a dedicated connection between the end parties. This dedicated connection cannot be used for transmitting any other data, even if the data load is very low.
 - Bandwidth requirement is high even in cases of low data volume.
 - There is underutilization of system resources. Once resources are allocated to a particular connection, they cannot be used for other connections.
 - Time required to establish connection may be high.

Message switching:

2) Message switching: Message switching is a connectionless network switching technique where the entire message is routed from the source node to the destination node, one hop at a time. It was a precursor of packet switching.

The following diagram represents routing of two separate messages from the same source to same destination via different routes, using message switching.



Message Switching:

Process:

- Message switching treats each message as an individual unit. Before sending the message, the sender node adds the destination address to the message. It is then delivered entirely to the next intermediate switching node. The intermediate node stores the message in its whole, checks for transmission errors, inspects the destination address and then delivers it to the next node. The process continues till the message reaches the destination.
- In the switching node, the incoming message is not discarded if the required outgoing circuit is busy. Instead, it is stored in a queue for that route and retransmitted when the required route is available. This is called store and forward network.

Message Switching:

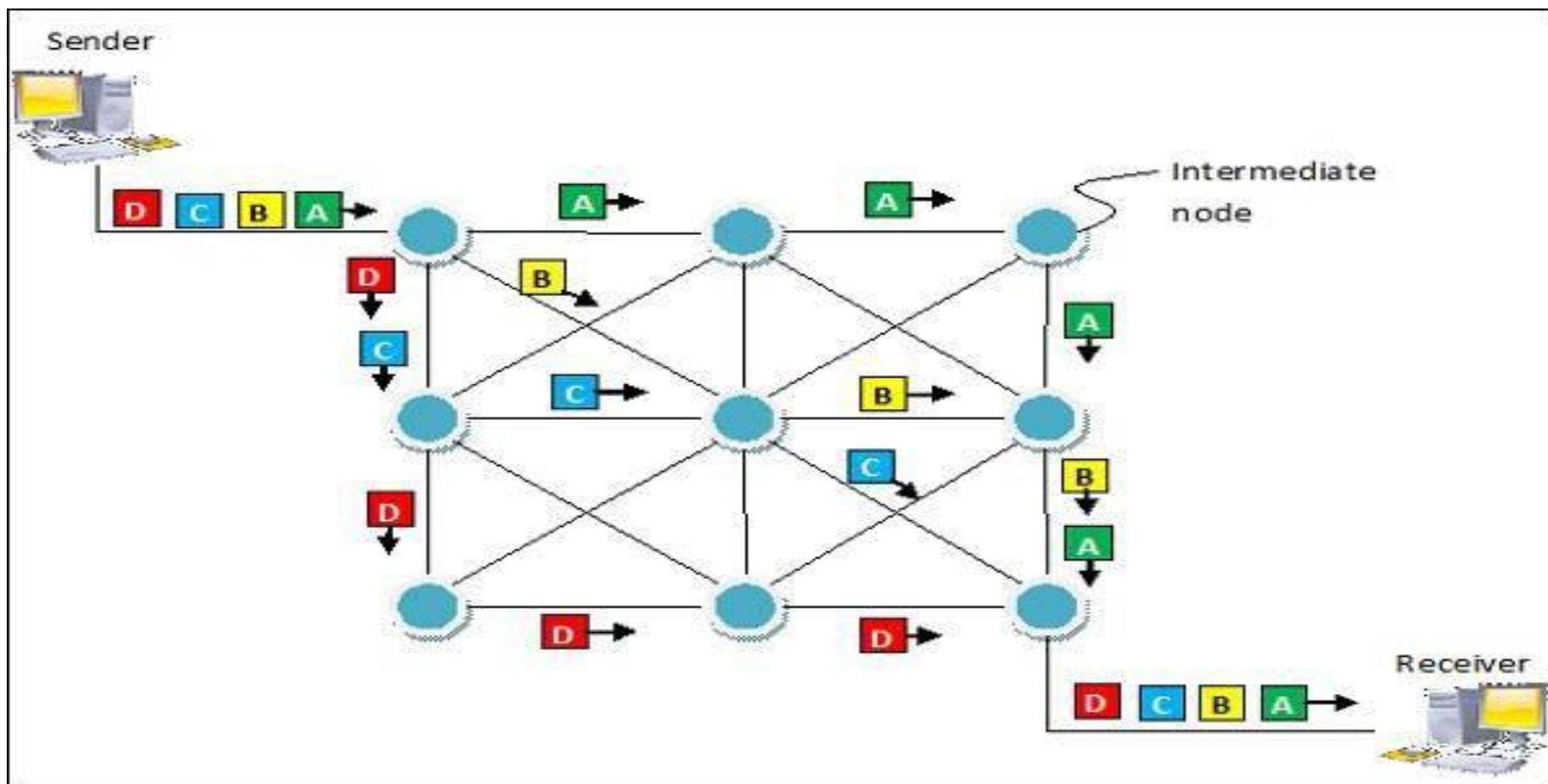
- **Advantages**
 - Sharing of communication channels ensures better bandwidth usage.
 - It reduces network bottleneck due to store and forward method. Any switching node can store the messages till the network is available.
 - Broadcasting messages requires much less bandwidth than circuit switching.
 - Messages of unlimited sizes can be sent.
 - It does not have to deal with out of order packets or lost packets as in packet switching.
- **Disadvantages**
 - In order to store many messages of unlimited sizes, each intermediate switching node requires large storage capacity.
 - Store and forward method introduces delay at each switching

Packet Switching:

- 3) **Packet switching** : Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication.
- **Process:** Each packet in a packet switching technique has two parts: a header and a shipment. The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination. The shipment carries the actual data.
 - A packet is transmitted as soon as it is available in a node, based upon its header information. The packets of a message are not routed via the same path. So, the packets in

Packet Switching:

- The process is diagrammatically represented in the following figure. Here the message comprises of four packets, A, B, C and D, which may follow different routes from the sender to the receiver



Packet Switching:

- **Advantages**
 - Delay in delivery of packets is less, since packets are sent as soon as they are available.
 - Switching devices don't require massive storage, since they don't have to store the entire messages before forwarding them to the next node.
 - Data delivery can continue even if some parts of the network faces link failure. Packets can be routed via other paths.
 - It allows simultaneous usage of the same channel by multiple users.
 - It ensures better bandwidth usage as a number of packets from multiple sources can be transferred via the same link.

Packet Switching:

- **Disadvantages**
 - They are unsuitable for applications that cannot afford delays in communication like high quality voice calls.
 - Packet switching high installation costs.
 - They require complex protocols for delivery.
 - Network problems may introduce errors in packets, delay in delivery of packets or loss of packets. If not properly handled, this may lead to loss of critical information.

Ch-5

Network Devices

Contents..

❖ **Cable Network type Devices:**

- Layer 1 Devices
 1. NIC (Network Interface Card) / LAN Card
 2. Modem
 3. DSL & ADSL
 4. HUB (Active, Passive, Smart Hub)
 5. Repeater
- Layer 2 Devices
 1. Switch (Manageable, Non-Manageable)
 2. Bridge (Source Route, Transactional)

Network Devices: Contents...

- Layer 3 Devices

1. Router
2. Layer 3 Switch
3. Brouter
4. Gateway
5. Network Printer

- ❖ **Wireless Network Devices:**

- Wireless Switch
- Wireless Router
- Access Point

Larger Devices _ 1. NIC :

- A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.
- **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

NIC:

- NIC cards are of two types:

I. Internal Network Cards: In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access.



NIC:

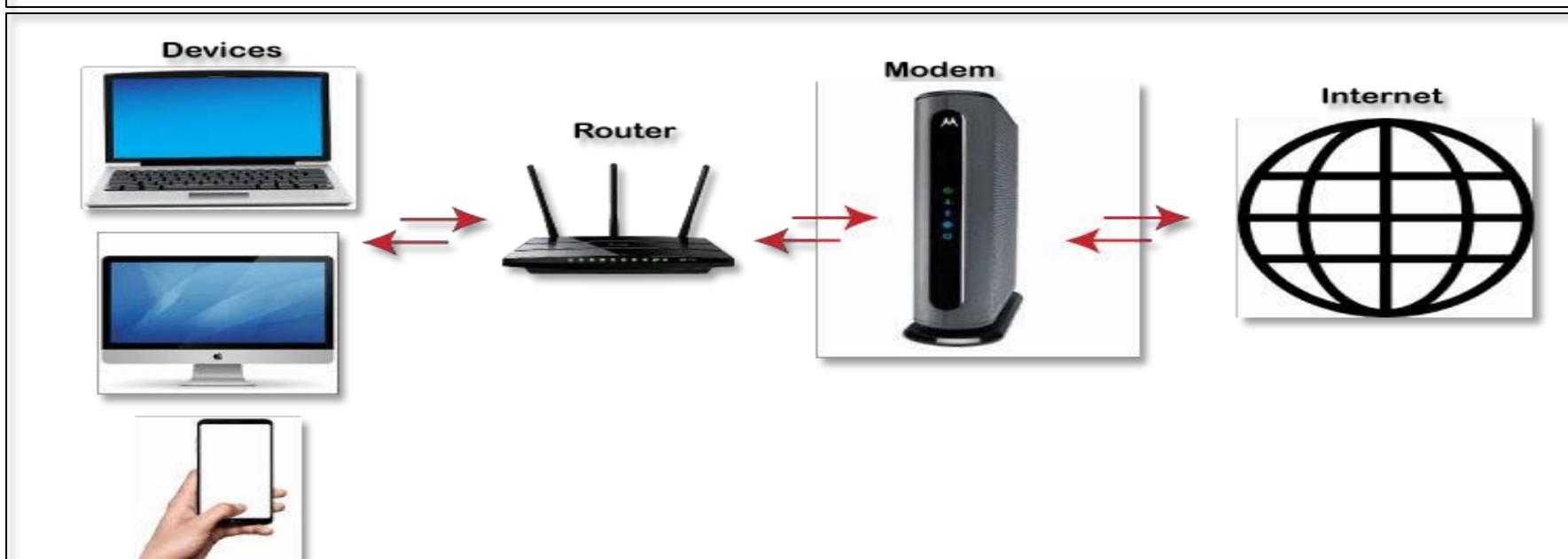
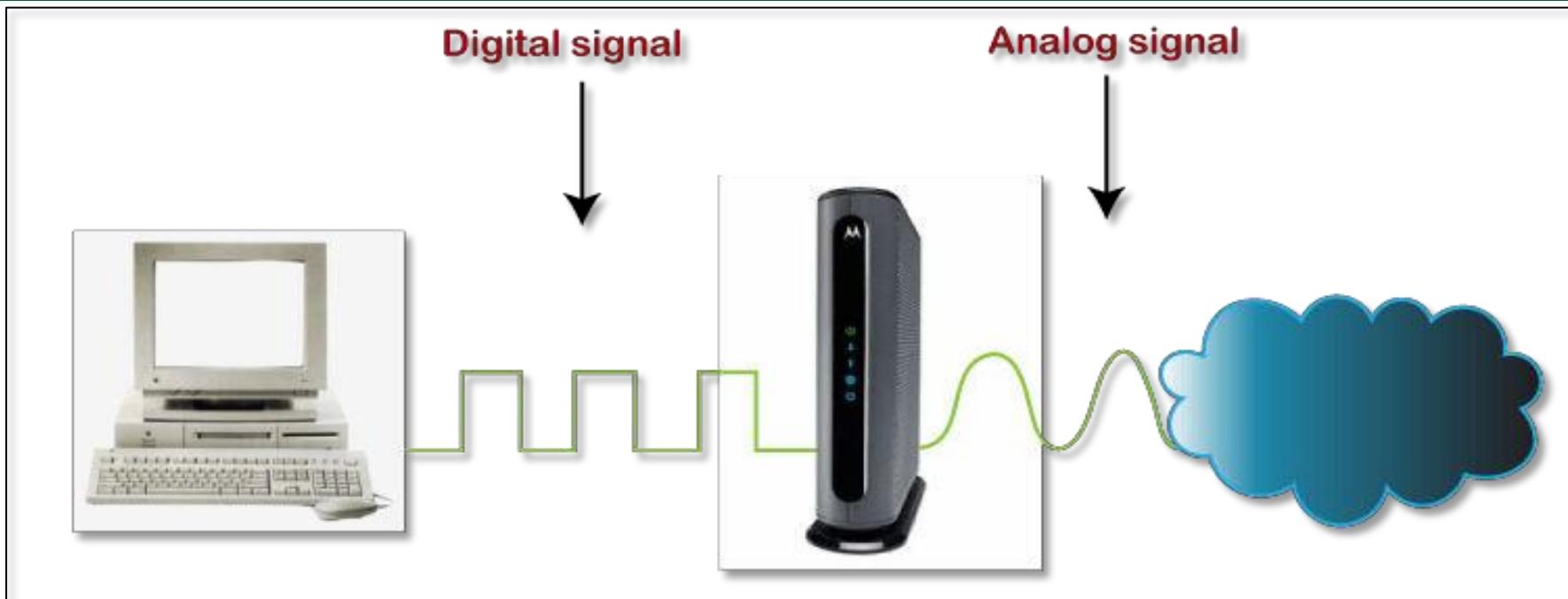
- **External Network Cards:** In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.



Layer1 Devices_2. Modem:

- Modem stands for Modulation Demodulation. A modem converts the digital data signals into analogue data signals. They can be installed within the computer in a development slot applicable for it.
- The most familiar example of a modem turns the digital' 1s and 0s' of a personal computer into sounds that can be transmitted over the telephone lines of plain old telephone system , and once received on the other side, converts those sounds back into 1s and 0s.
- Modems are classified according to the transmission method they use for sending and receiving data. The two basic types of modems are as follows:
 - Asynchronous modems

Modem:



□ Types Of Modems :

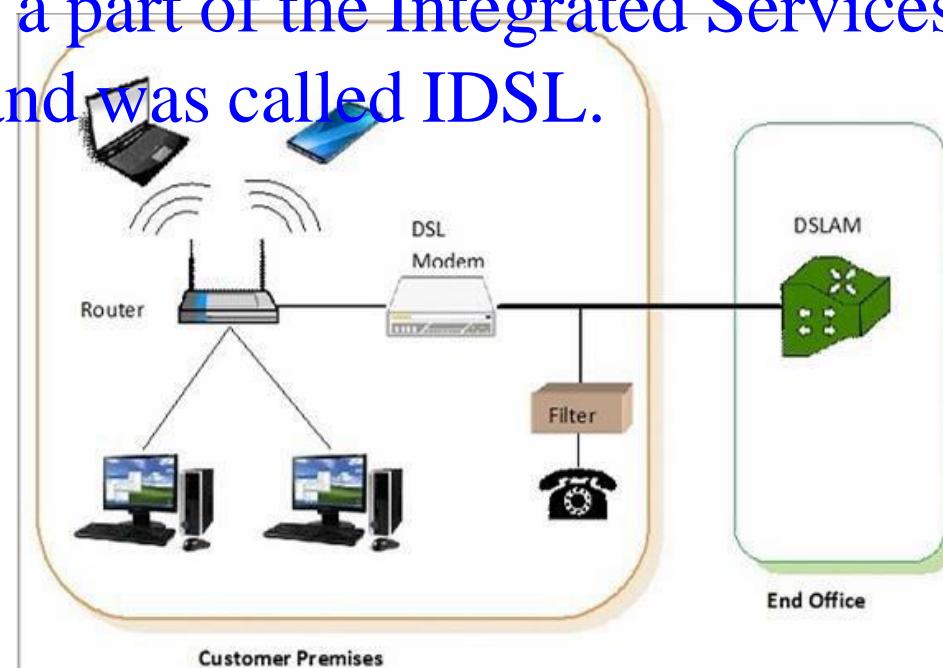
- Asynchronous modems :
 - The term asynchronous is usually used to describe communications in which data can be transmitted intermittently / irregularly rather than in a stable stream.
 - For ex. A telephone conversation is asynchronous because both parties can talk whenever they like.
 - The difficulty with asynchronous communications is that the receiver must have a way to distinguish between valid data and noise.
 - In computer communications this is usually accomplished through a special parity bit startbit and stopbit at the beginning and end of each piece of data

Types Of Modems :

- **Synchronous Modems :**
 - It does not use start stop mechanism for synchronization (match-status of sender and receiver)
 - It uses clocking mechanism to synchronize the receiving and transmitting ends.
 - This synchronization is accomplished with in three methods.

3. DSL & ADSL:

- **Digital Subscriber Line (DSL)** is a communication technology that offers high – bandwidth digital communication over standard telephone lines formed of copper wires.
- DSL is a family of technologies under the general name of xDSL, for various x, like ADSL, HDSL, and RADSL.
- Originally, it was a part of the Integrated Services Digital Network (ISDN) and was called IDSL.

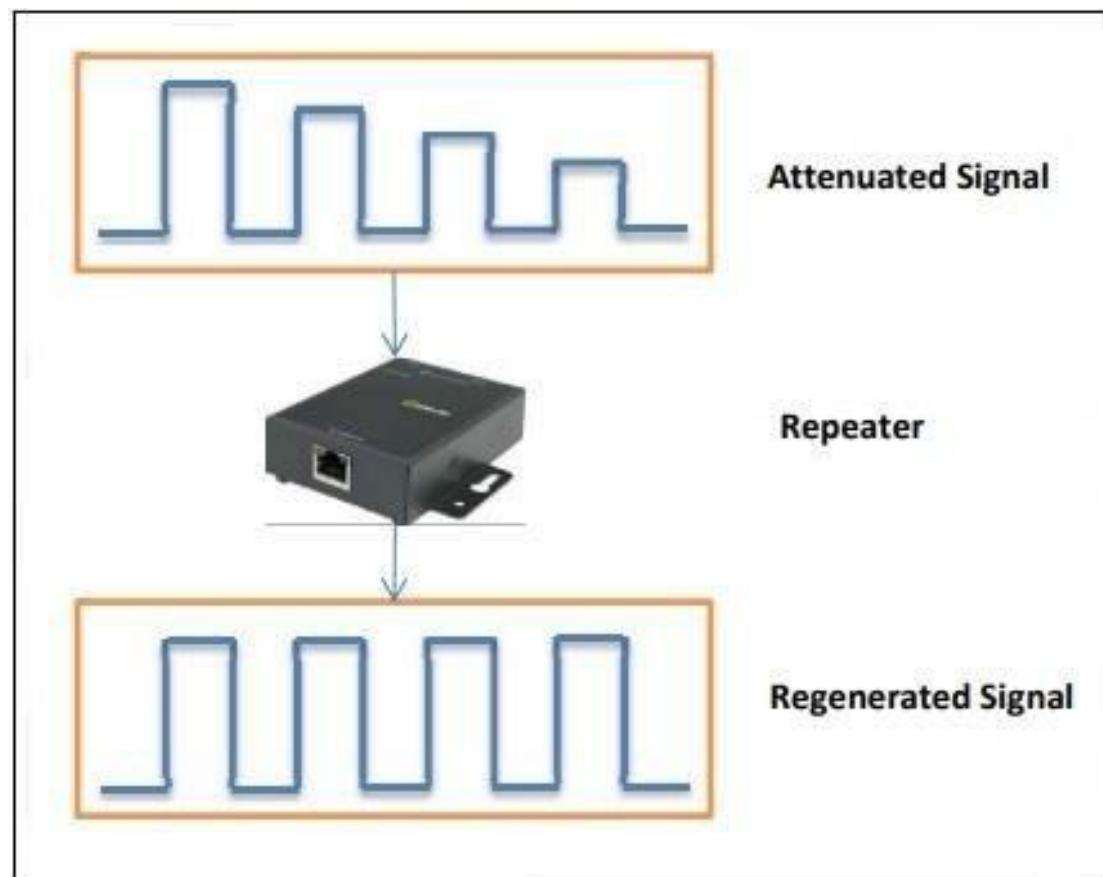


ADSL:

- **Asymmetric Digital Subscriber Line** (ADSL) is a type of broadband communications technology that transmits digital data at a high bandwidth over existing phone lines to homes and businesses.
- In order to access ADSL, a Digital Subscriber Line modem (DSL modem) is installed at the client side. The DSL modem sends data bits over the local loop of the telephone network. The local loop is a two – wire connection between the subscriber's house and the end office of the telephone company. The data bits are accepted at the end office by a device called Digital Subscriber Line Access Multiplexer (DSLAM).

Layer1 Devices_4. Repeater:

- Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.

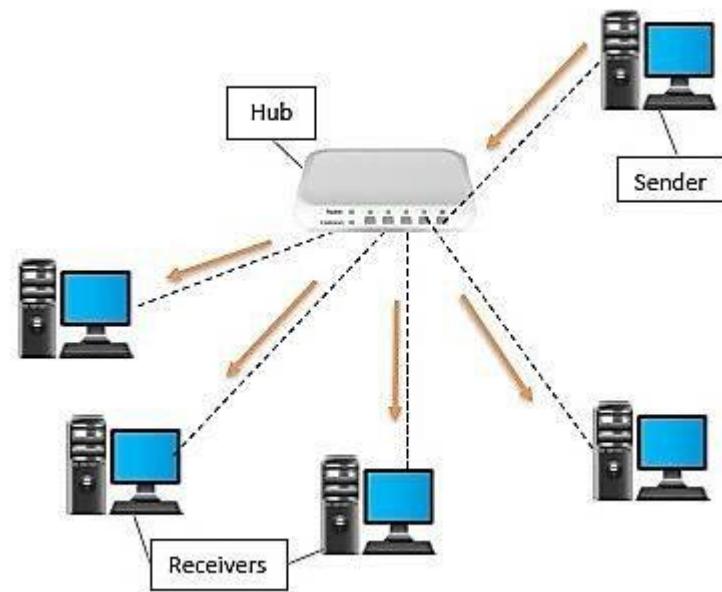


Repeater :

- **Types of Repeaters:**
 - According to the types of signals that they regenerate, repeaters can be classified into two categories:
 - **Analog Repeaters** – They can only amplify the analog signal.
 - **Digital Repeaters** – They can reconstruct a distorted signal.
 - According to the types of networks that they connect, repeaters can be categorized into two types:
 - **Wired Repeaters** – They are used in wired LANs.
 - **Wireless Repeaters** – They are used in wireless LANs and cellular networks.
 - According to the domain of LANs they connect, repeaters can be divided into two categories:
 - **Local Repeaters** – They connect LAN segments separated by small distance.

Layer1 Devices_5. Hubs:

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



Hubs:

- **Passive Hubs:**
 - It does not contain any electronic component and do not process the data signal in any way.
 - It only combines the signal from several network cable segments.
 - The distances between computer and hub must be less compare to distances in active hub.
- **Active Hubs:**
 - It is an electronic component that can amplify and clean up the electronic signals that flow between devices on the network.
 - This process of cleaning up the signals is called signal regeneration.

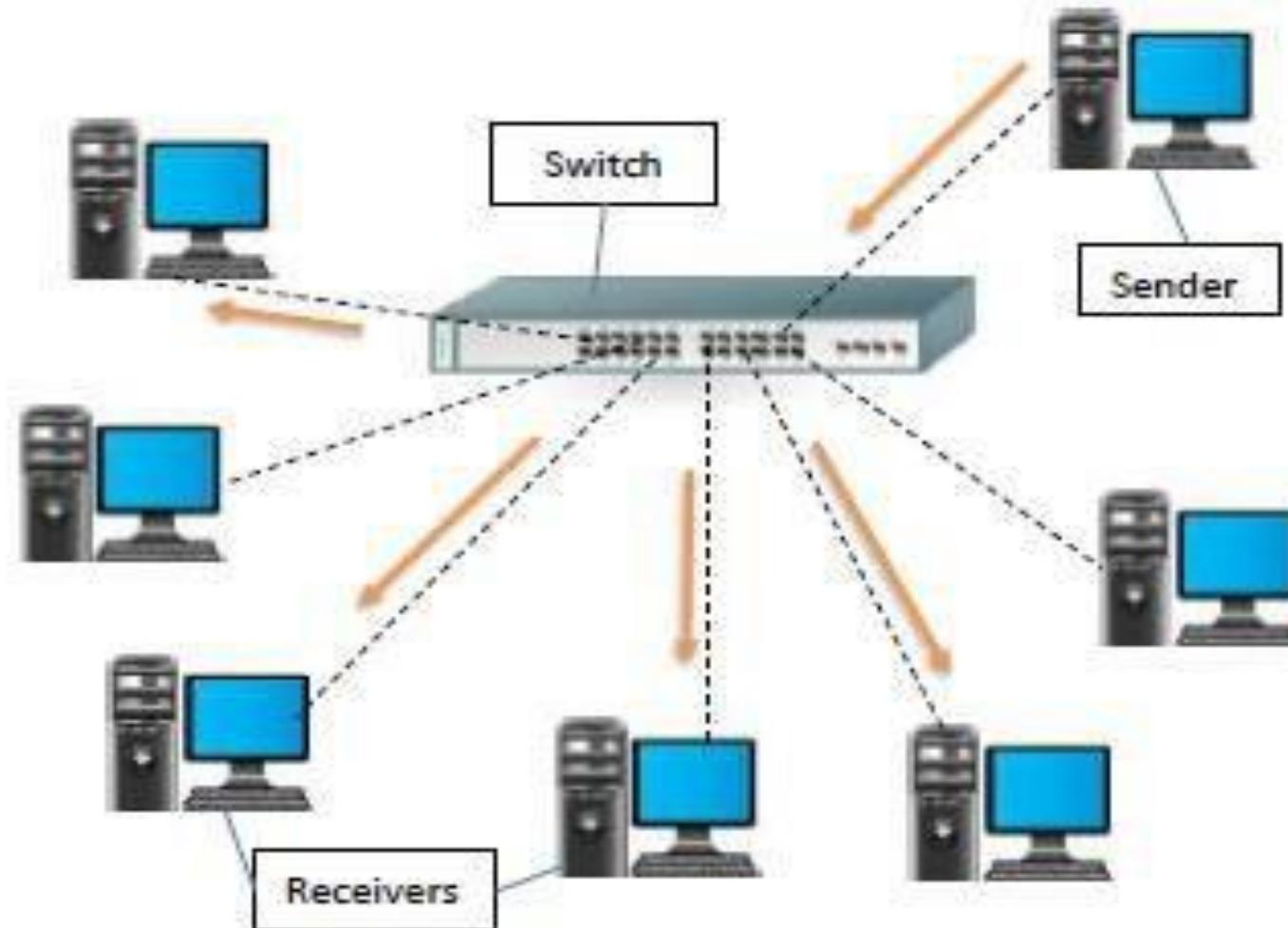
Hubs:

- Intelligent / Smart Hubs :
- In addition to signal regeneration, intelligent hubs perform some network management and intelligent path selection.
- Intelligent hubs are enhanced active hubs.

Layer 2 Devices _ 1. Switches:

- Switches are connects devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.
- A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.

Switches:



Multicasting by a Switch

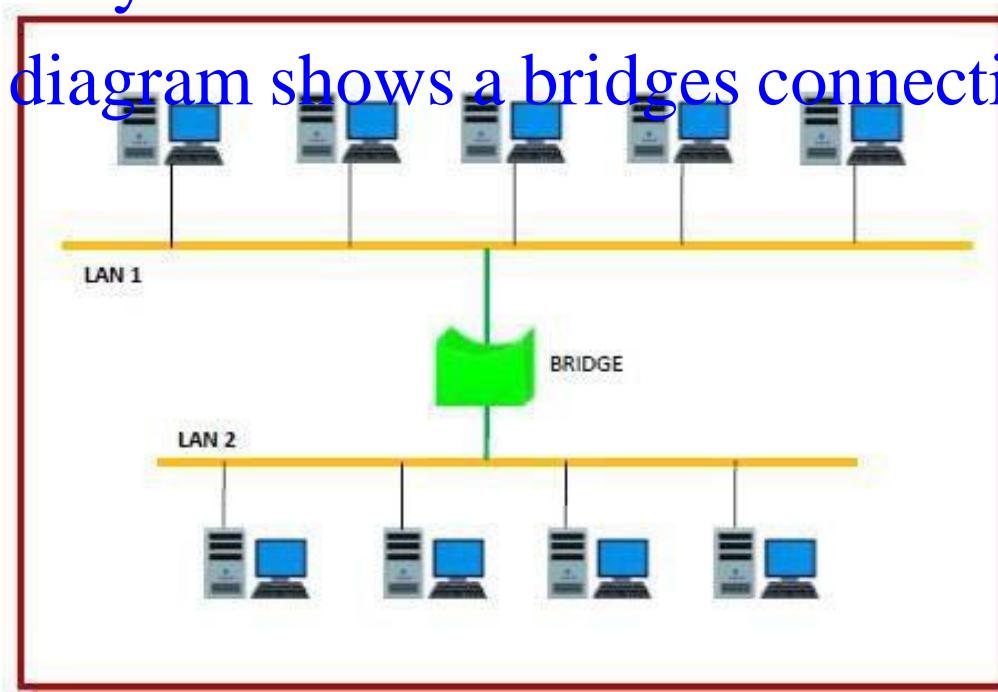
Switches:

- **Features of Switches**
- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It uses MAC addresses to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
- There are two types of switches:
 1. **Manageable Switch:** These are costly switches that are used in organizations with large and complex networks. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
 2. **Non-Manageable Switch:** These are inexpensive switches commonly

Layer 2 Devices _ 2. Bridges :

- A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of combining or linking networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.

- The following diagram shows a bridges connecting two LANs –



Bridges :

- **Usages of Bridge:**
 - By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
 - By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
 - In cases where the destination MAC address is not available, bridges can broadcast data frames to each node.

Advanced Bridges :

- Source Routing Bridge:** Source routing bridge decides the route between two hosts. Source routing bridge uses the MAC destination address of a frame to direct it by the source routing algorithm. In source routing, the route over which the frame is to send is Known to every station on the extended LAN. The routing information is stored in the frames.
- Transactional Routing Bridge:** This bridge automatically maintains a routing table and update table in response to maintain changing topology.
- This also called Transparent bridge is easy to use, install the bridge and no software changes are needed in hosts. In all the cases, transparent bridge flooded the broadcast and multicast frames.

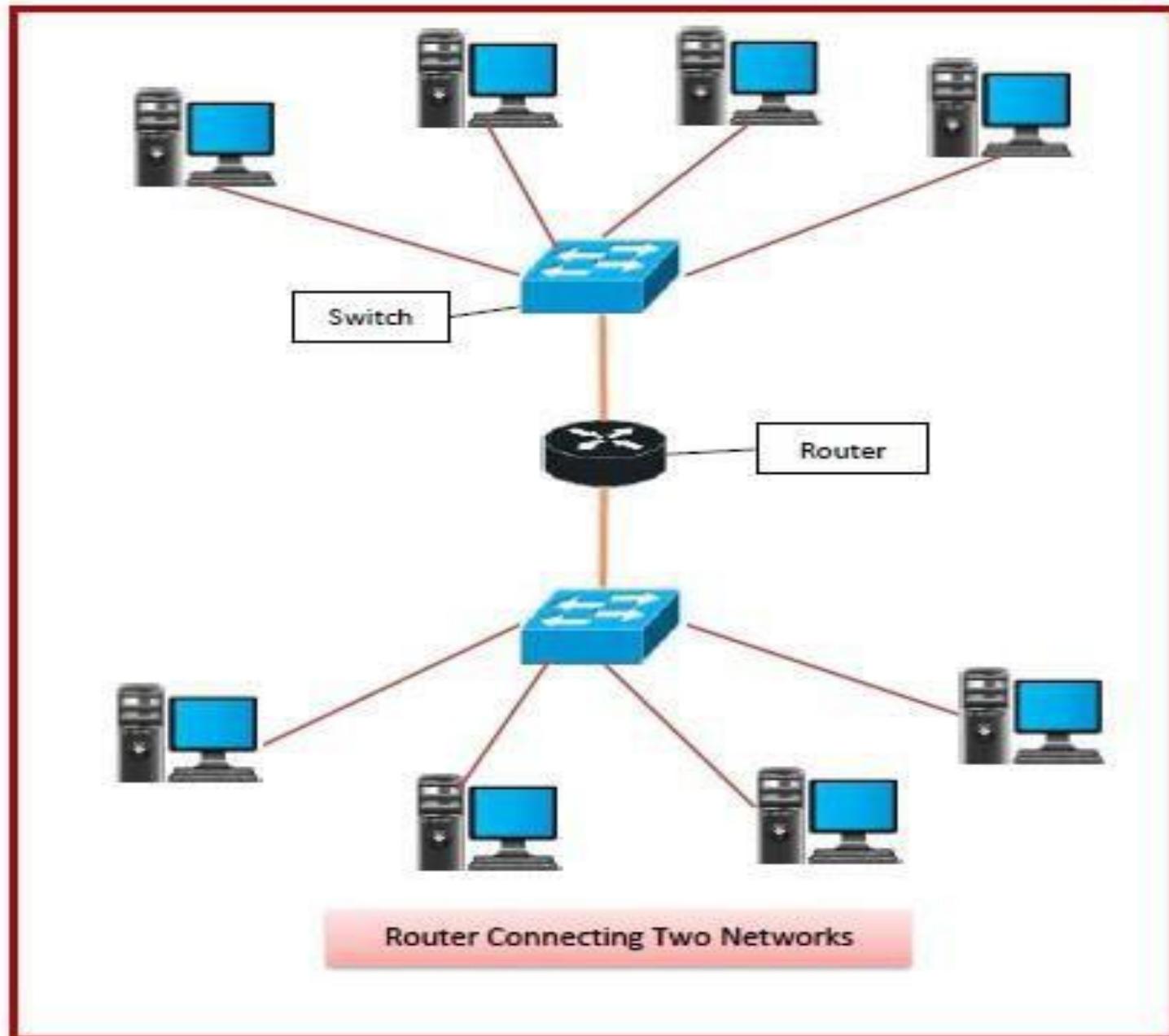
Layer 3 Devices _ 1. Router :

- Router are combination of hardware and software and used to connect separate network to form an internet work .
- Just as a switch connects multiple devices to create a network, a router connects multiple switches, and their respective networks, to form an even larger network. These networks may be in a single location or across multiple locations.
- When building a small business network, you will need one or more routers. In addition to connecting multiple networks together, the router also allows networked devices and multiple users to access the Internet.
- Ultimately, a router works as a dispatcher, directing traffic and choosing the most efficient route for information, in the form of data packets, to travel across a network. A router connects your business to the world, protects information

Router:

- **Features of Routers**
 - A router is a layer 3 or network layer device.
 - It connects different networks together and sends data packets from one network to another.
 - A router can be used both in LANs and WANs.
 - Routers are more expensive than other networking devices like hubs, bridges and switches.
 - A router is a devices that extracts the destination of a packet it receives, selects the best path to that destination and forwards data packets to the next devices along this path.
 - There are main two type :
 - Static Routers.
 - Dynamic Routers.

☐ Router:



Layer 3 Devices _ 2 Layer-3 Switch

- Layer-3 Switch Operate on layer 3 (Network Layer) of OSI model that's why it is called Layer-3 Switch.
- It Route Packet with help of IP address
- It can able to perform functioning of both 2 layer and 3 layer switch.
- Layer-3 switch Mostly Used to implement VLAN (Virtual Local area network)
- This takes time to examine data packets before sending them to their destination.
- It can communicate within or outside network.

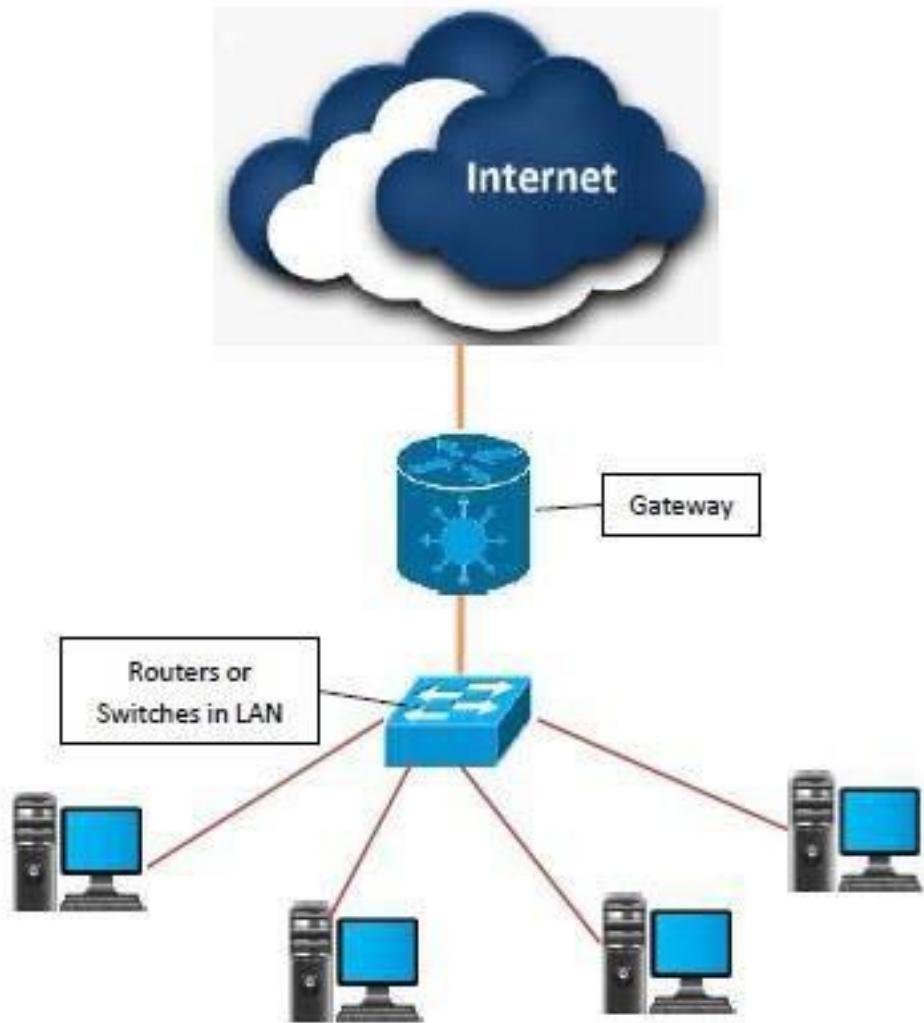
Layer-3 Devices_4. Brouters:

- A brouter called Bridge-Routher is a networking device that functions both as a bridge and a router. It can forward data between networks (serving as a bridge), but can also route data to individual systems within a network (serving as a router).
- Brouter stores routing table when it is configured as a router and stores MAC address when configured as a bridge.
- Brouter transmits data in the form of packets when it is configured as a router and It transmits data in the form of frames when configured as a bridge.
- Brouter is full duplex when it is configured as a router and it is half duplex when configured as a bridge

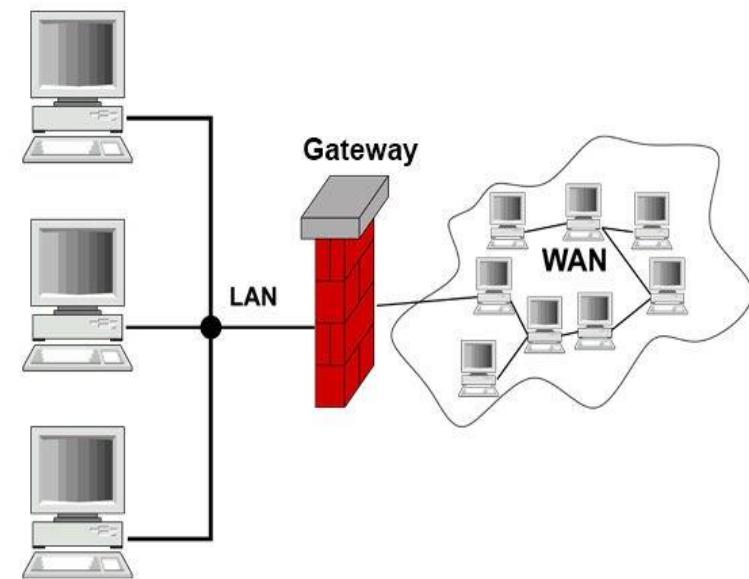
Layer-3 Devices_4. Gateway :

- A gateway is basically a device or a hardware which acts like a “gate” among the networks. So it can also be defined as a node which acts as an entrance for the other nodes in the network.
- It is also responsible for enabling the traffic flow within the network. Gateway uses more than one protocol for communication thus its activities are much more complex than a switch or a router.
- So a gateway is basically a device that is used for the communication among the networks which have a different set of protocols and is responsible for the conversion of one protocol into the other.
- The additional features provided by a gateway are network

Gateway:

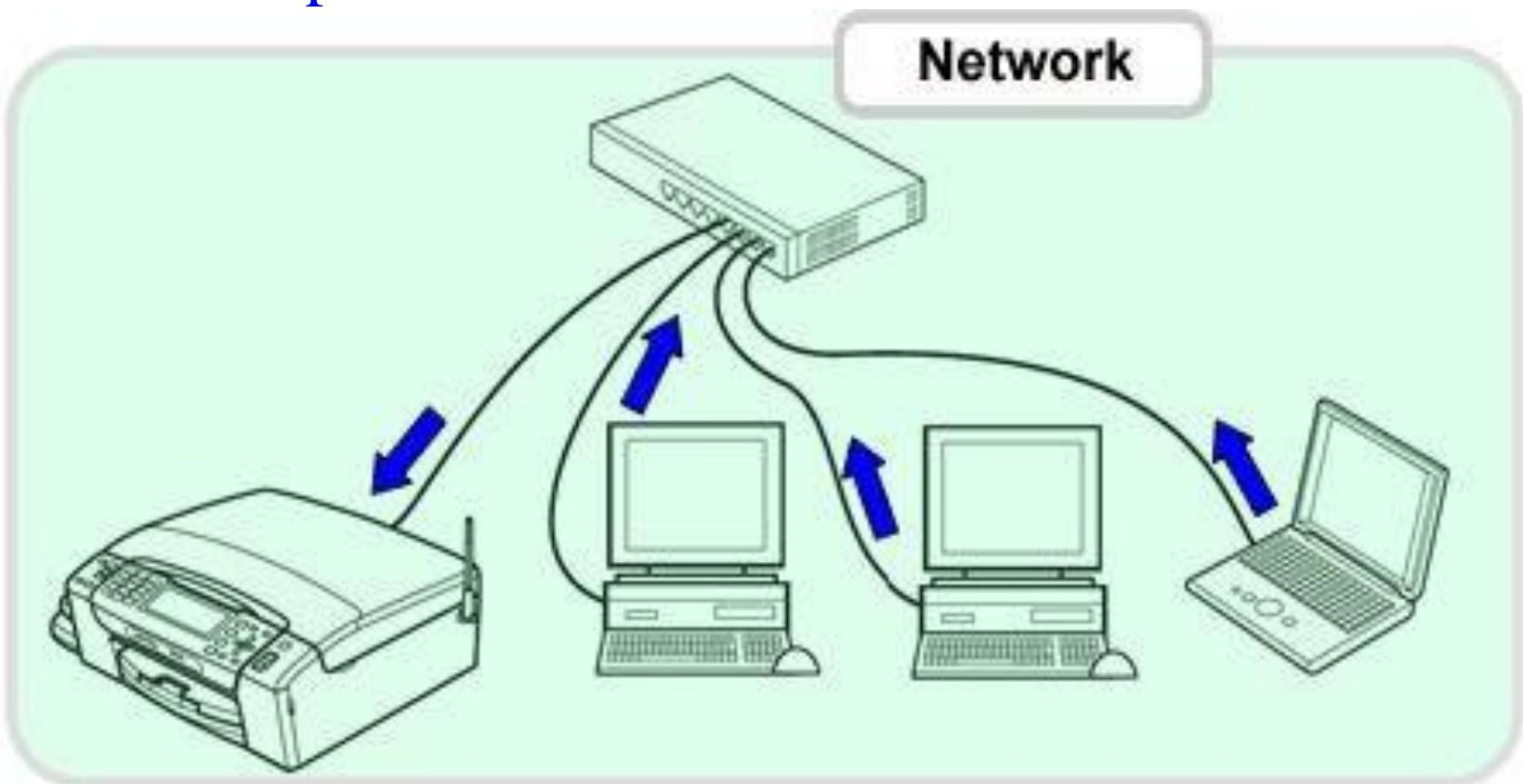


Gateway between a LAN and Internet



Layer-3 Devices_5. Network Printer:

- A network printer is a printer that is accessible by network connection, making it usable by other computers connected to the network. The printer may have its own network connection or use a local network to connect to a single, dedicated computer.



❖ Wireless Network Devices:

- **Wireless Switch / Router:**
- A wireless Switch / Router is a device that performs the functions of a wired switch / router but also includes the functions of a wireless access point. It is commonly used to provide access to the Internet or a computer network. It does not require a wired link, as the connection is made wirelessly, via radio waves. It can function in a wired LAN (local area network), in a wireless-only LAN (WLAN), or in a mixed wired/wireless network, depending on the manufacturer and model.

Wireless Network Devices:

□ **Access Point:**

- In computer networking, a **wireless access point (WAP)** is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards.
- The Access Point usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.

Assignment :

- 1 What is NIC ?
- 2 Explain Modems.
- 3 Write a Short Note On :Bridge & Router.
- 4 Define in Repeater.
- 5 Explain HUB.
- 6 What is Gateway.

Ch-6

Network Protocols

Ch – 6 _ Network Protocols, Content...

❖ Packets

❖ Protocol

- ❑ Connection Oriented Protocol – TCP
- ❑ Connection Less Protocol – UDP

❖ TCP/IP Stack

- HTTP
- FTP
- SMTP
- POP3
- SNMP
- TELNET
- ARP
- RARP

Ch – 6 _ Network Protocols, Content...

- ❖ **IPX/SPX**
 - ❖ Apple Talk
 - ❖ NetBIOS Names Protocol
 - ❖ L2CAP, RFCOMM Protocol

❖ Packets:

- **What is a network packet?**
 - A network packet is a small amount of data sent over Transmission Control Protocol/Internet Protocol (TCP/IP) networks. The packet size is around 1.5 kilobytes for Ethernet and 64 KB for IP Payload.
 - A packet is the unit of data routed between an origin and a destination on the internet or other packet-switched network.
- **How does a network packet work?**
 - When any file, like an email message, HTML file, GIF file or URL request is sent on the internet, it is broken down into small pieces/bits, or bytes. The TCP layer of TCP/IP divides the file into bytes for efficient routing. Typically, a packet holds 1,000 to 1,500 bytes of information.

packets:

- Each packet is separately numbered and includes the internet address of the destination. The individual packets for a given file may take different routes over the internet. Upon arrival at their destination, the packets are reassembled into the original file by the TCP layer at the receiving end.
- Depending on the type of network, packets can also be referred to by names such as *block*, *cell*, *frame* or *segment*.

□ What are the parts of a network packet?

- Network packets are made up of three different parts: header, payload and trailer. Conceptually, they're like a postal package. In this scenario, the header is the box/envelope, the payload is content and the trailer is the signature.

Packets:

➤ The header contains instructions related to the data in the packet. These instructions can include the following:

FRAME	PACKET	SEGMENT	Structure of a packet
Receiver's MAC address	Sender's MAC address	Receiver's IP address Sender's IP address TCP Protocol Port Number DATA	FCS
Ethernet "Frame" OSI layer 2 - Data linklayer	IP "Packet" OSI layer 3 - Network layer	TCP "Segment" OSI layer 3 - Transportlayer	
Sender's IP address Receiver's IP address Protocol Packet number	96 bits		Header <ul style="list-style-type: none">■ Internet protocol■ Size of the header and payload■ Source and destination IP address■ 16 bit identification number■ 96 bits
Data	896 bits		Payload <ul style="list-style-type: none">■ Content or data of the packet■ 896 bits
Data to show end of packet Error correction	32 bits		Trailer <ul style="list-style-type: none">■ Signature of the packet■ Error checking■ 32 bits

❖ Protocol:

□ What is Protocol?

- In Order to make communication successful between devices , some rules and procedures should be agreed upon at the sending and receiving ends of the system. Such rules and procedures are called as Protocols . Different types of protocols are used for different types of communication.
- In other words, protocols are the software or like a device drivers those governs some rules that how the data would be transferred over the particular network.
- **For Example:** If we are driving our vehicle over the road, there must be some rules that we have to follow; i.e. we must keep left our vehicle on the road, ensure the speed limit according the shine board, follow the traffic signals etc.
- If we are not following any of the rule, there may be a chances of accident. Likewise such an example, Protocols ensures the rules for

entire data transmissions.

Types of Protocols: TCP , UDP

□ Connection Oriented Protocol – TCP :

- TCP stands for **Transmission Control Protocol**. It is a transport layer protocol that facilitates the transmission of packets from source to destination.
 - It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network.
 - This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP
- **Functionality:**
- ✓ The main functionality of the TCP is to take the data from the application layer. Then it divides the data into a several packets, provides numbering to these packets, assign a port number to each packet and finally transmits these packets to the destination.

Connection Oriented Protocol – TCP

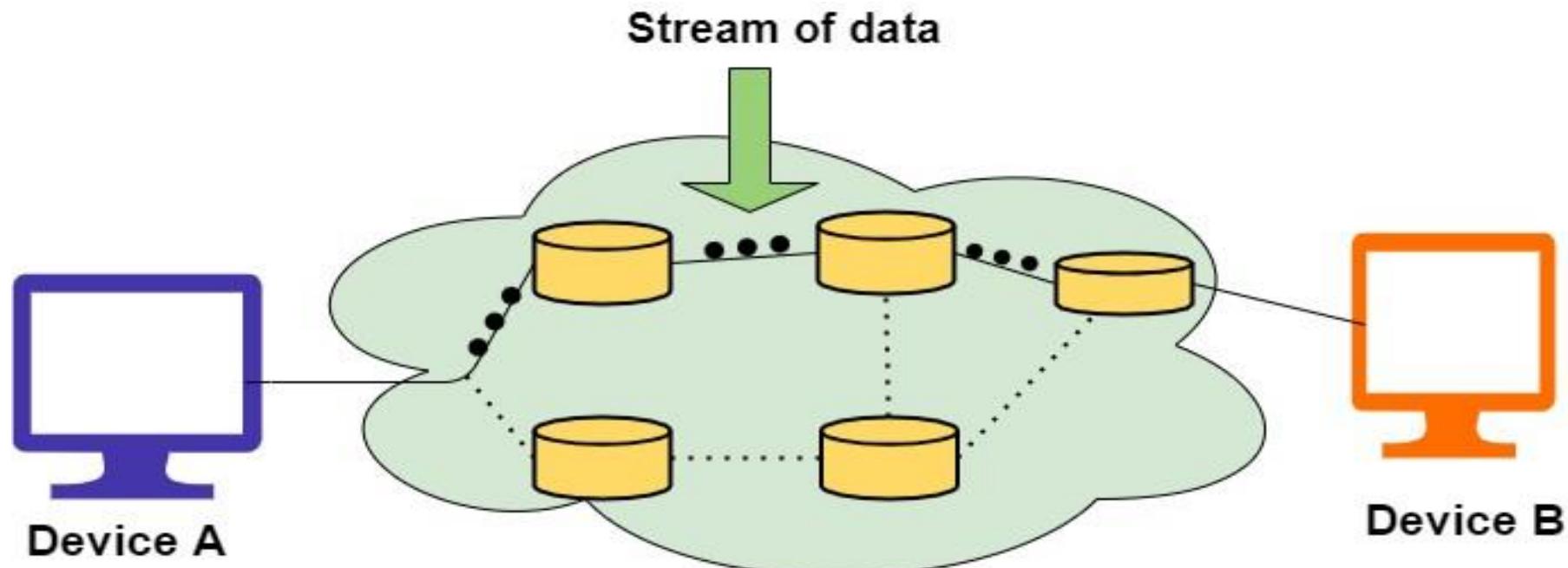
- ✓ The TCP, on the other side, will reassemble the packets and transmits them to the application layer.
- ✓ As we know that TCP is a connection-oriented protocol, so the connection will remain established until the communication is not completed between the sender and the receiver.

○ Features:

- ✓ **Reliable:** TCP is a reliable protocol as it follows the flow and error control mechanism. It also supports the acknowledgment mechanism. In the acknowledgment mechanism, the receiver sends either positive or negative acknowledgment to the sender so that the sender can get to know whether the data packet has been received or needs to resend.

Connection Oriented Protocol – TCP

- ✓ **Order of the data is maintained:** This protocol ensures that the data reaches the intended receiver in the same order in which it is sent. It orders and numbers each segment so that the TCP layer on the destination side can reassemble them based on their ordering.
- ✓ **Full-Duplex:** It is a full-duplex means that the data can transfer in both directions at the same time.



□ Connection Less Protocol – UDP

- **Connection Less Protocol – UDP:** The UDP stands for User Datagram Protocol. The David P. Reed developed the UDP protocol in 1980. It is a part of the TCP/IP protocol, so it is a standard protocol over the internet.
 - UDP does not provide message acknowledgments; rather, it simply transports datagrams(Data Packets).
 - The UDP protocol allows the applications to send the messages in the form of datagrams from one machine to another machine over the Internet Protocol (IP) network.
 - UDP is a connectionless protocol as it does not require any virtual circuit to transfer the data.

□ Connection Less Protocol – UDP

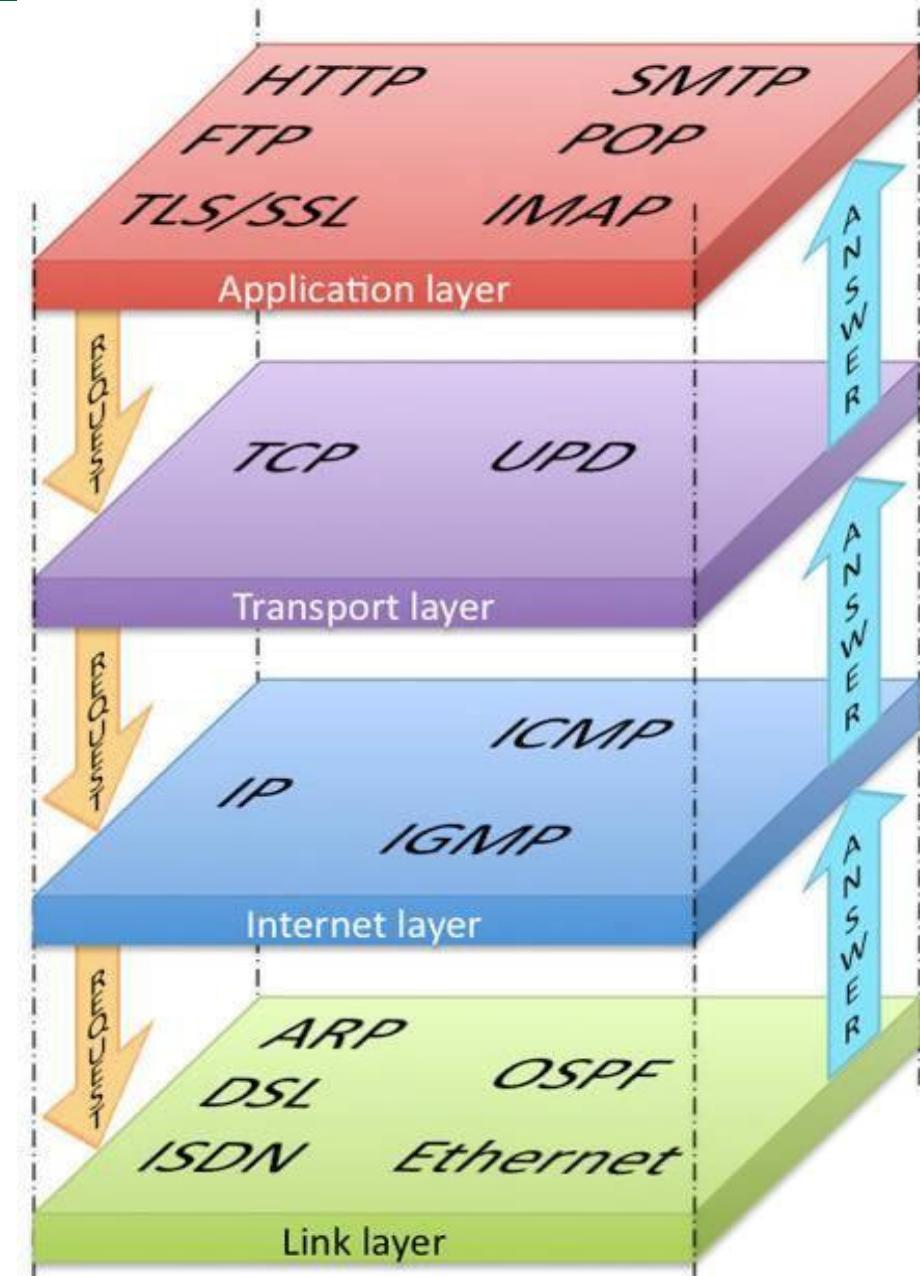
○ Features:

- ✓ **No Acknowledgement:** the receiver does not send the acknowledgment for the received packet, and the sender also does not wait for the acknowledgment for the packet that it has sent.
- ✓ **Connectionless:** It does not create a virtual path to transfer the data. So, packets are sent in different paths between the sender and the receiver, which leads to the loss of packets or received out of order.
- ✓ **Faster transmission:** UDP enables faster transmission. But there is a chance that the individual packet is lost, which affects the transmission quality. Whereas if the packet is lost in TCP connection, that packet will be resent, so it

guarantees the delivery of the data packets.

❖ TCP/IP Stack:

- ❑ The TCP/IP Stack, or the internet protocol suite, is a set of communication protocols used by the Internet or similar networks. Originally resulting from research at DARPA (Defense Advanced Research Projects Agency). The TCP/IP stack has gradually grown to include a suite of protocols.
- ❑ The TCP/IP Stack includes Several protocols as shown in Figure.



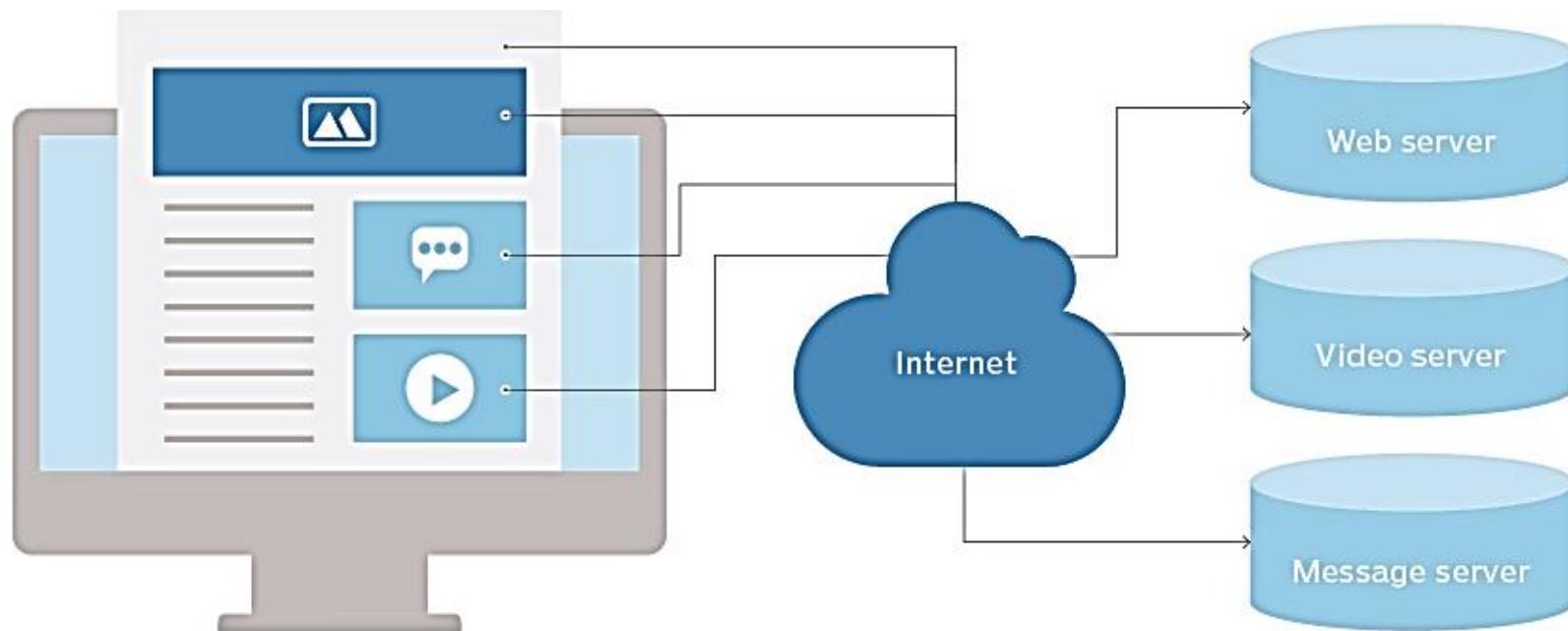
1. HTTP (Hypertext Transfer Protocol):

- It is a protocol used to access the data on the World Wide Web (www)
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext.
- This protocol is known as Hypertext Transfer Protocol because of its efficiency that allows us to use in a hypertext(Jumpy/Jerky) environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like (Symbolic) format.

HTTP:

- **Features:**
- **Connectionless protocol:** HTTP client sends a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** any type of data can be sent by HTTP as both the client and the server know how to handle the data content.
- **Stateless:** The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can keep information between different requests within the web pages.

How HTTP works



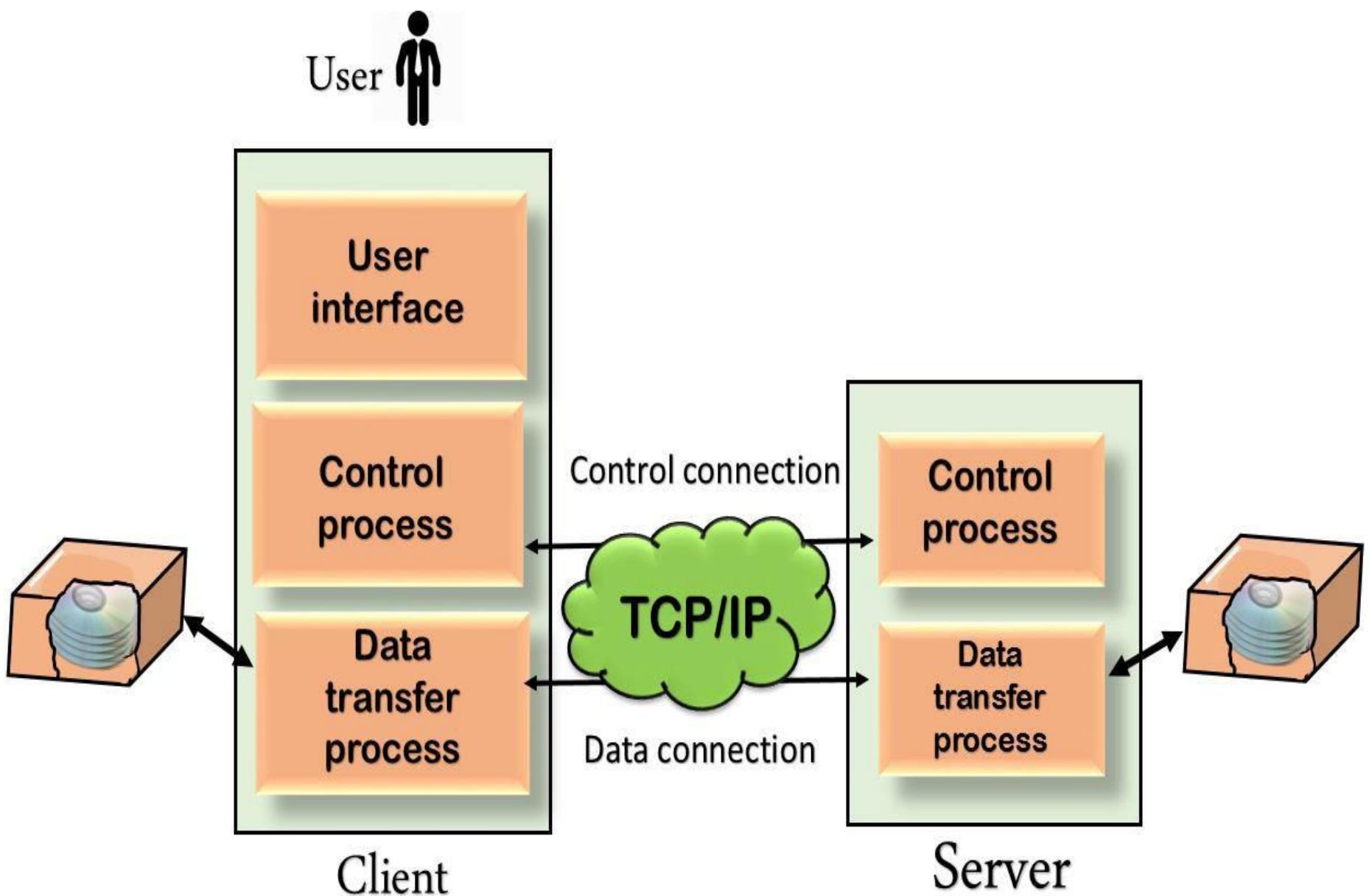
2. FTP (File Transfer Protocol):

- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers, It provides the sharing of files.
- Transferring files from one system to another is very simple but sometimes it can cause problems. For example, two systems may have different file standards. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

FTP

- **Control Connection:** For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of control connection. The control connection is initiated on port number 21.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP



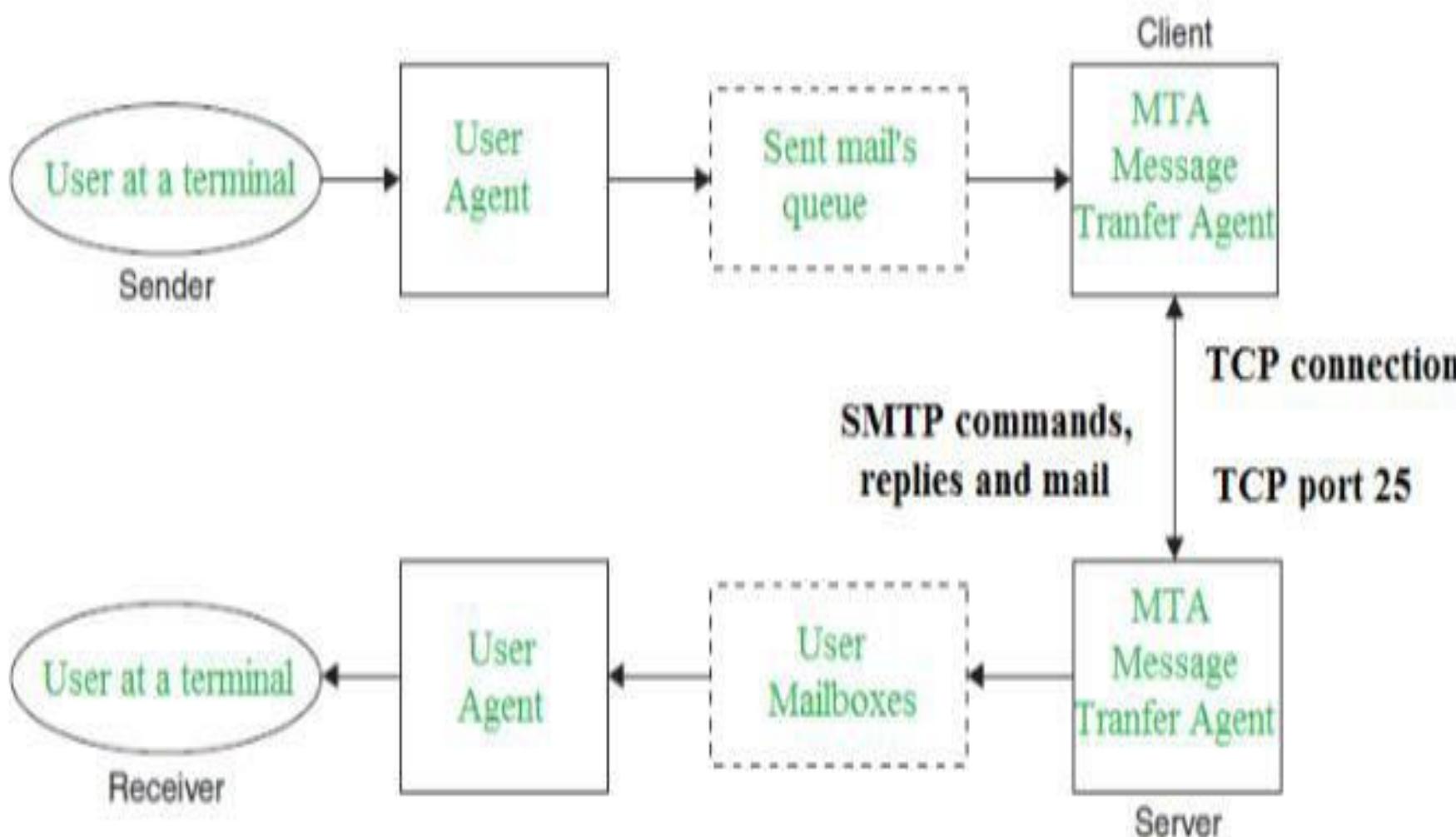
➤ SMTP (Simple Mail Transfer Protocol):

- Most internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those emails at the receiver's side.
- SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25.
- After successfully establishing a TCP connection the client process sends the mail instantly.

SMTP:

- The SMTP model is of two types:
 - End-to-end method
 - Store-and-forward method
- ✓ The end-to-end model is used to communicate between different organizations whereas the store and forward method is used within an organization.
- ✓ An SMTP client who wants to send the mail will contact the destination's host SMTP directly, in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.
- ✓ The client SMTP is the one that initiates the session so let us call it client-SMTP and the server SMTP is the one that responds to the session request so let us call it receiver-SMTP. The client-SMTP will start the session and the receiver-SMTP will respond to the request.

SMTP:

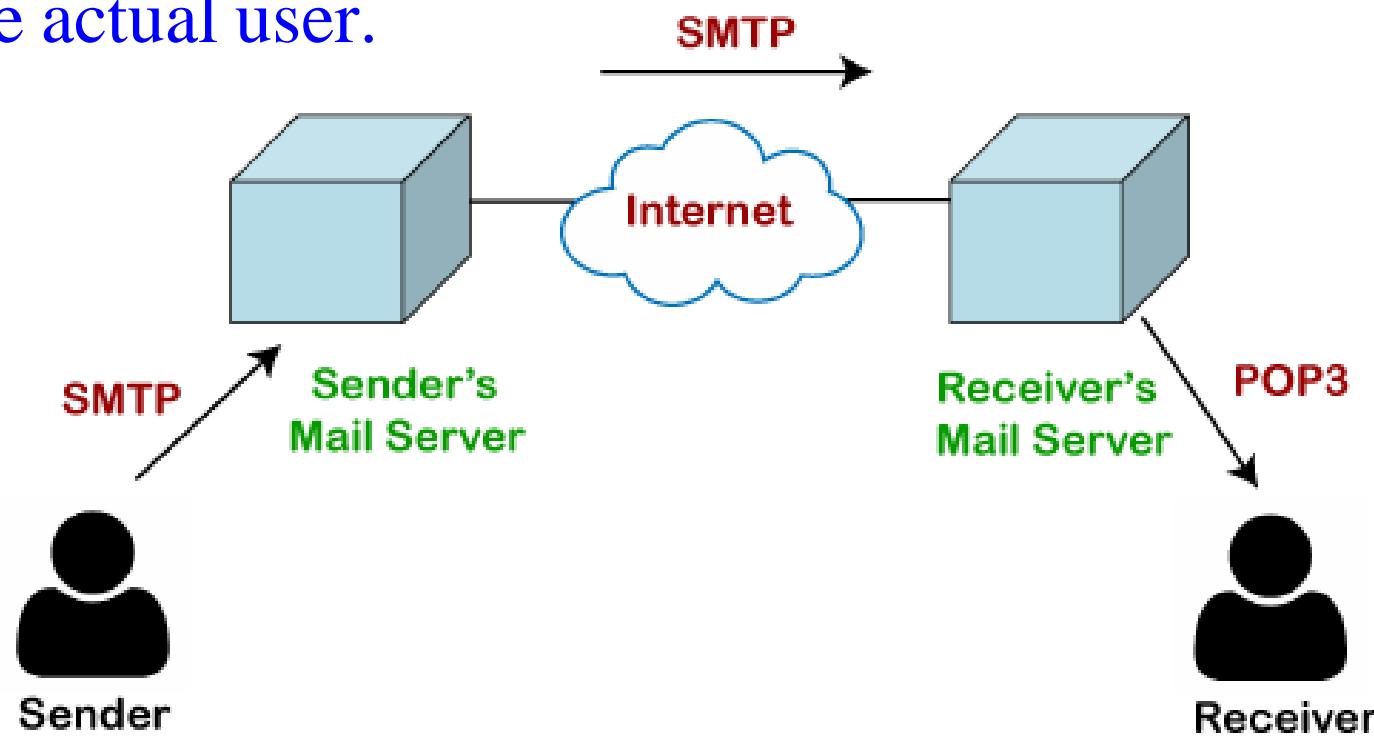


POP3:

- The POP protocol stands for Post Office Protocol. The POP3 is a simple protocol and having very limited functionalities. In the case of the POP3 protocol, the POP3 client is installed on the recipient system while the POP3 server is installed on the recipient's mail server.
- SMTP is used as a message transfer agent. When the message is sent, then SMPT is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.
- Suppose sender wants to send the mail to receiver. First mail is transmitted to the sender's mail server. Then, the mail is transmitted from the sender's mail server to the receiver's mail server over the internet.

POP3:

- On receiving the mail at the receiver's mail server, the mail is then sent to the user. The whole process is done with the help of Email protocols.
- The transmission of mail from the sender to the sender's mail server and then to the receiver's mail server is done with the help of the SMTP protocol. At the receiver's mail server, the POP or IMAP protocol takes the data and transmits to the actual user.



POP3:

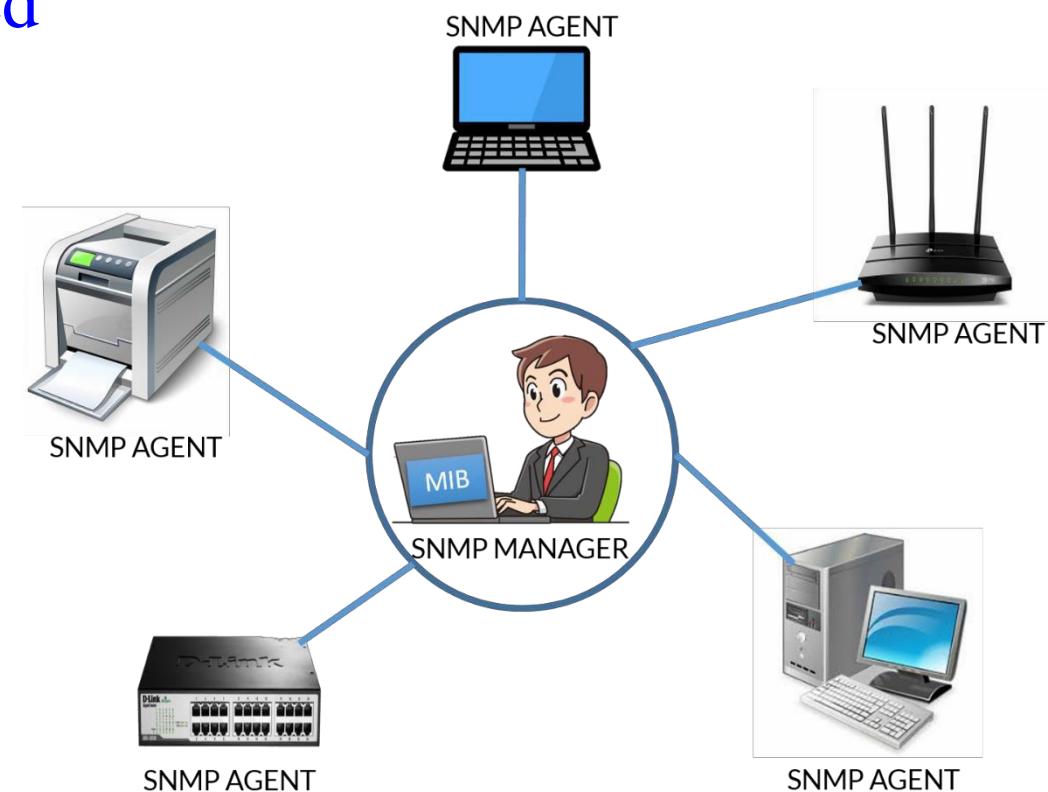
- Since SMTP is a push protocol so it pushes the message from the client to the server. As we can observe in the above figure that SMTP pushes the message from the client to the recipient's mail server. The third stage of email communication requires a pull protocol, and POP is a pull protocol. When the mail is transmitted from the recipient mail server to the client which means that the client is pulling the mail from the server.

SNMP: (Simple Network Management Protocol)

- If an organization has 1000 devices then to check all devices, one by one every day, are working properly or not is a difficult task. To ease these up, Simple Network Management Protocol (SNMP) is used.
- SNMP is an application layer protocol that uses UDP port number 161/162. SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.
- There are 3 components of SNMP:
 - **SNMP Manager –**
It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

SNMP:

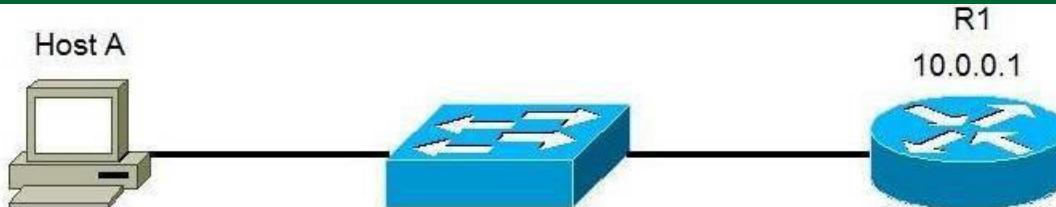
- **SNMP agent** – It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.
- **Management Information Base** – MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.



TELNET:

- ❑ **Telnet** is an application protocol that allows a user to communicate with a remote device. A user on a client machine can use a software (known as a Telnet client) to access a command-line interface of another, remote machine that is running a Telnet server program.
- ❑ Telnet is often used by network administrators to access and manage remote devices. A network administrator can access the device by telnetting to the IP address or hostname of a remote device. The network administrator will then be presented with a virtual terminal that can interact with the remote host.
- ❑ Telnet uses a well-known TCP port 23 for its communication.
- ❑ To use telnet, you must have a software (Telnet client) installed. On a remote device, a Telnet server must be installed and running. Consider the following example:

TELNET:



- The network administrator wants to use his computer (**Host A**) to access and manage the router (**R1**). The administrator will start a Telnet client program on Host A and enter the IP address of the router R1 (**telnet 10.0.0.1**)

```
telnet 10.0.0.1
Trying 10.0.0.1 ...Open

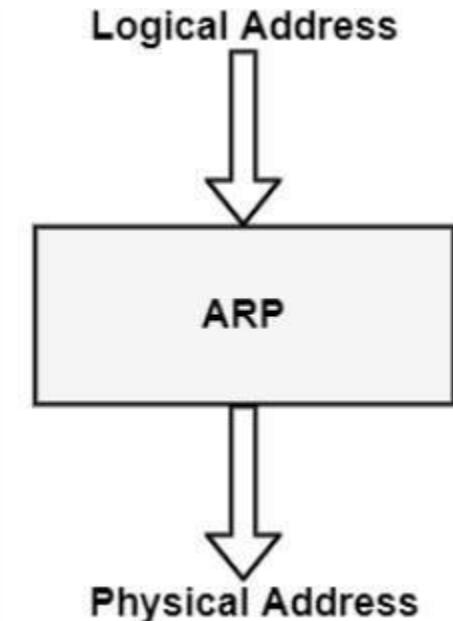
User Access Verification

Password:
```

- The administrator can now manage the remote device (**R1**) from his own computer.
- Although Telnet is simple and easy to use, it is not widely used anymore. This is because Telnet sends all data in clear-text, including usernames and passwords! **SSH** is commonly used today instead of Telnet. Telnet is only used if **SSH** is not available on the device

ARP (Address Resolution Protocol):

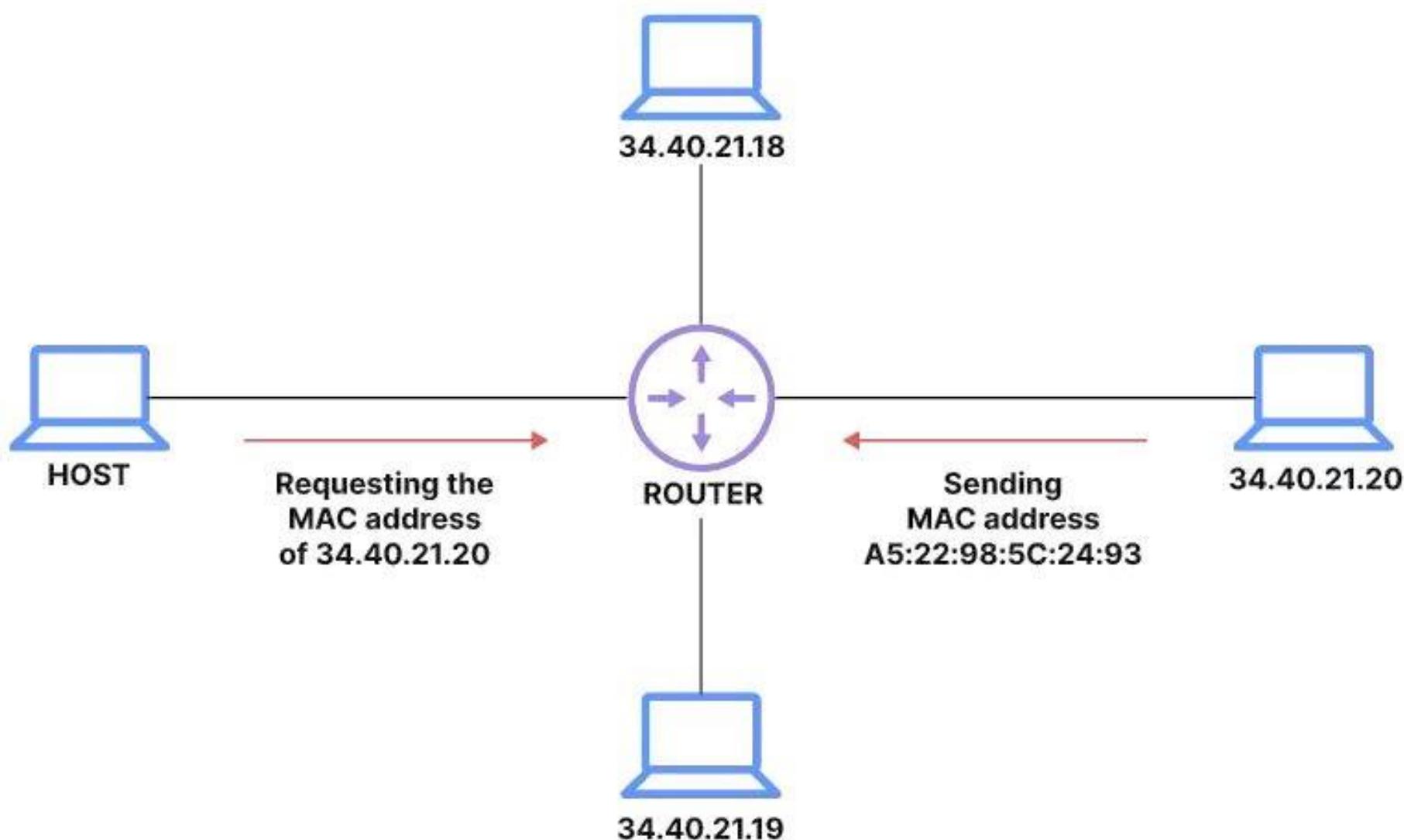
- Address Resolution Protocol (ARP) is a communication protocol used to find the MAC address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.
- The ARP is important for changing the IP (Logical) addresses to physical (MAC) network addresses.
- When one host wants to communicate with another host on the network, it needs to resolve the IP address of each host to the host's hardware address.



ARP:

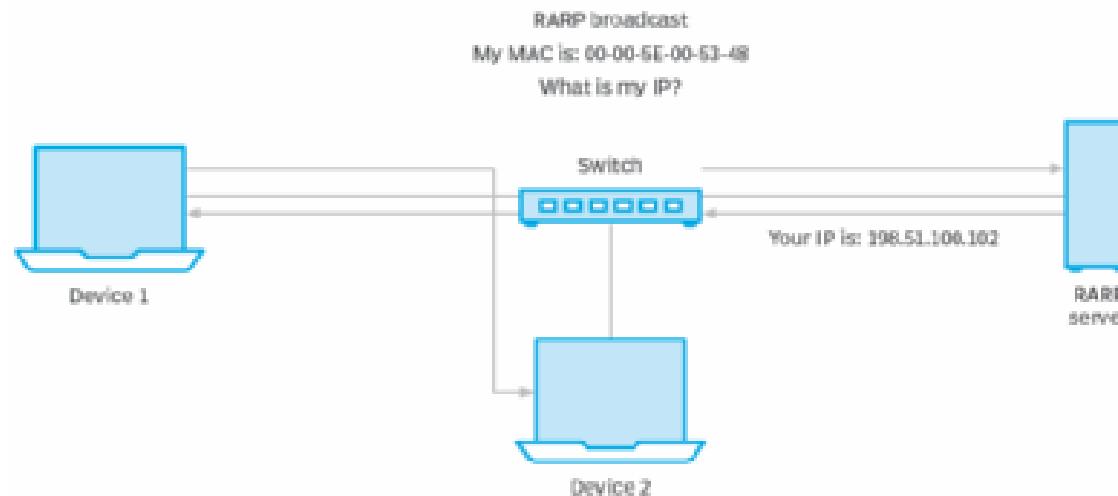
- ARP relates an IP address with the physical address. On a typical physical network such as LAN, each device on a link is identified by a physical address, usually printed on the NIC. A physical address can be changed easily when NIC on a particular machine fails / changed.
- The IP Address cannot be changed. ARP can find the physical address of the node when its internet address is known.

ARP:



RARP:

- Reverse Address Resolution Protocol (RARP) is a protocol or a physical machine in a local area network (LAN) can use to request its IP address. It does this by sending the device's physical address to a specialized RARP server that is on the same LAN and is actively listening for RARP requests.



RARP LOOKUP TABLE	
MAC	IP address
00-00-5E-00-03-48-F3	198.51.100.101
00-00-5E-00-03-09-09	198.51.100.102
00-00-5E-00-03-0C-7C	198.51.100.103

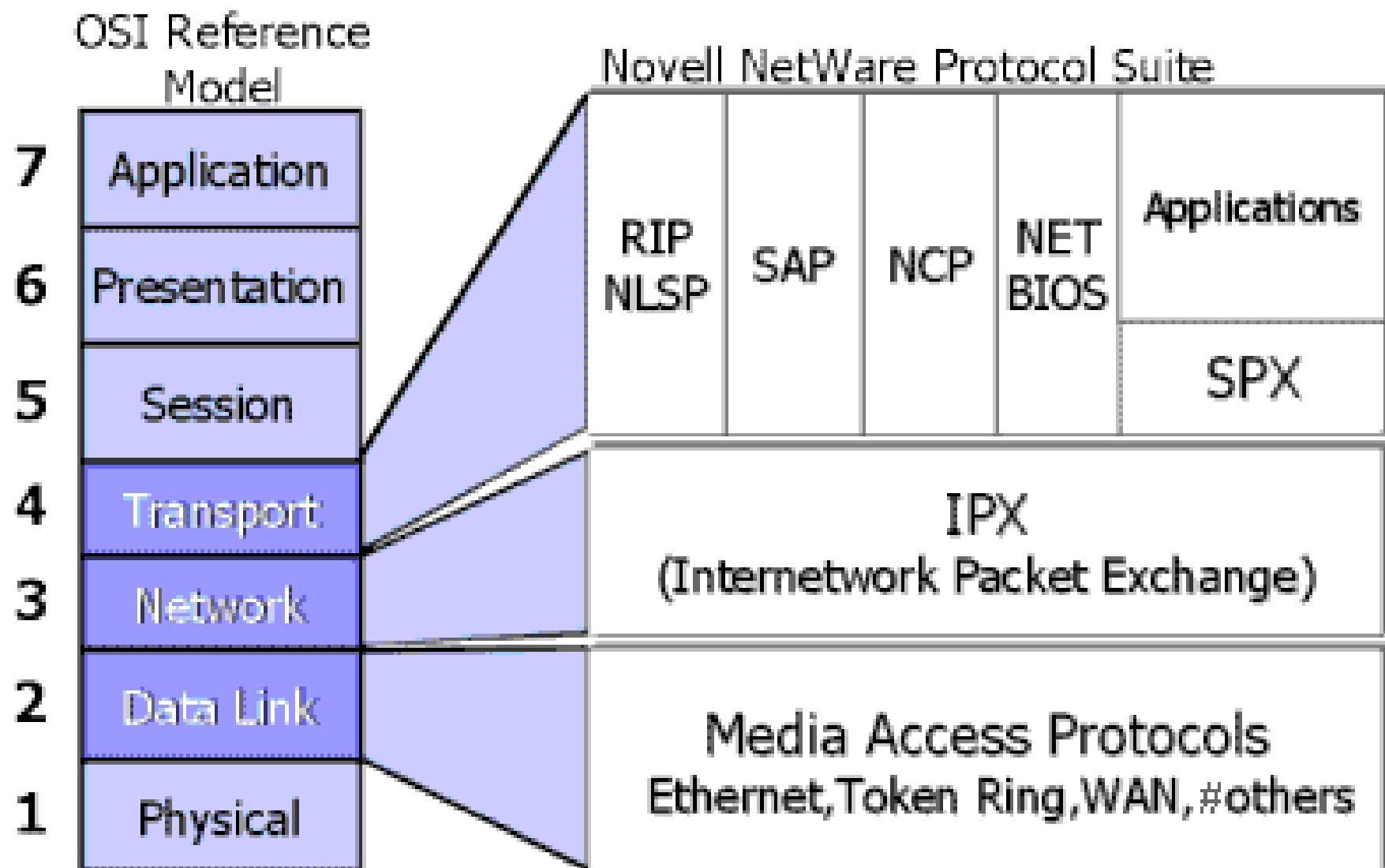
IPX/SPX: (Internetwork Packet Exchange)

- **IPX/SPX** stands for **Internetwork Packet Exchange/ Sequenced Packet Exchange** is a set of network protocols that provide packet switching and sequencing for small and large networks, Originally used by the Novell NetWare operating system and it was later adopted by Windows. As they replaced NetWare LANs they became widely used on networks deploying Microsoft Windows LANs.
- IPX/SPX was developed to be a replacement to the TCP/IP Protocol Suite. This was introduced in the early 1980s and remained fairly popular till the 1990s. After which the TCP/IP protocol has largely replaced it.

IPX/SPX:

- IPX is the network layer and SPX is the transport layer of the IPX/SPX network protocol.
- IPX and IP protocol have similar functions and this defines how data is sent and received between devices.
- The transport layer protocol or SPX protocol is much like TCP used to establish and maintain a connection between devices. Together, they can be used to transfer data and create a network connection between systems.
- IPX does not require a consistent connection to be maintained while packets are being sent from one system to another, this is what is called being connectionless. It can resume the transfer from the point where it was interrupted due to bad connection or power loss.

IPX/SPX:



APPLE TALK:

- AppleTalk is a set of registered / copyrighted networking protocols developed by Apple for their computer systems.
- AppleTalk was included in the original Macintosh released in 1984. In 2009, it became unsupported with the release of Mac OS X v10.6 and was dropped in favor of TCP/IP networking, allowing Apple computers to use the same standard to communicate with other computers.
- The design of AppleTalk followed the OSI Model of protocol layering with two protocols aimed at making the system completely self-configuring:
 - AppleTalk Address Resolution Protocol (AARP): Allowed hosts to automatically generate their own network addresses
 - Name Binding Protocol (NBP): A dynamic system that maps network addresses to user-readable names.

APPLE TALK:

7. Application	Apple Filing Protocol (AFP)
6. Presentation	
5. Session	Zone Information Protocol (ZIP) AppleTalk Session Protocol (ASP) AppleTalk Data Stream Protocol (ADSP)
4. Transport	AppleTalk Transaction Protocol (ATP) AppleTalk Echo Protocol (AEP) Name Binding Protocol (NBP) Routing Table Maintenance Protocol (RTMP)
3. Network	Datagram Delivery Protocol (DDP)
2. Data Link	EtherTalk Link Access Protocol (ELAP) LocalTalk Link Access Protocol (LLAP) TokenTalk Link Access Protocol (TLAP) Fiber Distributed Data Interface (FDDI)
1. Physical	LocalTalk driver EtherTalk driver TokenTalk driver FDDI driver

AppleTalk OSI Model

NETBIOS (Network Basic Input/Output System) Names:

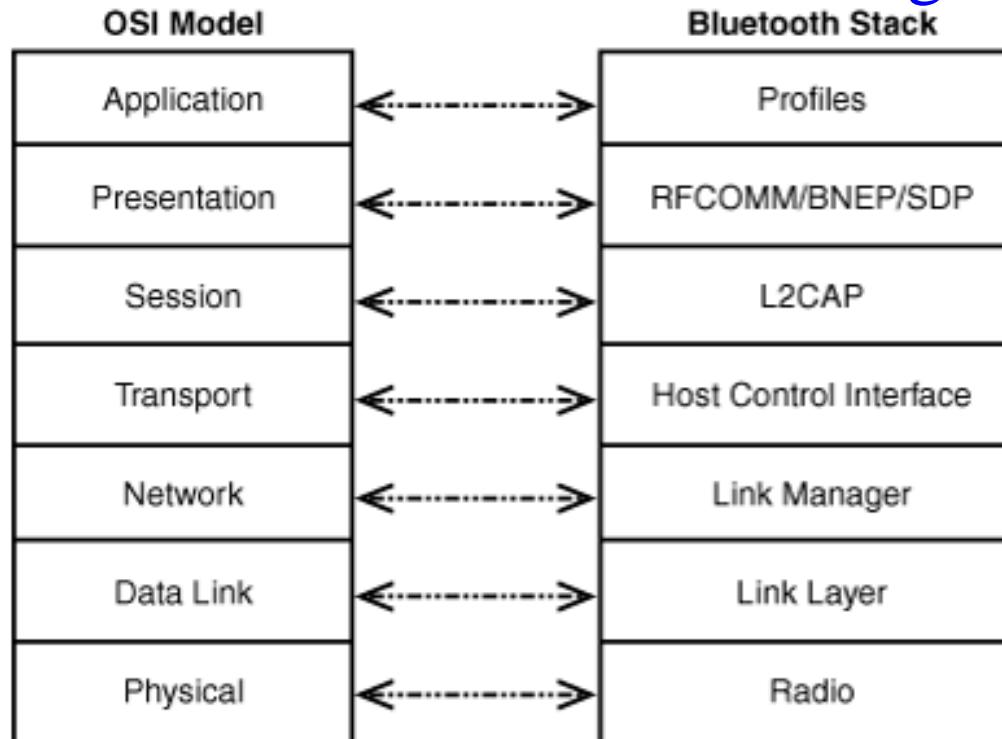
- ❑ Implement a NetBIOS naming scheme for all computers on a given Network.
- ❑ NetBIOS is an interface that provides NetBIOS-based applications with access to network resources. Every computer on a WindowsNT network must have a unique name for it to be accessible through the NetBIOS interface. This unique name is called a computer name or a NetBIOS name.
- ❑ NetBIOS is a network service that enables applications on different computers to communicate with each other across a local area network (LAN).

NETBIOS Names:

- ❑ It was developed in the 1980s for use on early, IBM-developed PC networks. A few years later, Microsoft adopted NetBIOS and it became a actual industry standard.
- ❑ NetBIOS has been used in Ethernet and Token Ring networks and, is included as part of the NetBIOS Extended User Interface (NetBEUI). Because NetBIOS is not a network protocol, it originally used NetBEUI to facilitate network communications on NetBIOS's behalf.
- ❑ While NetBEUI could operate on a flat network, it could not route data between networks. Thus, NetBEUI was quickly replaced with a TCP/IP transport alternative and has long become destroyed.

L2CAP (Logical Link Control and Adaptation):

- Logical Link Control and Adaptation Protocol (L2CAP) is a protocol used in the Bluetooth standard that provides adaption between higher layers and the baseband layer of the Bluetooth stack. It operates just above the host-controller interface (HCI) passing data frames from the higher layers to either HCI or Link Manager.



RFCOM (Radio-Frequency Communication):

- RFCOM protocol is also a Bluetooth device protocol that located at the top of L2CAP protocol. It generally used to allow multiple devices can able to join a single device.
- For ex: We are using a Bluetooth headphone. Headphone is connected with cell phone as well as laptop simultaneously. Both the device can not only connect but also communicates with the same headphone device at a time.
- The RFCOMM protocol supports up to 60 simultaneous connections between two Bluetooth devices. The number of connections that can be used simultaneously in a Bluetooth device is implementation-specific.

Assignments:

- 1) What is Packet in Computer Network?
- 2) What are the protocols? Explain types of protocol.
- 3) What is TCP/IP Stack? Explain various protocols available in TCP/IP Stack.
- 4) Difference between HTTP and FTP
- 5) Difference between SMTP and POP3
- 6) Difference between ARP and RARP.
- 7) What is IPX/SPX?
- 8) What is Apple Talk?
- 9) Difference between TCP/IP and Apple Talk.
- 10) What is NETBIOS Names?
- 11) What are the L2CAP and RFCOM?

Ch-7

Network Routing

Ch - 7 _ Network Routing, Content...

❖ What is Routing?

□ Types of Routing

- Static Routing
- Dynamic Routing
- Default Routing

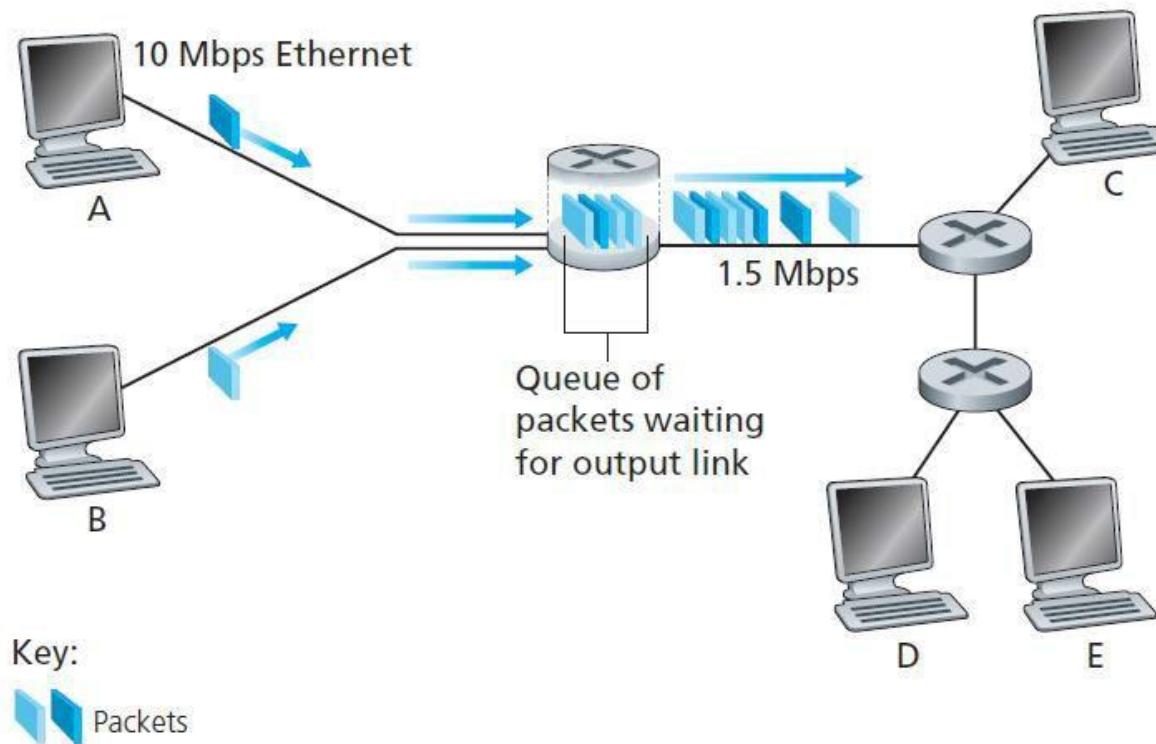
❖ Routing Protocols

- Exterior Routing Protocols (BGP)
- Interior Routing Protocols
 - Distance Vector Routing
 1. RIP
 2. IGRP
 3. EIGRP
 - Link State Routing
 1. OSPF
 2. ISIS

❖ What is Routing?

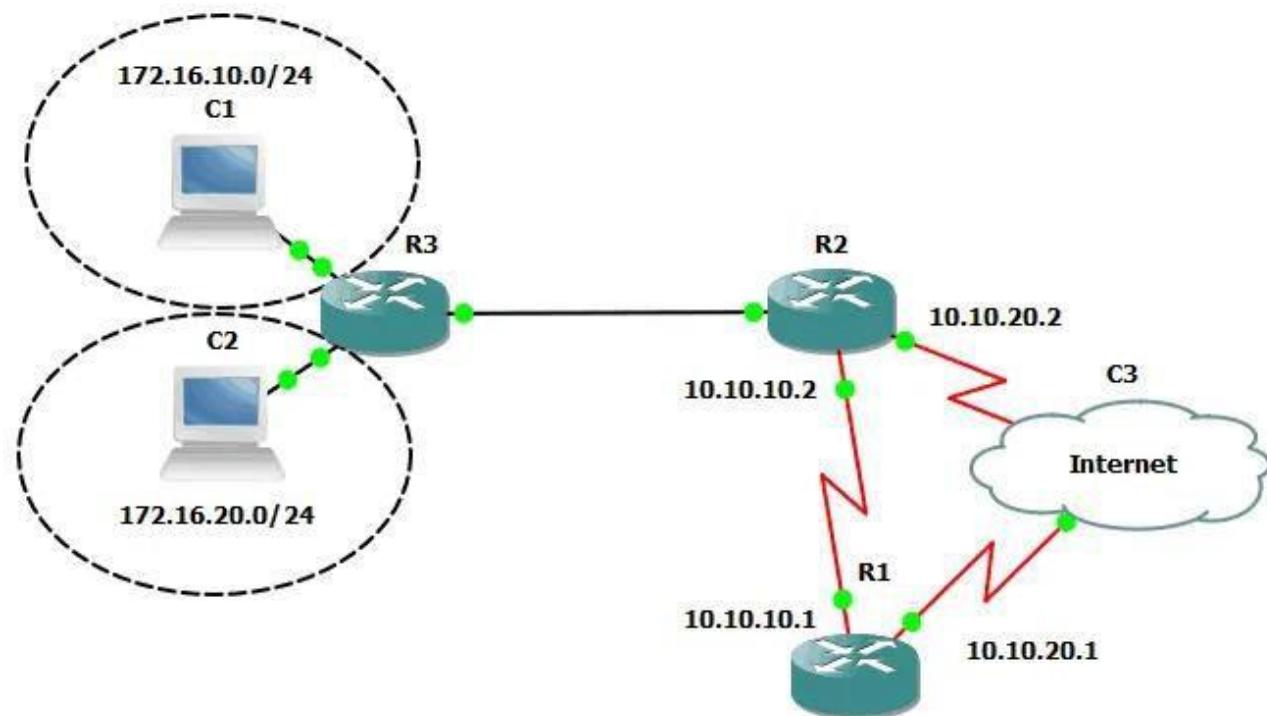
- When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes. The software-based routers have limited functionality and limited scope.
- A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple path existing to reach the same destination, router can make decision based on the following information:
- **Hop Count:** If the routing protocol considers the hop as a primary metric(unit of measurement) value, then the path with the least hop count will be considered as the best path to move from source to the destination.

- **Bandwidth:** The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.
- **Delay:** It is a time taken by the router to process, queue and transmit a datagram. The protocols use this metric to determine the delay values for all the links. The path having the lowest delay value will be considered as the best path.



❖ Types of Routing: 1. Static Routing

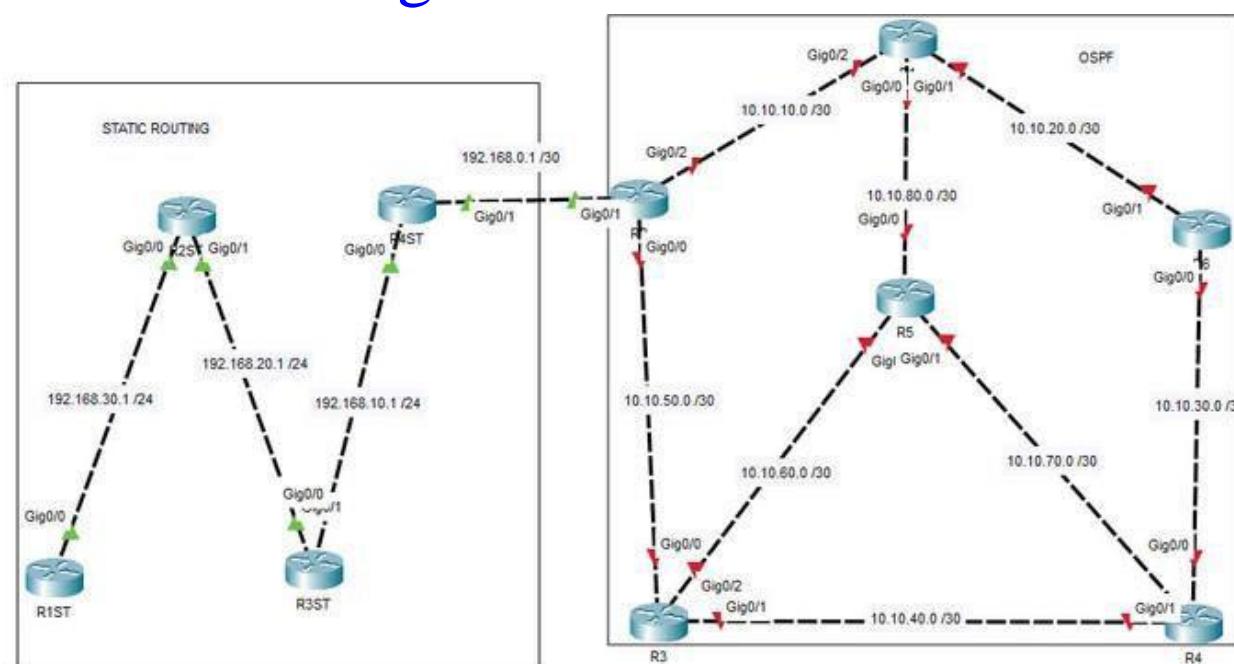
- ❑ **Static Routing:** Static Routing is also known as non-adaptive routing which doesn't change routing table unless the network administrator changes or modify them manually. Static routing does not use complex routing algorithms and It provides high or more security than dynamic routing.
- ❑ Static routing generally used in small networks. Here The routes are user defined or manual hence, failure of link disrupts the rerouting.
- ❑ It may not follow Any protocols for Routing packets in the network.



2. Dynamic Routing:

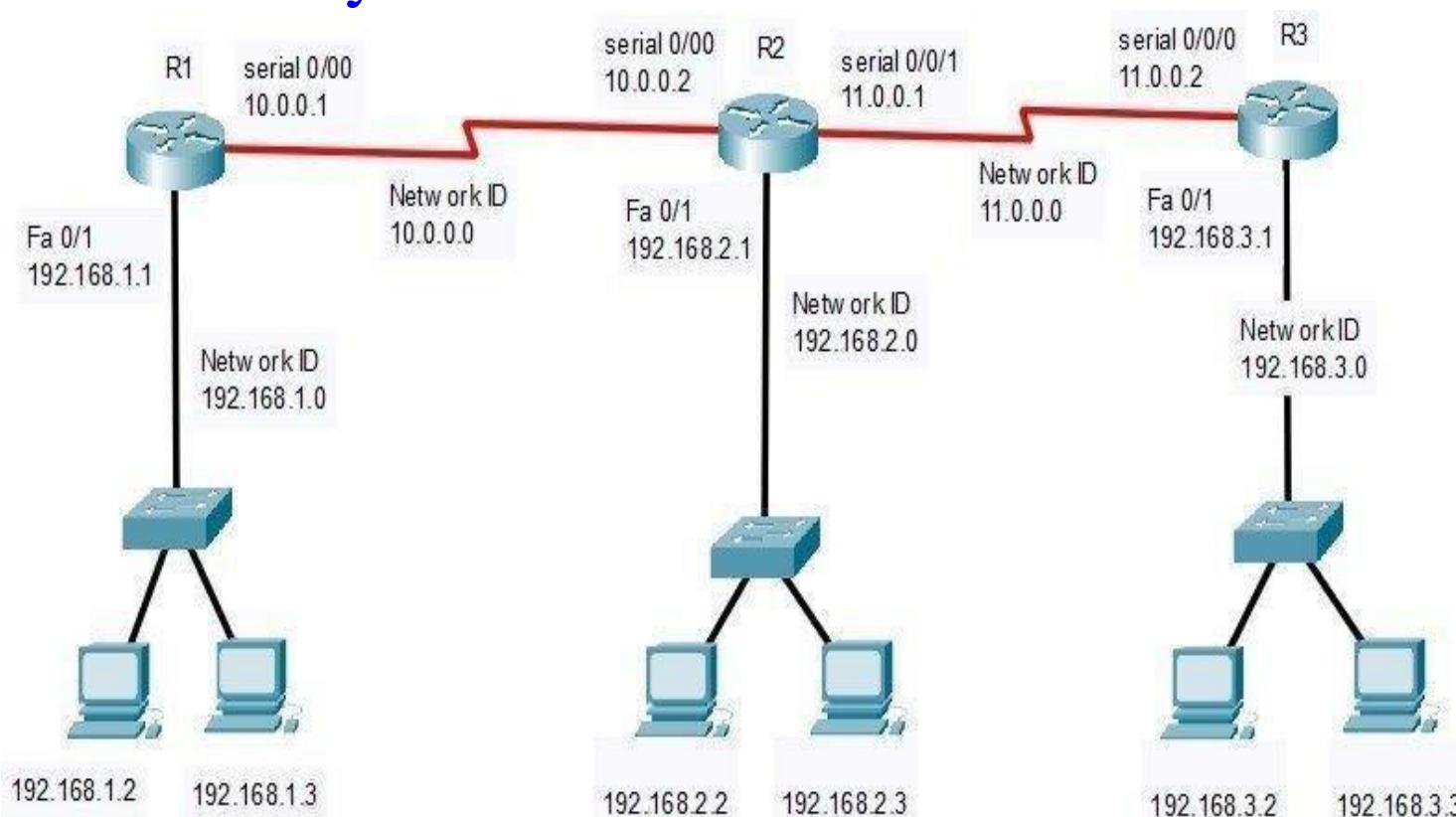
- **Dynamic Routing:** Dynamic Routing is also known as adaptive routing which changes routing table according the changes occurs in network/topology. Dynamic routing uses complex routing algorithms and it provides less security than static routing.
- Dynamic routing is used in large networks. Here The routes are taken automated by with the help of algorithm hence, failure of link does not disrupts the rerouting.

- It follows protocols Like BGP, RIP and EIGRP packets in the network.



3. Default Routing:

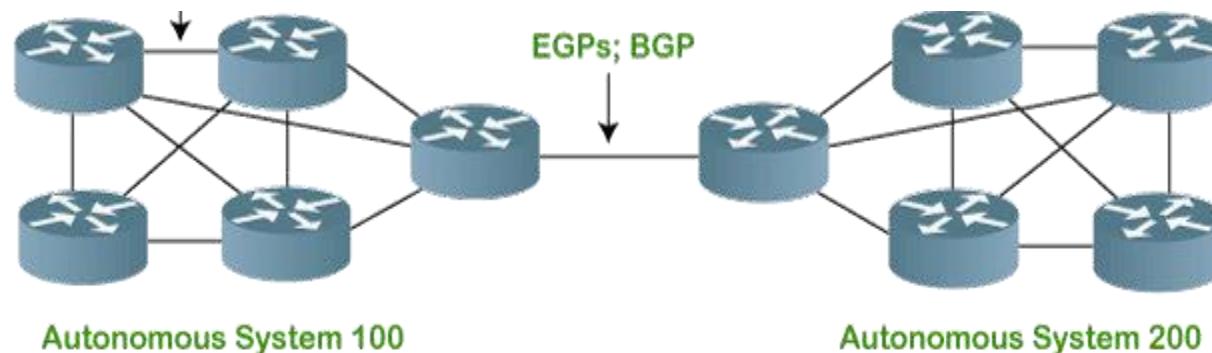
- This is the method where the router is configured to send all packets towards a single router.
- It doesn't matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing. It is generally used with stub routers. A stub router is a router that has only one route to reach all other networks.



❖ Routing Protocols:

□ **Exterior Routing Protocols (BGP):**

- BGP stands for **Border Gateway Protocol**. It is a standardized gateway protocol that exchanges routing information within independent (self-directed) network systems. When one network router is linked to other networks, it cannot decide which network is the best network to share its data to by itself.
- Border Gateway Protocol considers all peering partners that a router has and sends traffic to the router closest to the data's destination. This communication is possible because, BGP allows peers to communicate their routing information.



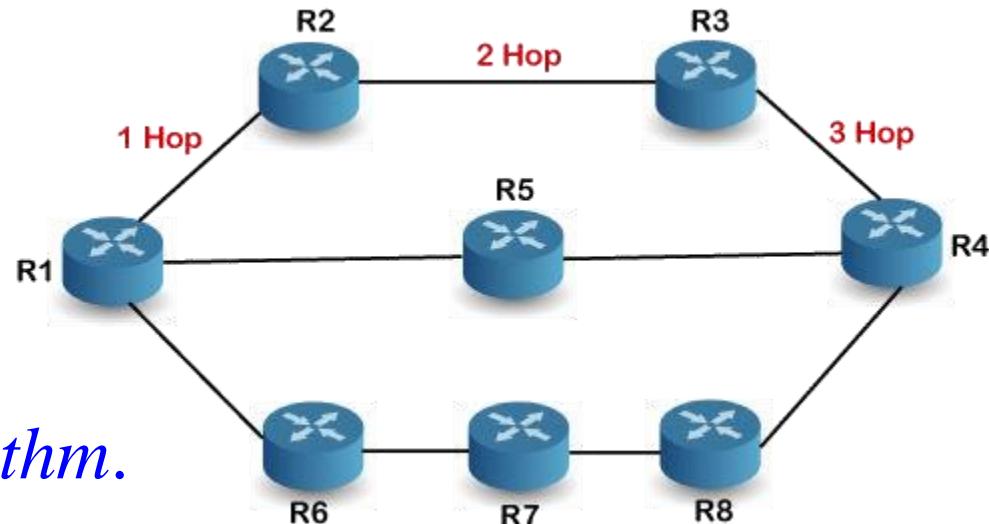
□ Interior Routing Protocols:

- An interior protocol is a routing protocol used inside - interior to - an independent network system. In TCP/IP terminology, these independent network systems are called autonomous systems. Within an autonomous system (AS), routing information is exchanged using an interior protocol chosen by the autonomous system's administration.
- All interior routing protocols perform the same basic functions. They determine the "best" route to each destination, and they distribute routing information among the systems on a network.
- How they perform these functions, in particular, how they decide which routes are best, is what makes routing protocols different from each other. There are several interior protocols:

➤ **Distance Vector Routing:** In distance-vector routing (DVR), each router is required to inform the topology changes to its neighboring routers periodically. Historically it is known as the old ARPNET routing algorithm or Bellman-Ford algorithm.

■ **RIP:** The *Routing Information Protocol* (RIP) is the interior protocol most commonly used on UNIX systems. It is adequate for local area networks and is simple to configure. RIP selects the route with the lowest "hop count" (*metric*) as the best route. The RIP hop count represents the number of gateways through which data must pass to reach its destination.

■ RIP assumes that the best route is the one that uses the fewest gateways. This approach to route choice is called a *distance-vector algorithm*.



Interior Protocols:

2. IGRP: Interior Gateway Routing Protocol is also a distance vector routing protocol. In this, Bellman ford algorithm is used. The least hop count in IGRP is 255.

3. EIGRP: Enhanced Interior Gateway Routing Protocol is routing protocol like IGRP. It is the link state routing protocol as well as vector routing protocol.

✓ IGRP is Classful routing technique. Where as EIGRP is class less technique.

➤ Link State Routing:

1. OSPF: Open Shortest Path First (OSPF) is another link-state protocol developed for TCP/IP. It is suitable for very large networks and provides several advantages over RIP.

2. IS-IS: Intermediate System to Intermediate System (IS-IS) is an interior routing protocol from the OSI protocol suite. It is a Shortest Path First (SPF) link-state protocol. It was the interior routing protocol that is still used by some large service providers.

Assignments:

- 1) What is routing in Computer Network?
- 2) Explain all routing technique in brief.
- 3) Differentiate Interior Routing Protocol & Exterior Routing Protocol.
- 4) Explain following:
 - Interior Routing Protocols
 - Distance Vector Routing
 1. RIP
 2. IGRP
 3. EIGRP
 - Link State Routing

- 1. OSPF
- 2. IS-IS

Ch-8

IP Addressing

Ch – 8 _ IP Addressing, Content...

❖ What is IP Address?

❖ Types of IP Address

- Private IP

- Public IP

- Static IP

- Dynamic IP

❖ IPV4

- Class Structure

- Subnetting

- Supernetting

❖ IPV6

- Basic Structure of IPV6

- Implementation of IPV6

❖ Migration from IPV4 to IPV6

❖ What is IP Address:

- ❑ An IP address stands for Internet Protocol address is a unique address that is used to identify computers or nodes on the internet. This address is just a string of numbers written in a certain format.
- ❑ Your IP address never be consistent, it can be changed. For example, turning your router on or off can change your IP Address.
- ❑ When you are out from your home location, your home IP address doesn't go with you. It changes as you change the network of your device. Whenever you change your location with your device every time your IP address changed.

- Whenever you change your location you will be accessing the different networks to connect your device with the internet. Therefore, your device will be allocated a different (temporary) IP address by the ISP (router) of that particular access point.
- It's a responsibility of a router to allot you an IP address to whom you are connected.
- IP address can be of:
 - Private IP
 - Public IP
 - Static IP
 - Dynamic IP

❖ Types of IP Address:

- **Private IP:** Every device that connects to your internet network has a private IP address. This includes computers, smartphones, and tablets but also any Bluetooth-enabled devices like speakers, printers, or smart TVs.
- With the growing internet of things, the number of private IP addresses you have at home is probably growing. Your router needs a way to identify these items separately, and many items need a way to recognize each other.
- Therefore, your router generates private IP addresses that are unique identifiers for each device that differentiate them on the network. Ex: 192.168.20.100
- **Public IP:** It is the primary address associated with your whole network. While each connected device has its own IP address, they are also included within the main IP address

- ❑ **Static IP:** Static addresses remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web.
- ❑ **Dynamic IP:** Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers.
 - ❑ Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers. The reason for this approach is to generate cost savings for the ISP.
 - ❑ Automating the regular movement of IP addresses means they don't have to carry out specific actions to re-establish a customer's

❖ IPV4

- **IPV4:** Internet Protocol version 4. It consists of 4 numbers or octets separated by the dots. Each number/octet can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111).
- Since each number N can be represented by a group of 8 binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^{32}) devices approximately = 4,294,967,296 (around 4.3 billion) can be assigned with IPv4.
- IPv4 can be written as: **189.123.123.90** and it's binary equivalent is: **10111101. 1111011. 1111011. 1011010**

□ Class Structure of IPV4:

- There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible.
- For Ex: If we have to find a word from a dictionary, how long will we take? Usually, we will take less than 5 minutes to find that word. We are able to do this because words in the dictionary are organized in alphabetical order. If we have to find out the same word from a dictionary that doesn't use any sequence or order to organize the words, it will take a very much time to find the word.
- If a dictionary with one billion words without order can be so upsetting, then we can imagine the pain behind finding an address from 4.3 billion addresses.
- For easier management and assignment IP addresses are

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.

Table of classes

Class	Value of w	Net ID	Host ID	No of Networks	No of Hosts Per network
A	1-126	W	X.Y.Z	126	16,777,214
B	128-191	W.X	Y.Z	16,384	65534
C	192-223	W.X.Y	Z	2,097,152	254
D	224-239	Reserved for Multicast	N/A	N/A	N/A
E	240-254	Reserved for Experiment	N/A	N/A	N/A

Class Structure of IP:

Private IP

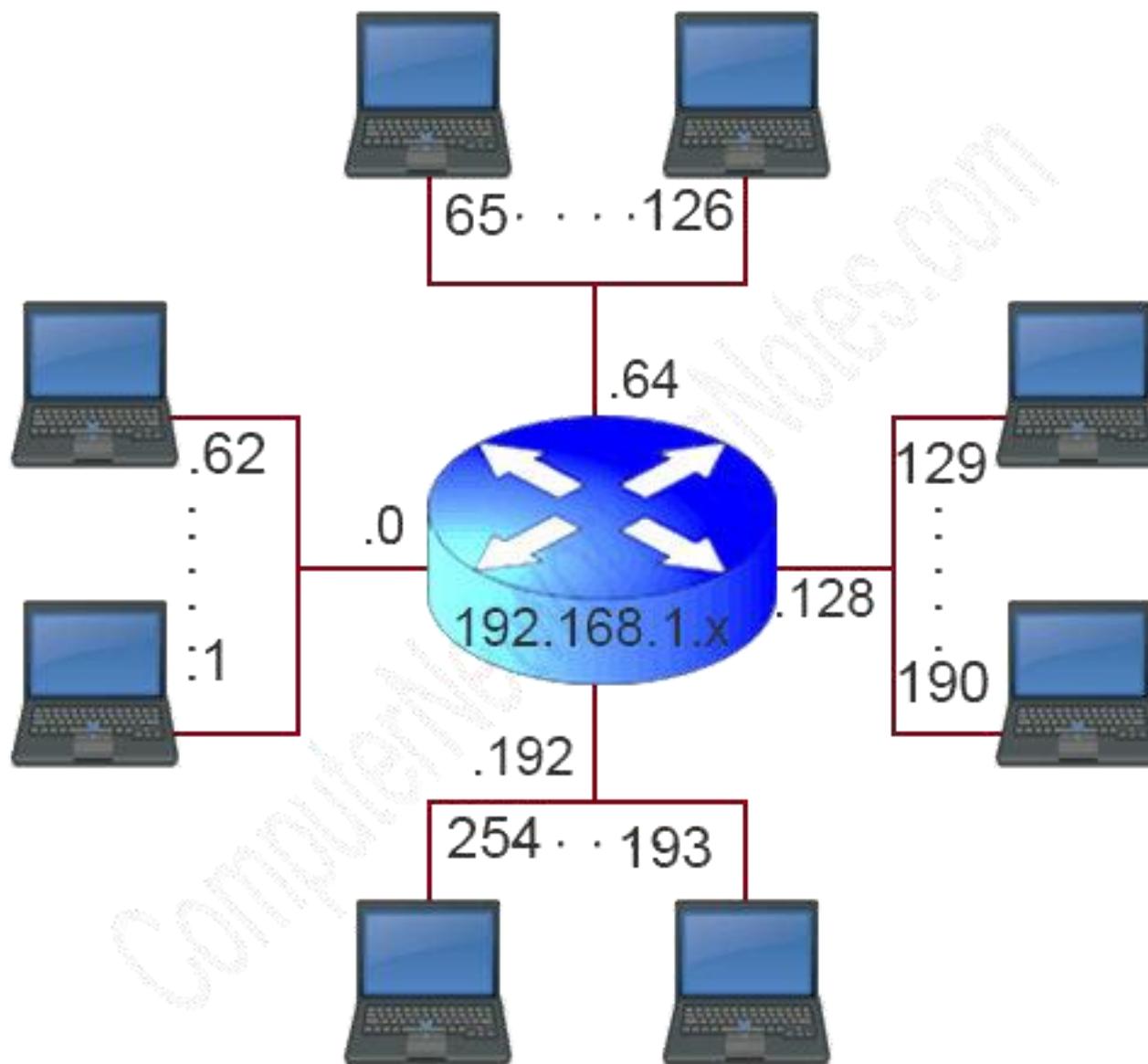
Class	Range	No. of Networks	No. of Hosts
A	10.0.0.0 to 10.255.255.255	1	1,67,77,216
B	172.16.0.0 to 172.31.255.255	15	9,83,040
C	192.168.0.0 to 192.168.255.255	1	65,536

- Remaining all IP addresses from above are public IP addresses.

Subnetting:

- ❑ A subnet, or sub-network, is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments.
- ❑ Each computer, or host, on the internet has at least one IP address as a unique identifier.
- ❑ Organizations will use a subnet to subdivide large networks into smaller, more efficient sub-networks. One goal of a subnet is to split a large network into a grouping of smaller, interconnected networks to help minimize traffic. This way, traffic doesn't have to flow through unnecessary routes, increasing network speeds.
- ❑ Subnetting, the segmentation of a network address space, improves address allocation efficiency as well as network security.

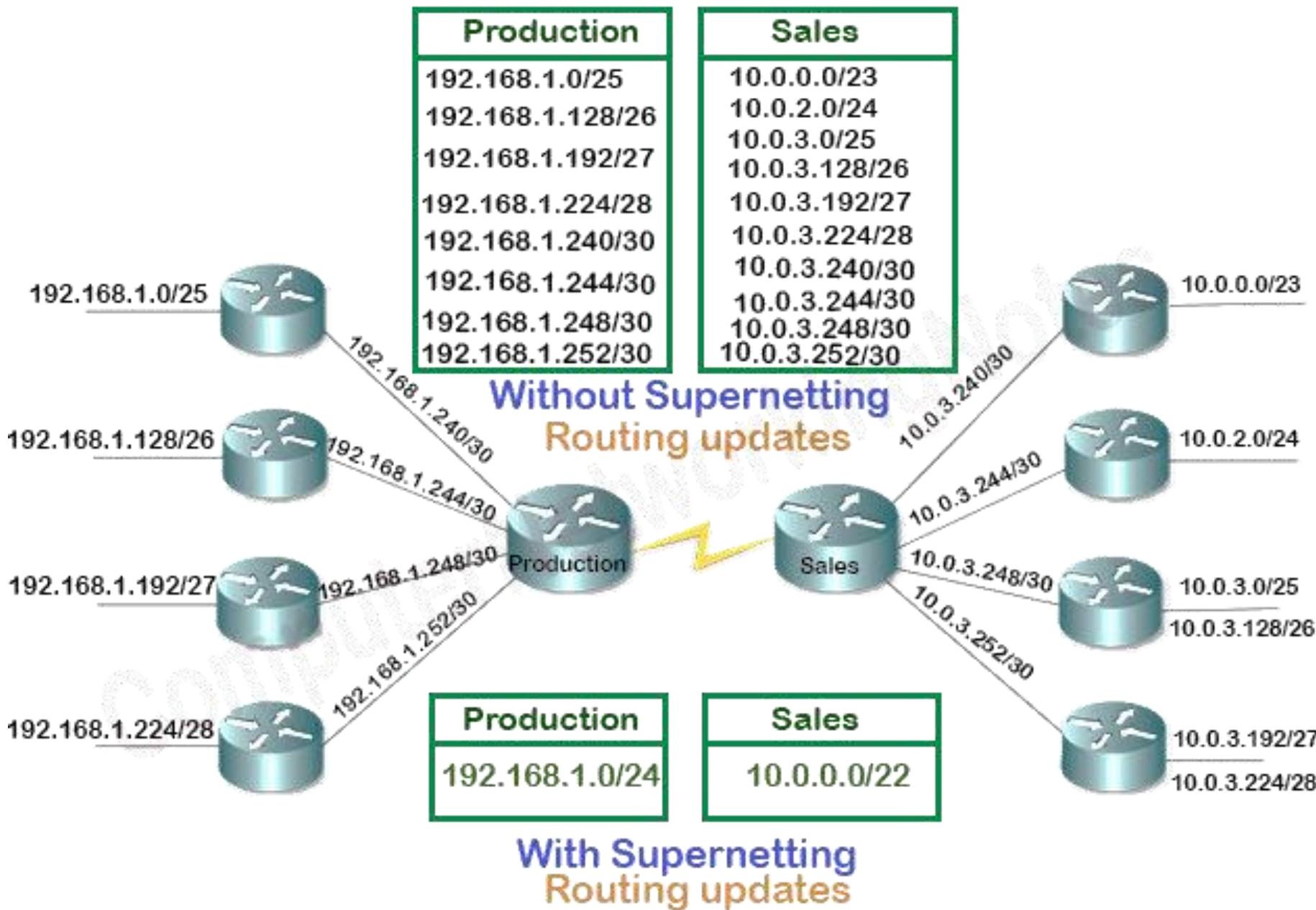
Subnetting:



Supernetting:

- ❑ Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller sub-networks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.
- ❑ Supernetting is used in route aggregation to reduce the size of routing tables and routing table updates.
- ❑ This technique Controls and reduces network traffic and It also helpful to solve the problem of lacking IP addresses.
- ❑ Ex: If we have to post any letter from Surat to Baroda, then we have to deliver it to post office and post authorities will send it firstly at main branch office of Baroda not directly at the exact address. When letter once delivered at main office in Baroda, then it's a responsibility of that main branch

Supernetting:



□ IPv6:

- **IPv6:** With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So, gradually we are making our way to **IPv6 Address** which is a 128-bit IP address.
- In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons(:). But in the computer-friendly form, it can be written as 128 bits of 0s and 1s. Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet. So, via IPv6 a total of (2^{128}) devices can be assigned with unique addresses which are actually more than enough for upcoming future generations.

❖ Migration from IPV4 to IPV6:

- It is going to take step forever for the world to migrate from IPv4 to IPv6. Fortunately, the IPv6 committees took this into account when they designed IPv6. Hence, they have had pre-planed concept that the partial or entire world will have to migrate from IPV4 to IPV6.
- Why should anyone have to migrate from IPV4 to IPV6, here are some reasons:
 - **Greatly larger IP address space:** IPv6 uses 128 bits for IPv6 addresses which allows for 340 billion billion billion billion (3.4×10^{38}) unique addresses. To get an idea of the scale involved, consider the entire IPv4 space as being contained in an iPod, then the new IPv6 space would be the size of the Earth.

Migration from IPV4 to IPV6

- **Better end-to-end connectivity:** IPv6 with its large address space no longer requires Network Address Translation (NAT) and can ensure true end-to-end connectivity. This means peer-to-peer applications like VoIP or streaming media can work very effectively and efficiently with IPv6.
- **Better ability for auto configuring devices:** IPv6 offers automatic configuration and more importantly, simple configuration mechanisms. Known as plug-and-play auto configuration, these capabilities are way beyond what IPv4 currently offers.
- Better Security, Better Quality of Service, better Multicast and Anycast abilities, Offers better mobility features etc.

Assignments:

- 1) What is IP addressing?
- 2) Explain all types of IP addresses.
- 3) Explain IPV4 with it's Class Structure.
- 4) Answer in details:
 - I. Subnetting
 - II. Supernetting
- 5) What is IPV6? Why we should have to migrate from IPV4 to IPV6?

Ch-9

Windows Server - 2008

Ch – 9 _ Windows Server-2008, Content...

- ❖ Installation of 2008 Enterprise Server
- ❖ **Installation & Configuration of Active Directory**
 - Domains
 - Trees
 - Forest Concepts.
- ❖ Accounts
 - User
 - Group
 - Computer
- ❖ Policy (Security and Audit)
- ❖ Logging Events

❖ MMC (Microsoft Management Console)

❖ Installation of 2008 Enterprise Server

- As an experienced IT professional, you are familiar with the installation process of any operating system in computer.
- Some of the important and enhanced considerations when installing Windows Server 2008 are:

★ **Bootable CD-ROM installation:** Windows Server 2008 can be installed directly from the CD-ROM. There is no support for starting installation from floppy disks.

★ Improved graphical user interface (GUI) during setup :

Windows Server 2008 uses a GUI during setup that look like that of Windows XP.

★ **Product activation :** Retail and evaluation versions of Windows Server 2008 require that you activate the product.

Volume licensing programs, such as Open License, Select

Steps required installing Windows 2008:

1. Configure the computer's BIOS, to boot from CD-ROM.
2. Insert the Windows Server 2008 installation CD-ROM into the CD-ROM drive and restart the computer.
3. Reboot the computer.
4. When prompted for an **installation language** and other regional options, make your selection and press **Next**.
5. Next, press **Install Now** to begin the installation process.
6. Product activation is now also identical with that found in Windows Vista. Enter your **Product ID** in the next window, and if you want to automatically activate Windows the moment the installation finishes, click **Next**. If you do not have the Product ID available right now, you can leave the box empty, and click **Next**. You will need to provide the

7. Because you did not provide the correct ID, the installation process cannot determine what kind of Windows Server 2008 license you own, and therefore you will be prompted to select your correct version in the next screen, assuming you are telling the truth and will provide the correct ID to prove your selection later on.
8. If you did provide the right Product ID, select the Full version of the right Windows version you're prompted, and click Next.
9. Read and accept the license terms by clicking to select the checkbox and pressing Next.
10. In the “Which type of installation do you want?” window, click the only available option – Custom (Advanced).
11. In the “Where do you want to install Windows?”, if you’re installing the server on a regular IDE hard disk, click to select

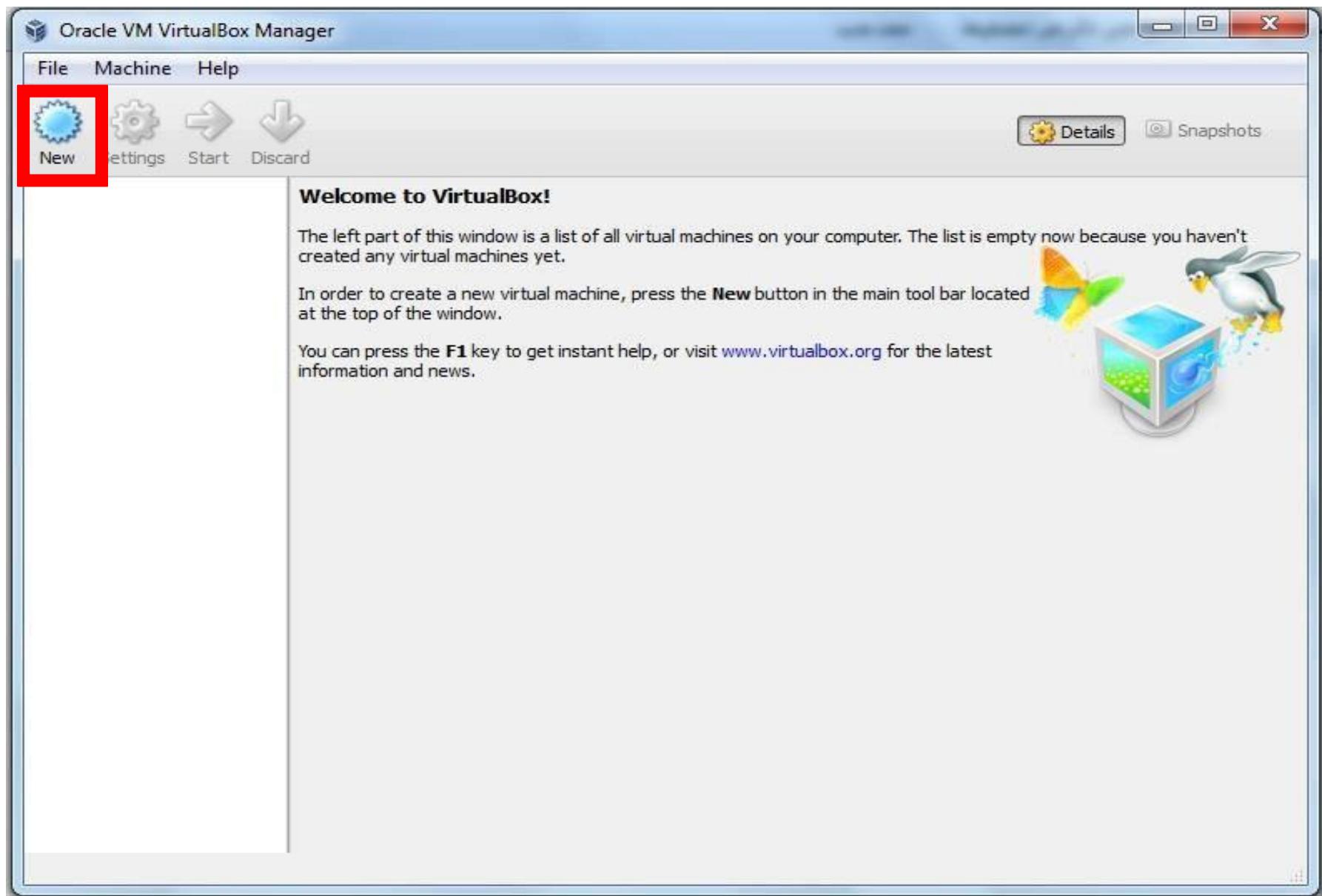
12. The installation now begins, and you can go and have lunch. Copying the setup files from the DVD to the hard drive only takes about one minute. However, extracting and uncompressing the files takes a good deal longer. After 20 minutes, the operating system is installed. The exact time it takes to install server core depends upon your hardware specifications. Faster disks will perform much faster installs... Windows Server 2008 takes up approximately 10 GB of hard drive space.
13. Then the server reboots you'll be prompted with the new Windows Server 2008 type of login screen.
Press **CTRL+ALT+DEL** to log in.
14. Click on **Other User**.
15. The default **Administrator** is **blank**, so just type **Administrator** and press **Enter**.

17. In the password changing dialog box, leave the **default password blank** (duh, read step #15...), and enter a new, complex, at-least-7-characters-long new password twice. A password like “topsecret” is not valid (it’s not complex), but one like “T0pSeReT!” sure is. Make sure you remember it.
18. Someone thought it would be cool to nag you once more, so now you’ll be prompted to accept the fact that the password had been changed. Press **Ok**.
19. Finally, the desktop appears and that’s it, you’re logged on and can begin working. You will be greeted by an assistant for the **initial server configuration**, and after performing some initial configuration tasks, you will be able to start working.

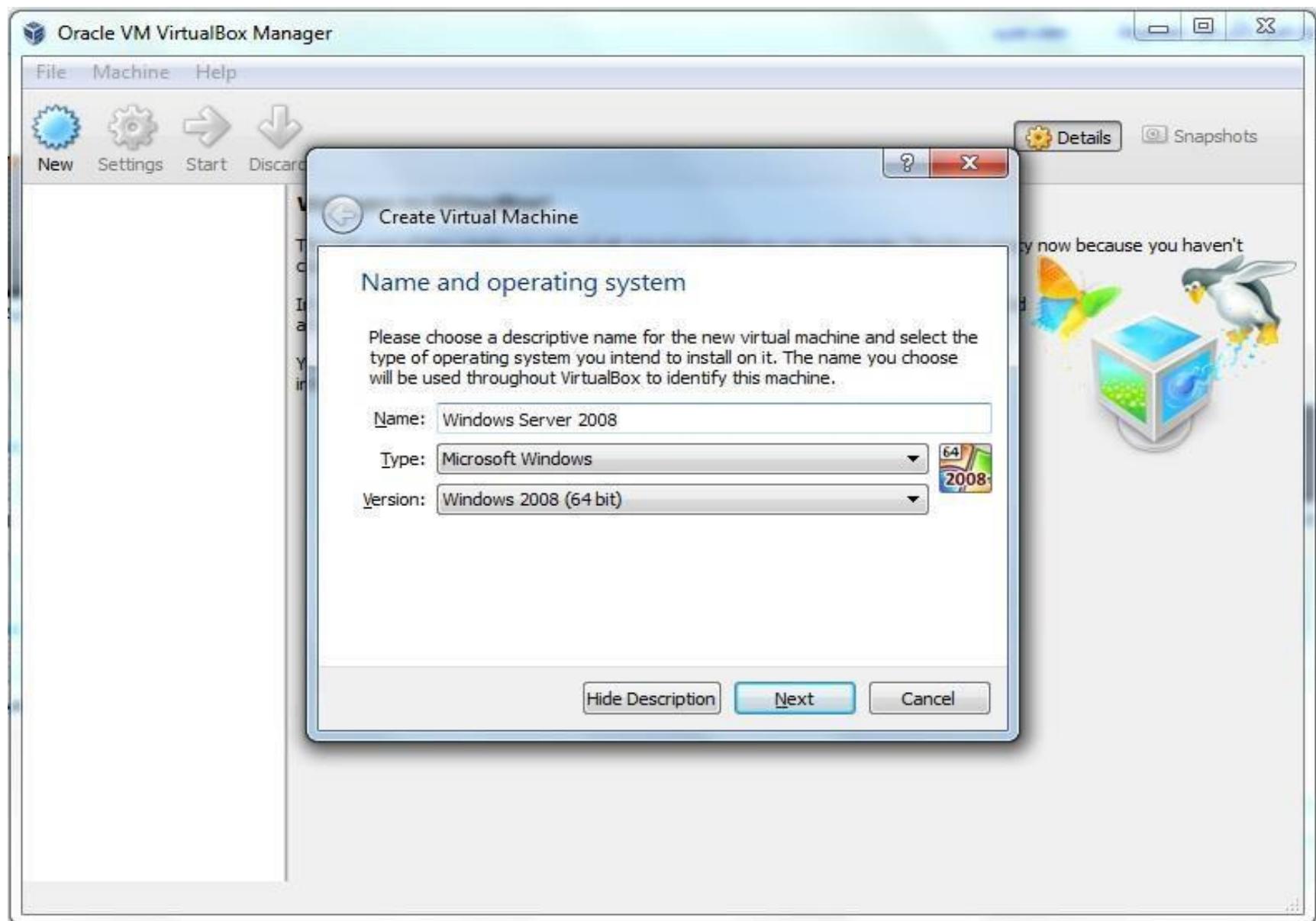
Installation Steps

- First, check if Windows Server 2008 minimum hardware requirements matches your computer hardware through link below
<http://technet.microsoft.com/en-us/windowsserver/bb414778.aspx>
- you have to install Virtual Box to enable Windows Server install on your computer.
- Install Windows Server 2008 R2 by following the steps.

Installing Windows Server 2008



Installing Windows Server 2008

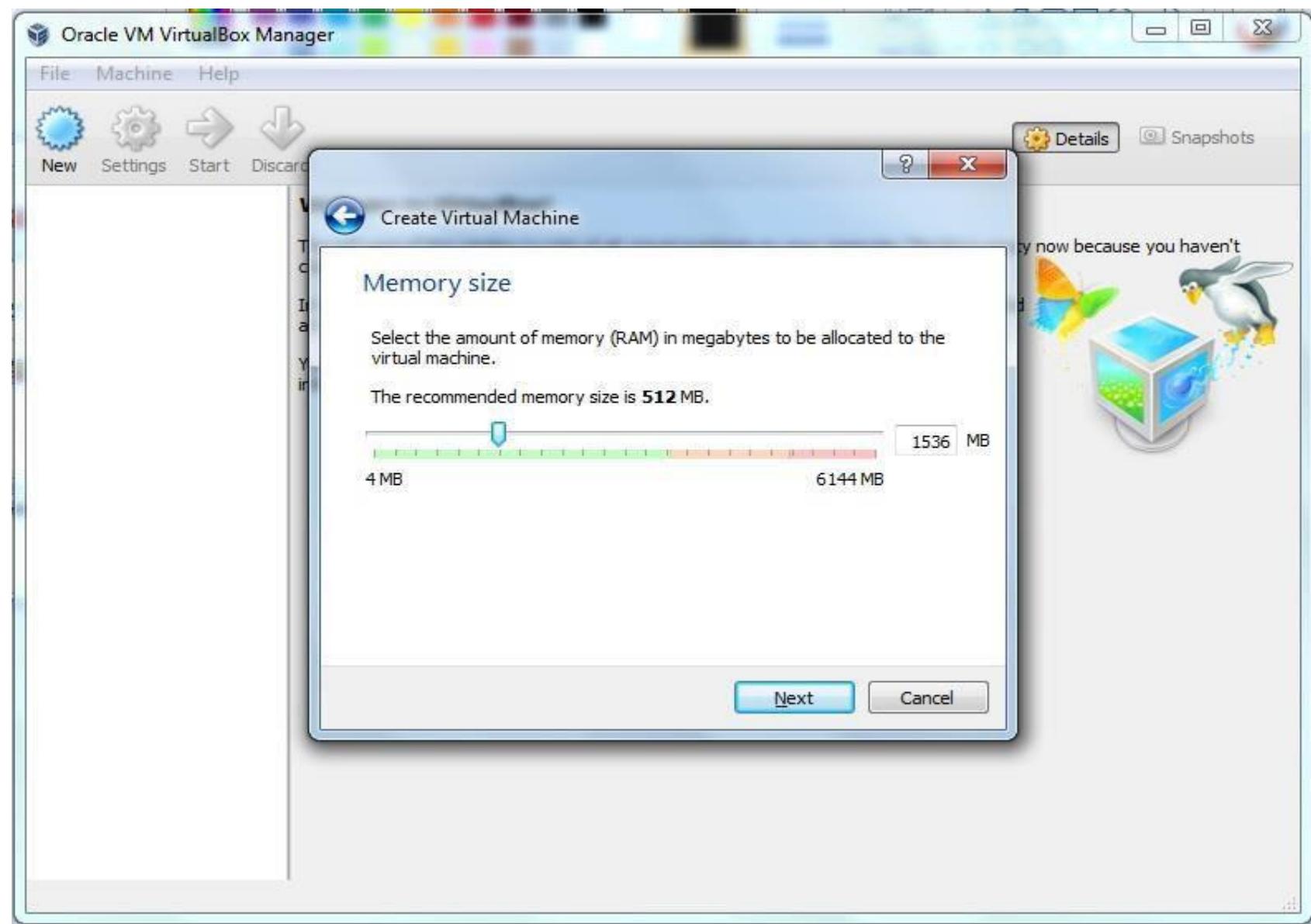


Installing Windows Server 2008

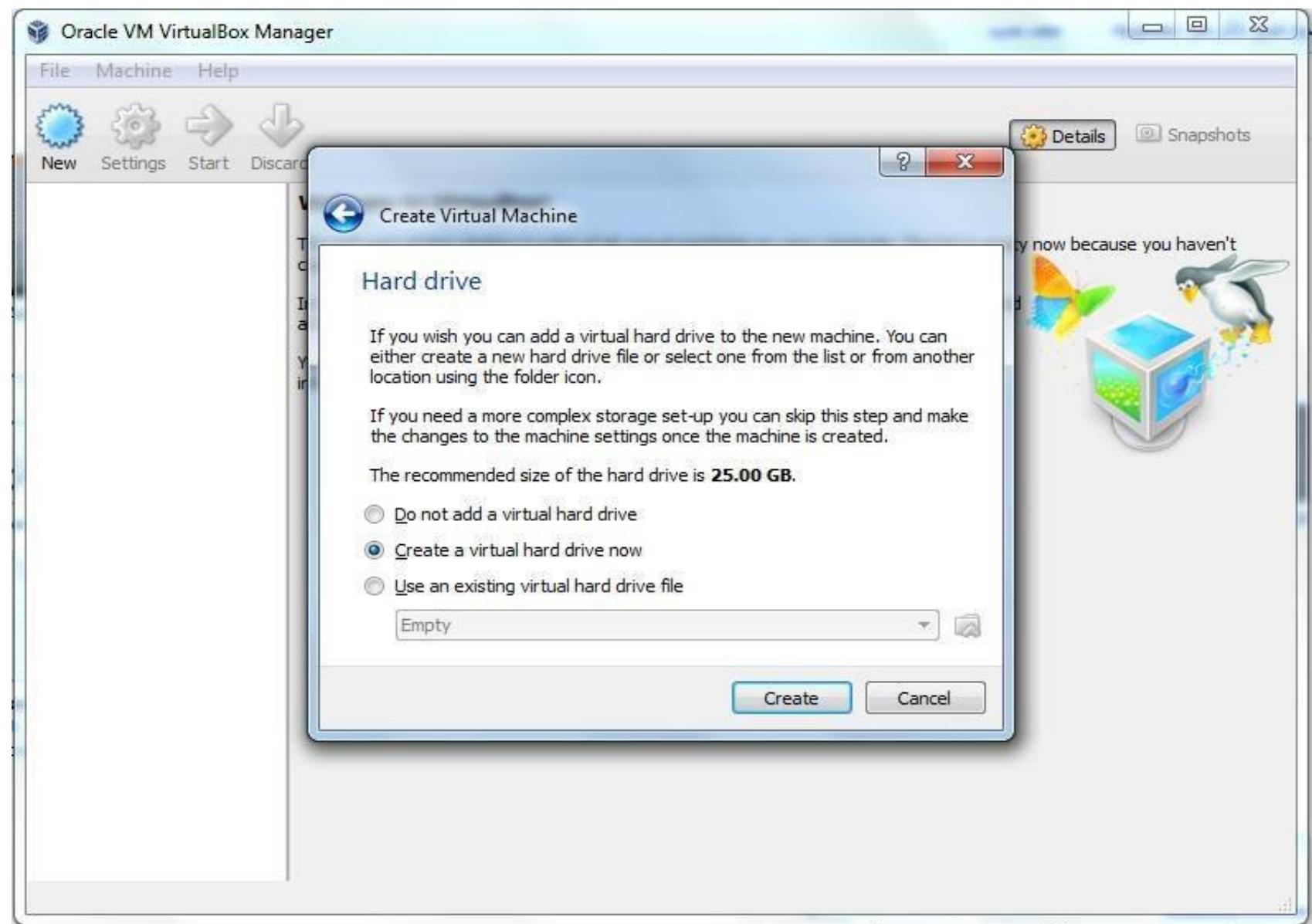
capacity for Windows Server 2008

- It depends on your computer RAM but its recommended to be between 512 MB to 1 GB

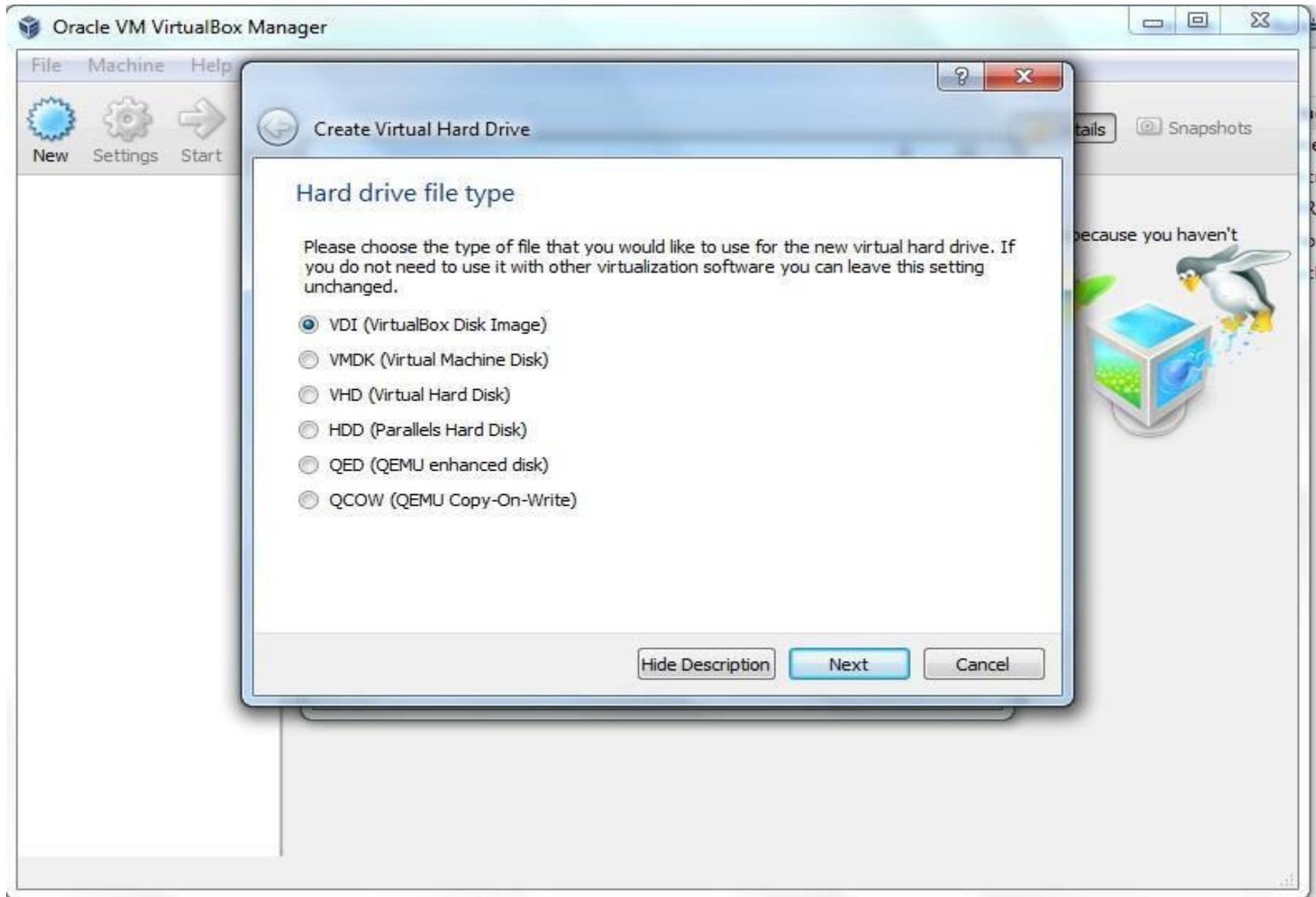
Installing Windows Server 2008



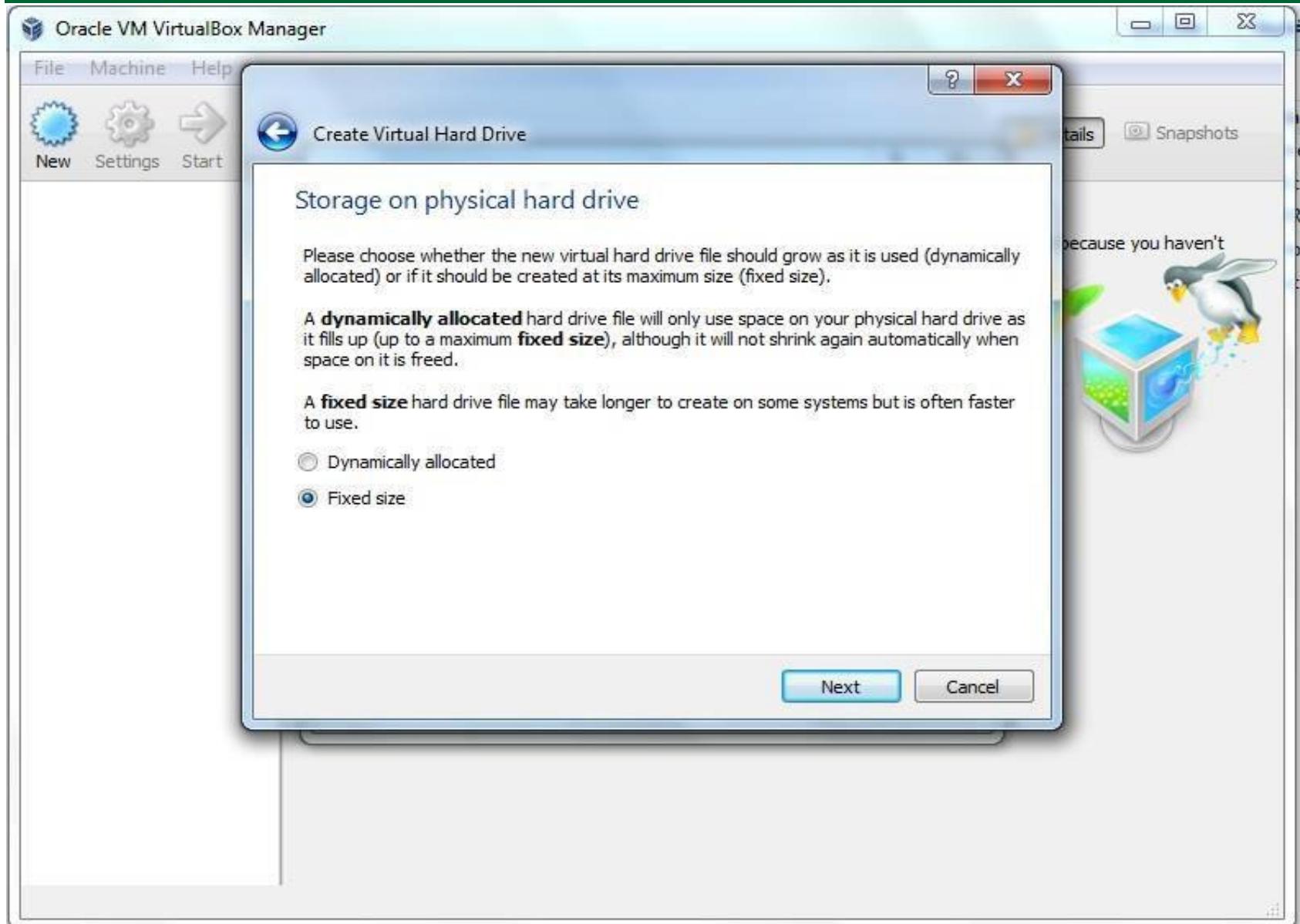
Installing Windows Server 2008



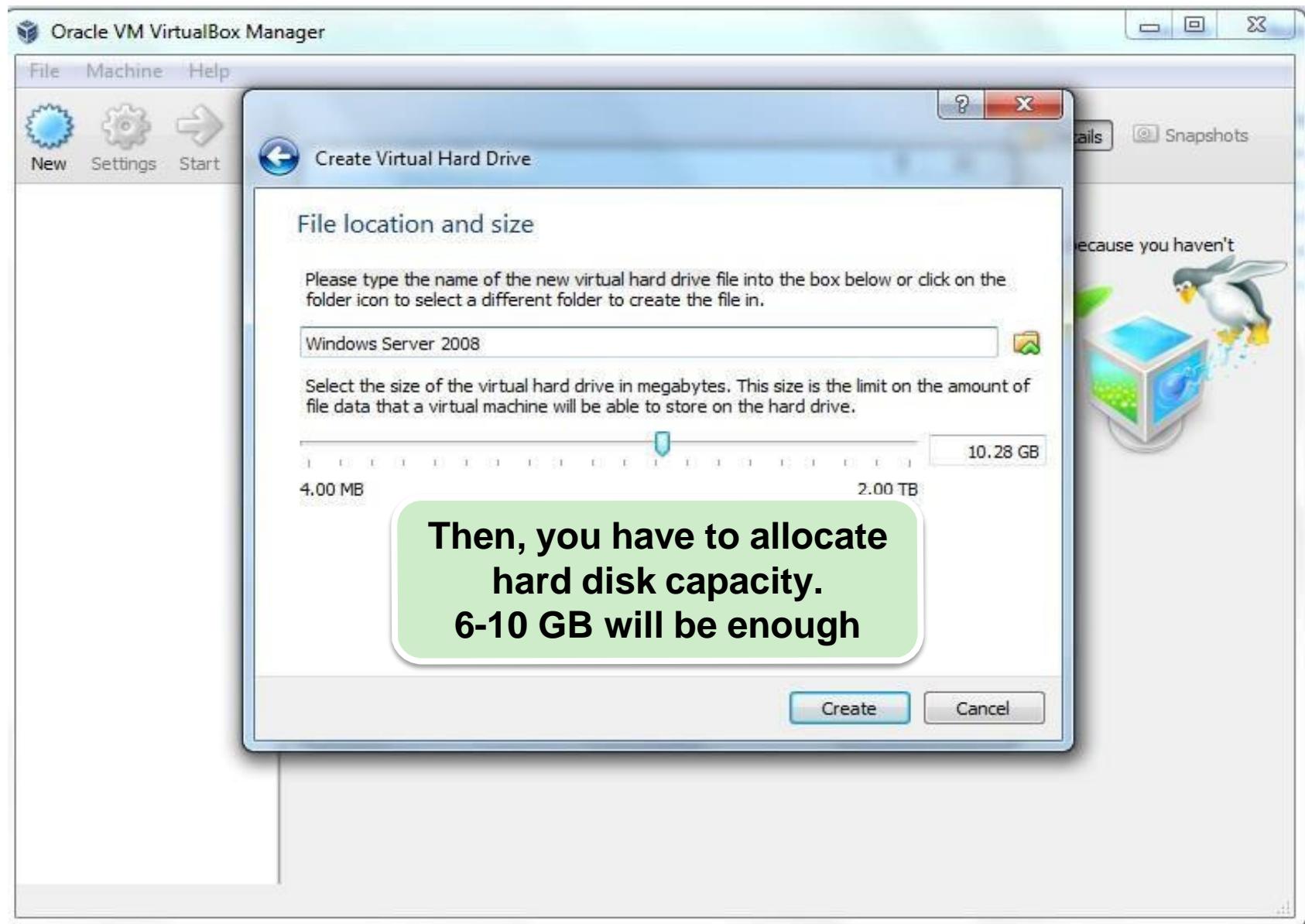
Installing Windows Server 2008



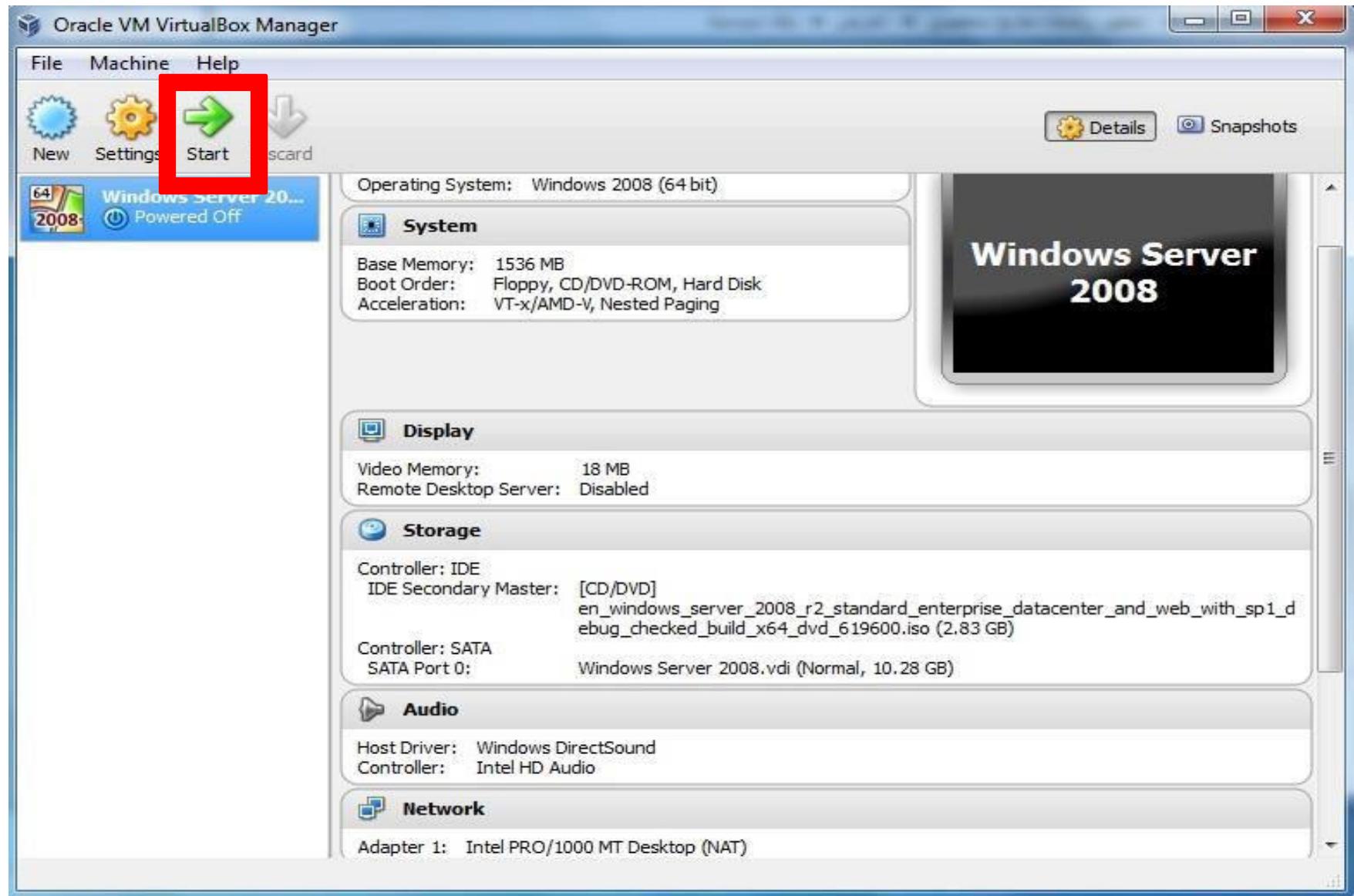
Installing Windows Server 2008



Installing Windows Server 2008



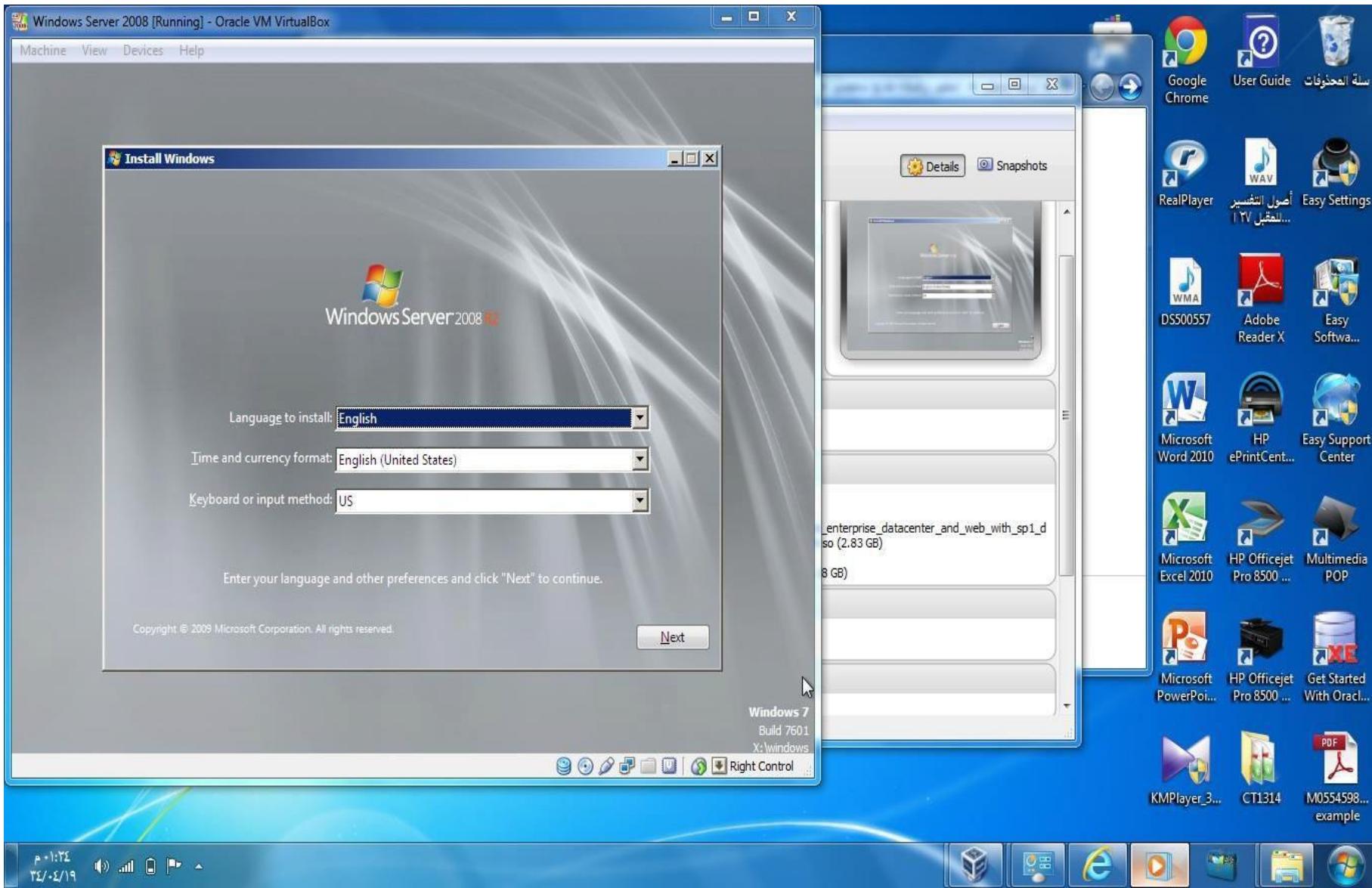
Installing Windows Server 2008



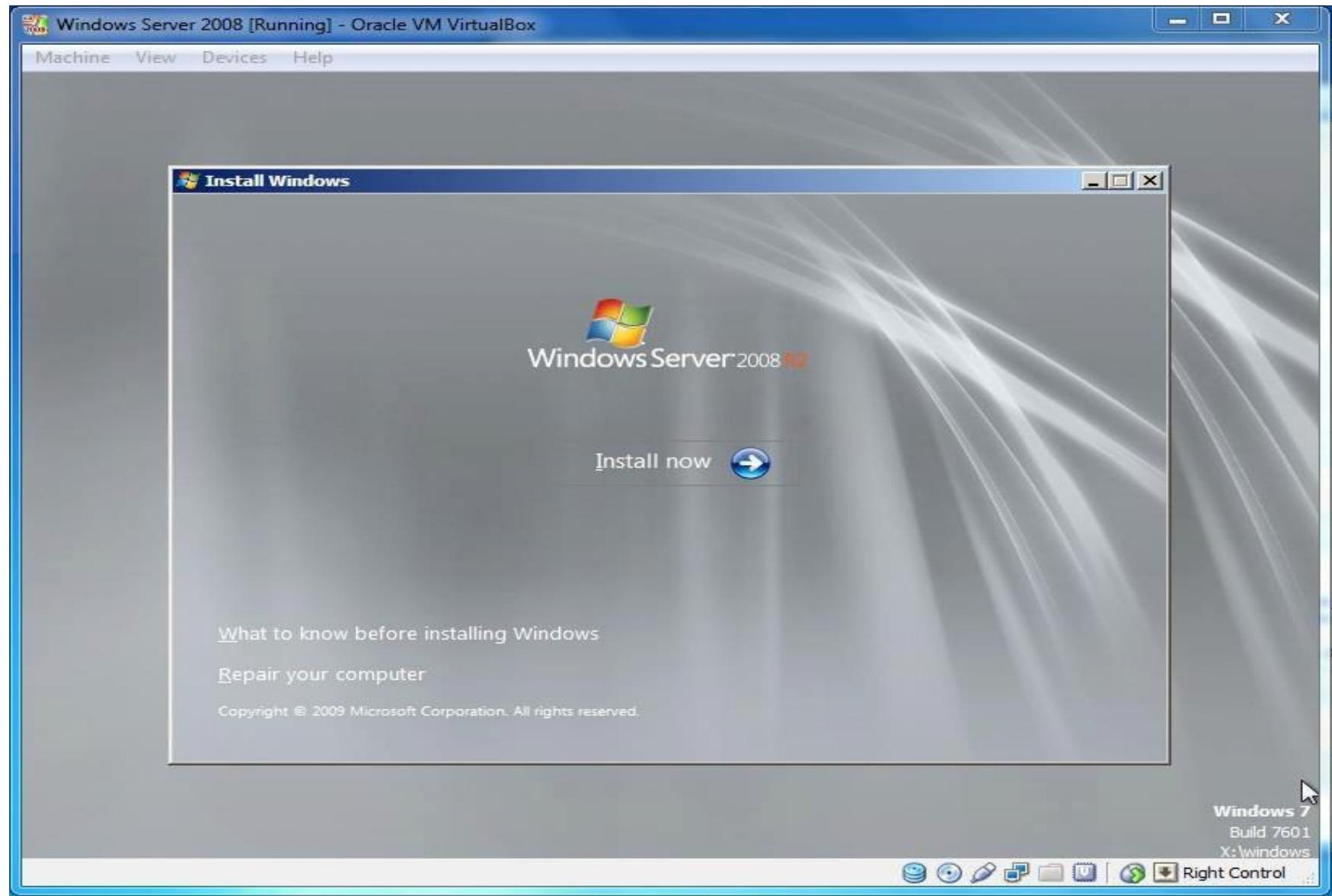
Installing Windows Server 2008

- Windows Server 2008 should start then you will be asked for OS ISO file
- Browse for it then open it

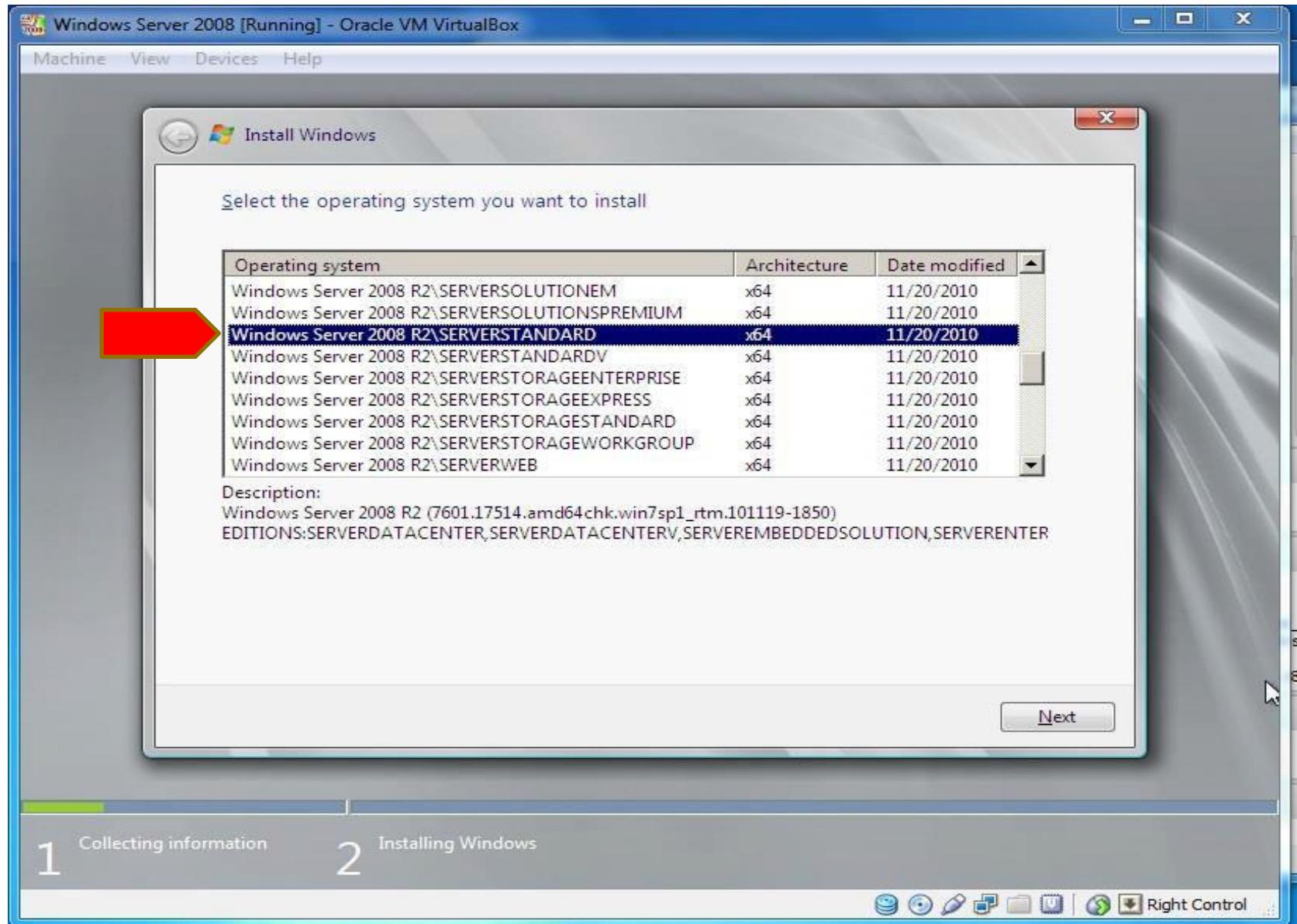
Installing Windows Server 2008



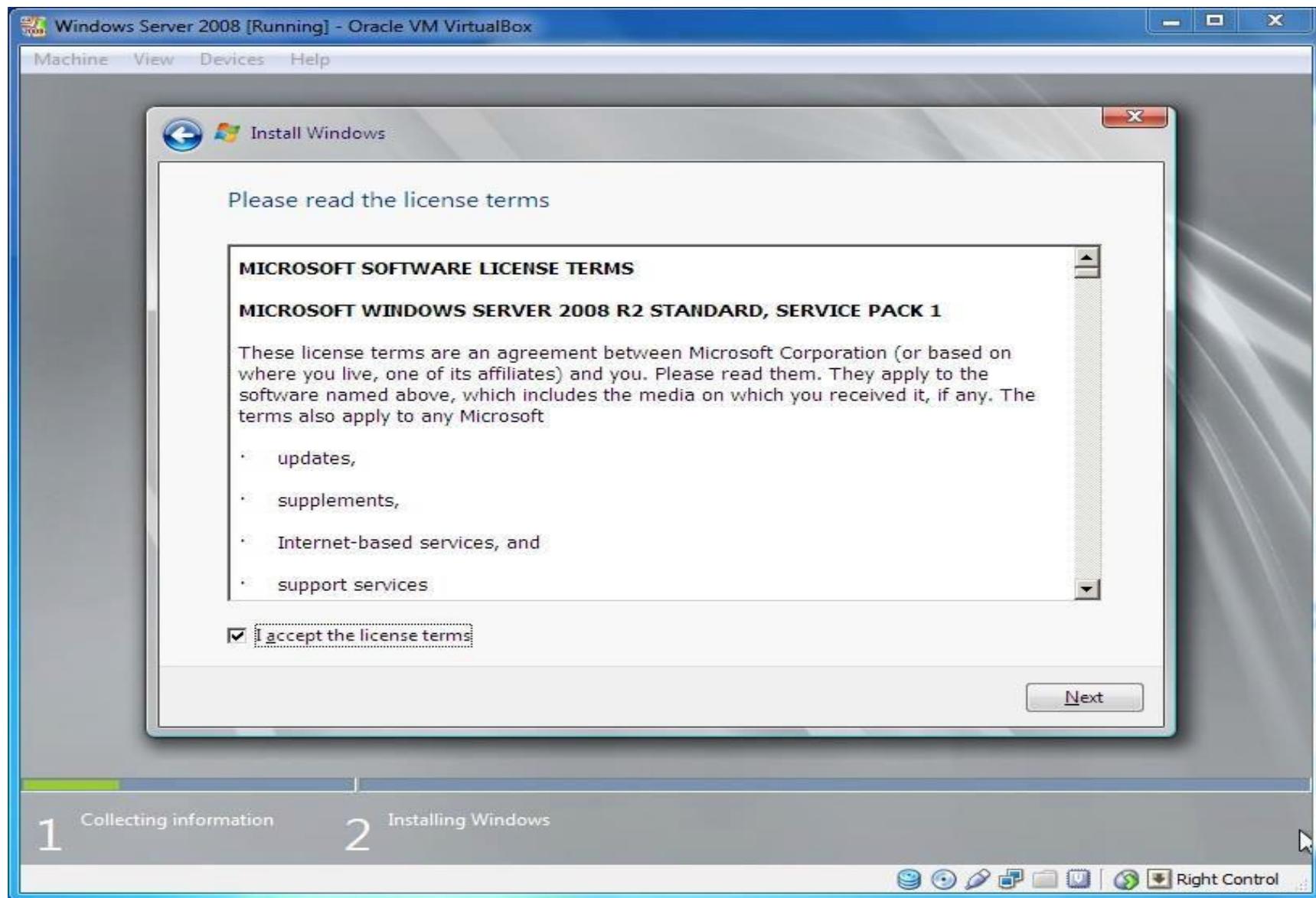
Installing Windows Server 2008



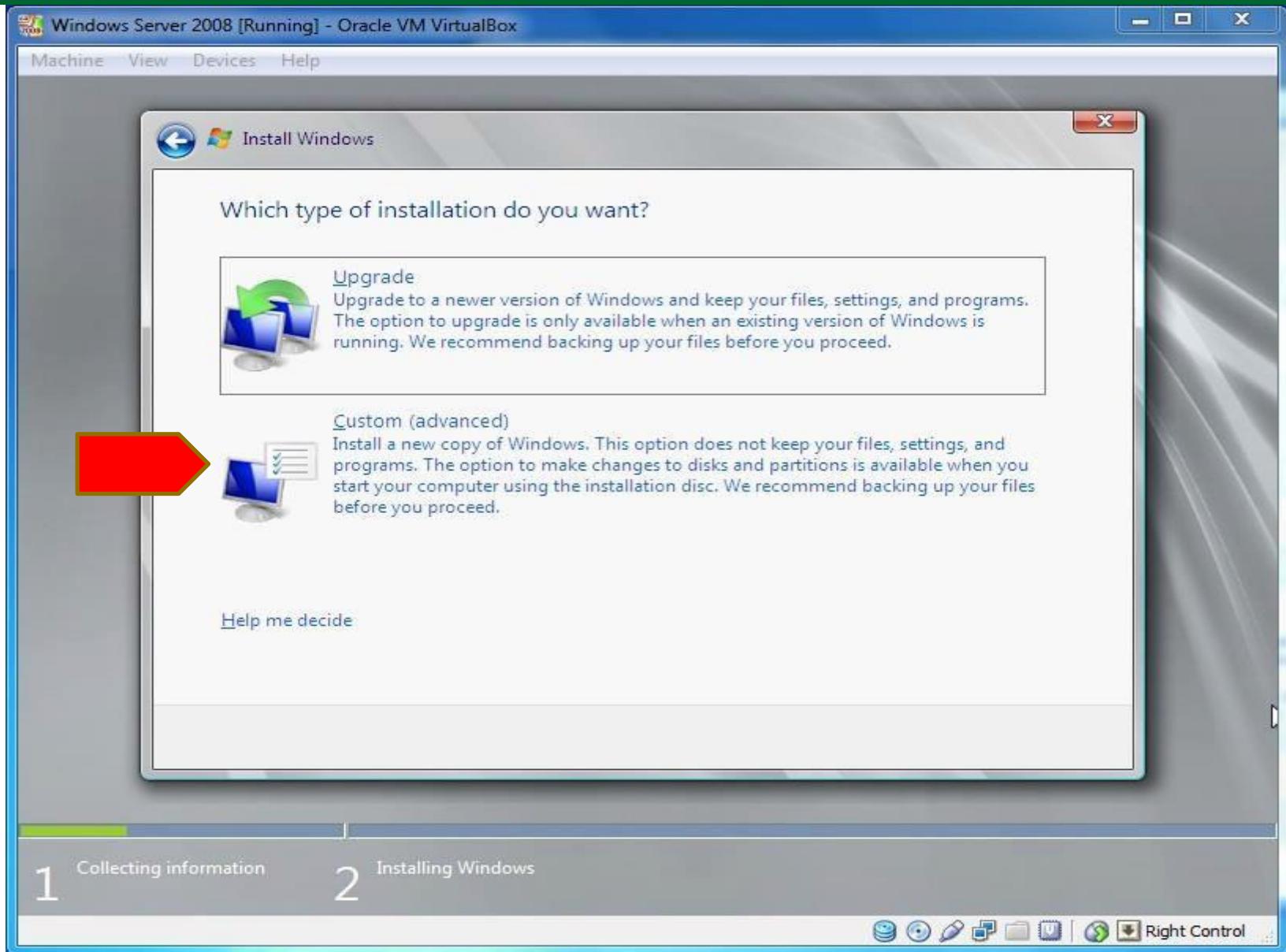
Installing Windows Server 2008



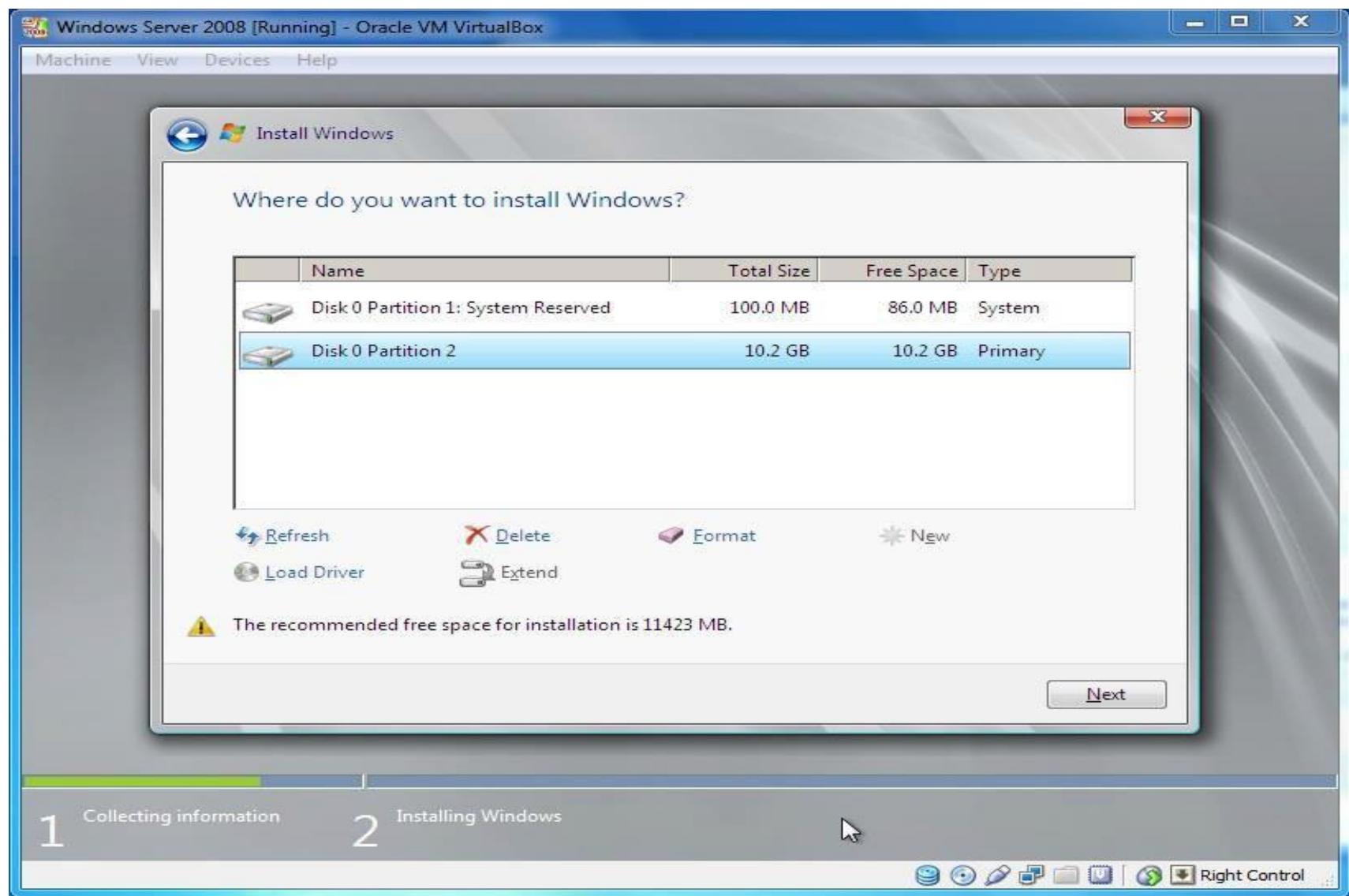
Installing Windows Server 2008



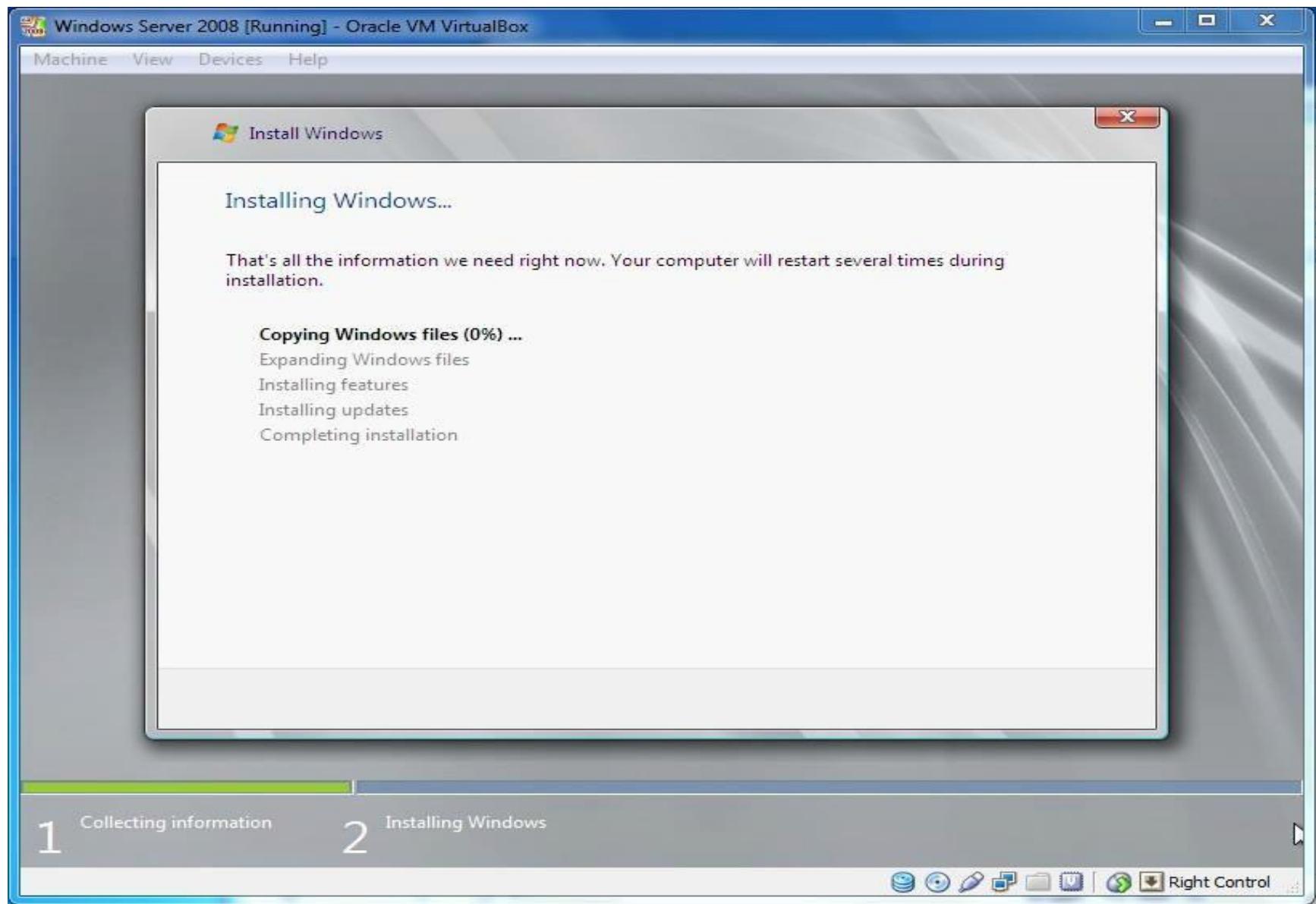
Installing Windows Server 2008



Installing Windows Server 2008



Installing Windows Server 2008



Installation and Configuring of Active Directory

Installation and Configuring of Active Directory Microsoft

Windows networks support two directory service models:

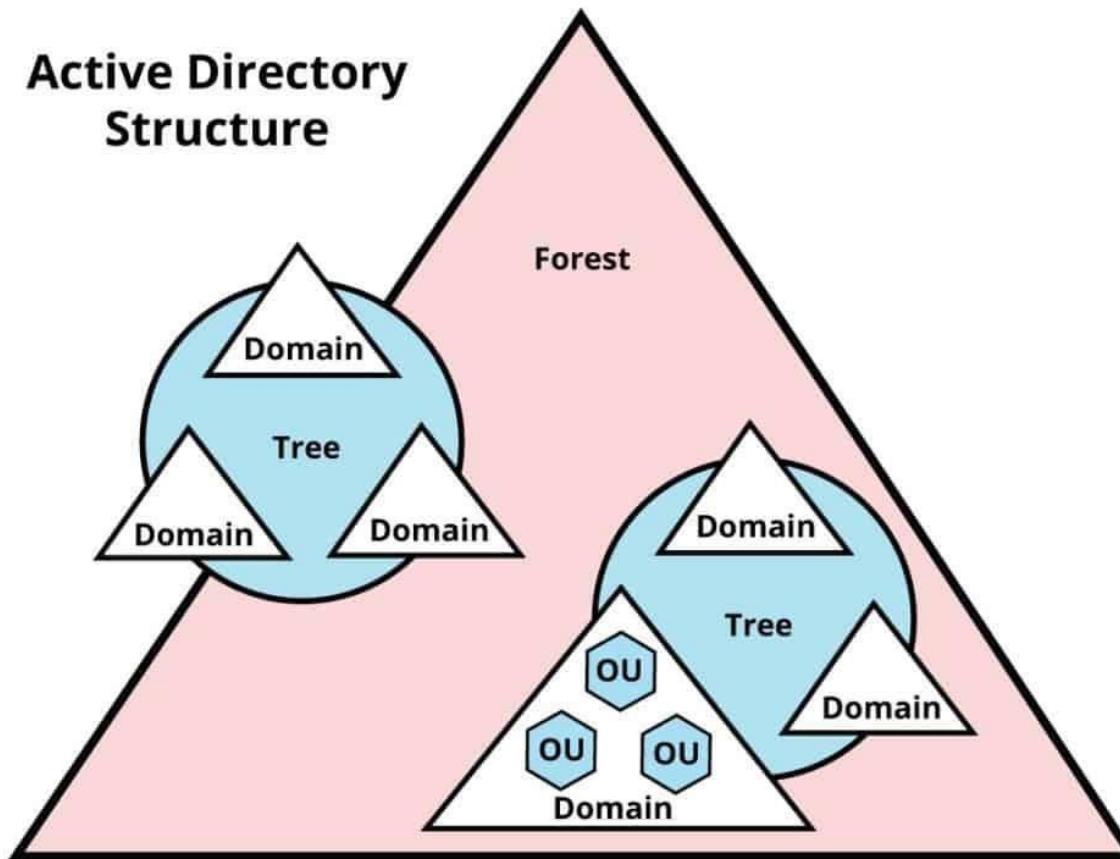
- The workgroup
- And the domain
- The domain model is by far the more common in organizations implementing Windows Server 2003.
- The domain model is characterized by a single directory of enterprise resources that is trusted by all secure systems that belong to the domain.
- Those systems can therefore use the security principals

(user, group, and computer accounts) in the directory to secure their resources.

- Active Directory thus acts as an identity store, providing a

- Active Directory itself is more than just a database.
- It is a collection of supporting files including transaction logs and the system volume, or Sysvol, that contains logon scripts and group policy information.
- It is the services that support and use the database, including Lightweight Directory Access Protocol (LDAP), Kerberos security protocol, replication processes, and the File Replication Service (FRS).
- The database and its services are installed on one or more domain controllers.
- A domain controller is a server that has been promoted by running the Active Directory Installation Wizard by running DCPROMO from the command line or by running the Configure Your Server Wizard.

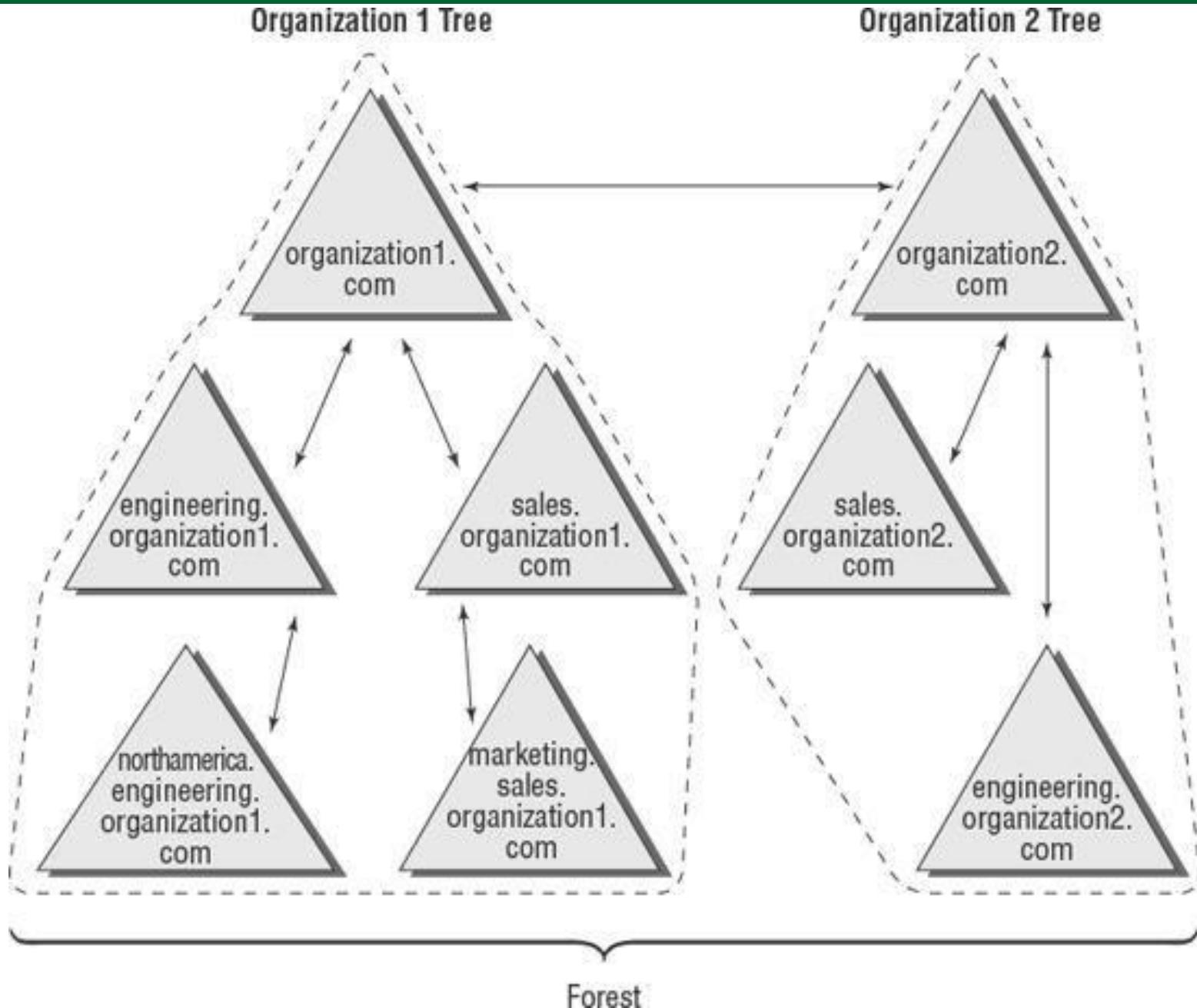
- Once a server has become a domain controller, it hosts a copy, or replica, of Active Directory and changes to the database on any domain controller are replicated to all domain controllers within the domain.



Domain, Trees and Forest Concept:

- **Domain:** A domain is defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database.
 - When you add a domain to an existing tree, the new domain is a child domain of an existing parent domain.
- There is no limit of objects in a domain. Active directory can able to group the very large amount of objects in a single system.
- This is the system that allows system administrators to mange large networks and large amount to users and computers.
- For Ex: DNS; www.google.com in which .com is domain, means of that all the related computers, users, network

Domain, Tree and Forest:



Domain, Tree and Forest:

- Tree:
 - A collection of multiple domains in active directory is called tree.
 - There is always Parent-Child relationship between domains in a tree.
 - As the name suggests, the main domain or level1 domain is like a trunk of tree and other it's child domains are branches, sub branches and leaves of the tree.
- For Ex. mail.google.com,
drive.google.com,

play.google.com,

maps.google.com and sbi.co.in

- As the above examples shows multilevel domains that is actually a tree. .com is level1 domain, .google is level2 domain and mail is level3 domain. As the mail and google both are the child domain of .com and hence all it's child

.com

google.com

cdmi.com

mail.google.co
m

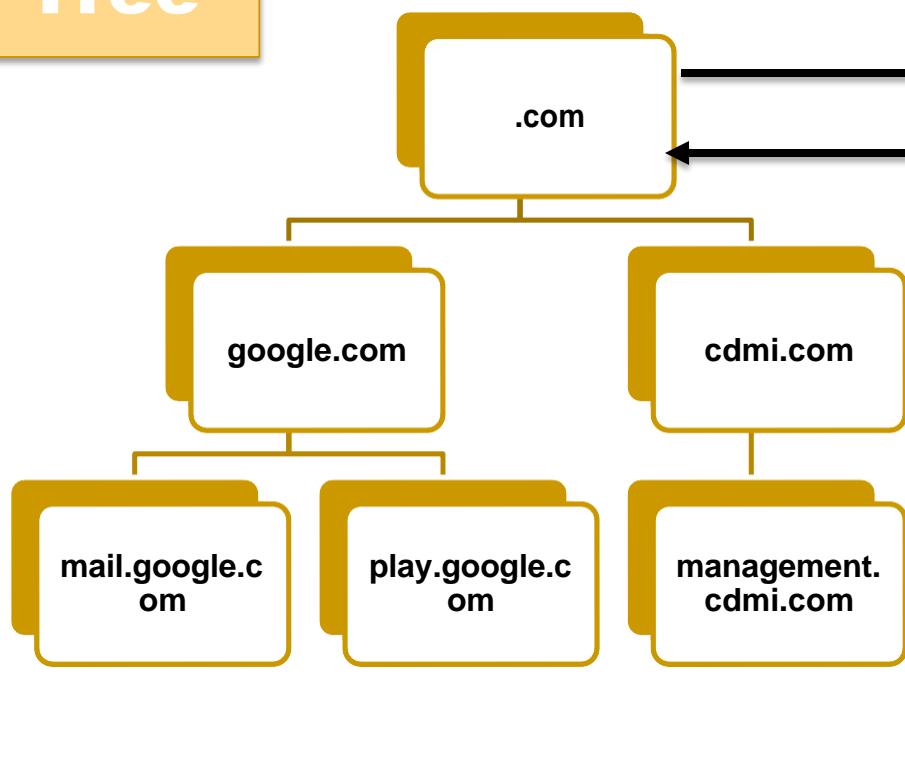
play.google.co
m

management.c
dmi.com

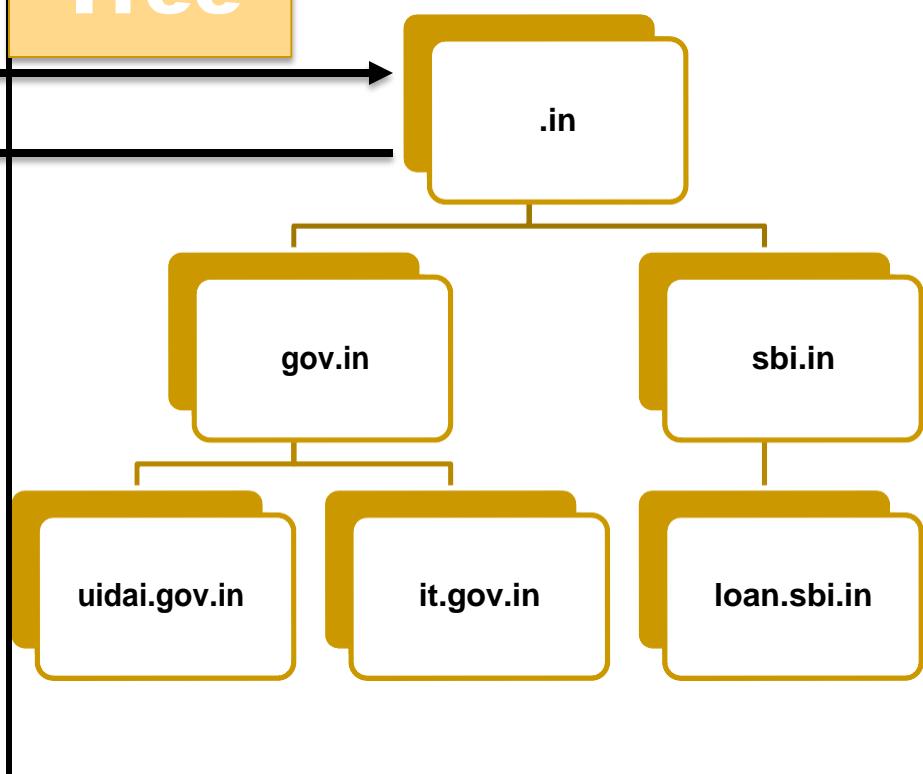
Domain, Tree and Forest:

- Forest: Forest is a collection of multiple domain trees. As the name suggests, there are many trees available in the forest. The adjacent trees may be connected to each others.
- There are multiple trees can be communicated each other by the uni-directional way or bi-directional way in the forest with the help of trust relationship between two trees.
- The forest is considered the primary security boundary in Active Directory.

Tree



Tree



❖ Accounts:

- Account determines 3 factors:
 - When a user may log on
 - Within where the domain/workgroup
 - What privilege level a user is assigned
- **Computer Accounts:** Computer accounts are created and stored in the Active Directory like User and group accounts.
- Computer accounts are used to identify computers in a domain with their security principles.
- A user with a valid user account and a password in Active Directory cannot log on to a domain, if the computer is not represented in that domain.
- Each Windows Server 2003 computer, Windows XP, Windows 2000 Server and Professional computer, Windows NT Server and workstation computer must have a

□ Groups:

- Groups are a collection of user and computer accounts that you manage as a single unit.
- Groups simplify administration by enabling you to grant permissions to resources to the group rather than to each user individually.
- Groups can be nested (groups can be members of other groups).
- In addition to user accounts, you can add other groups, contacts, and computers to groups
- Windows Server 2008 provides the ability to create groups in a stand-alone computer security accounts database in Active Directory

- User:
 - There may be multiple users logged into the single client/computer. At that time user account service allows multiple users to have an access of the particular domain on account of their user credentials.
 - Within a single client each user have their unique login credentials. Each users than differentiated by their user credentials rather than client/computer credentials.
 - Here each user are separately having access of domain form active directory regardless of they are within the

single client / computer.

❖ Policy (Security and Audit)

- Policy is a feature of Windows that facilitates a wide variety of advanced settings that network administrators can use to control the working environment of users and computer accounts in Active Directory.
- It essentially provides a centralized place for administrators to manage and configure operating systems, applications and users' settings.
- Policies, when used correctly, can enable you to increase the security of user's computers and help defend against both insider threats and external attacks.
- **Security** policies are for the purpose of giving a security to the resources of active directories.
- **Audit** policies are the service of checking eventually that

the provided securities are working properly or not.

❖ Logging Events:

- Some operating systems, such as Windows NT, have the capability to keep a running log of system events.
- That log serves as a record of previous errors, warnings, and other messages from the system.
- Studying the event log can help you find recurring errors and discover when a problem first appeared.
- The event log should also be scanned on a regular basis to look for any indications of potential problems.
- Windows NT's Event Viewer application provides you with access to the event log.
- There are three types of events:
 - System Events
 - Security Events

❖ Microsoft Management Console:

- Microsoft management console hosts administrative tools that you can use to administer networks, computer, services, and other system components.
- The first things to understand is that a MMC is a host for an administrative tool called snap in.
- A snap-in is actually an Active –x module that is used to perform a specific function, but without a snap-in a console is useless.

Assignments:

- 1) How to Install Windows Server-2008?
- 2) What are Active Directories? How to configure it in window server – 2008 architecture?
- 3) Explain in details:
 - A. Active Directory Domain
 - B. Active Directory Domain Tree
 - C. Active Directory Domain Forest
- 4) What account? Explain all account services of Active Directory Architecture.
- 5) What is Logging events?

6) What is MMC (Microsoft Management Console)?

Ch-10

Basics of
Network Security

Ch – 10 _ Basics of Network Security, Content...

❖ Fundamentals of Network Security

❖ Requirements of Network Security

❖ Policies, Standards, Procedures, Baselines, Guidelines

❖ Security methods

- Encryption
- Cryptography
- Authentication

❖ Security principle – CIA Model

❖ Fundamentals of Network Security:

- ❑ We live in an age of information. Businesses these days are more digitally advanced than ever, and as technology improves, organizations' security postures must be enhanced as well. Now, with many devices communicating with each other over wired, wireless, or cellular networks, network security is an important concept.
- ❑ **What is Network Security?**
- ❑ Network security is the process of taking defensive actions to protect the underlying / central networking infrastructure from unauthorized access, misuse, malfunction or breakdown, modification, damage or improper identification.
- ❑ Once a network is secured, the users and the devices

connected can work without experiencing data breaches. In

Fundamentals of Network Security

- When you are planning, designing, or implementing a network or are assigned to operate and manage one, it is useful to ask yourself the following questions:
 1. What are you trying to protect or maintain?
 2. What are your business objectives?
 3. What do you need to achieve these objectives?
 4. What technologies are required to support these objectives?
 5. Are your objectives compatible with your security infrastructure, operations, and tools?
 6. What risks are related with poor security?
 7. What are the effects of not implementing security?
 8. How do you reduce that risk?
 9. What is your tolerance / acceptance for risk?

❖ Requirements of Network Security:

- ❑ As we know that today internet becomes virtual world. Each and every users generates large amount of data and that may be personal or professional. So users frequently needs store these data elsewhere servers or storage devices.
- ❑ The path that users choose to transfer their data to specific server is obviously a computer networks and the network always / sometimes acts as public network. It means data are going through the publically. Hence, there may be a chance of data to be theft, hacking, tempered or completely destroyed.
- ❑ It's just not only to protect our data but also have to protect network devices as well. Network security always concerns security in two way. Firstly secure network devices so that overall we secures data transportations.

Here's why both businesses and households should consider the security of their networks seriously:

- **To protect the computers in the network:**

Computers and other devices connected to unsecured networks are highly vulnerable to external threats such as malware, ransomware and spyware attacks. A single attack can bring down the entire computer system of an organization and compromise your personal information. By assuring the security of the network – typically with the assistance of a network security specialist – you can stay away from such expensive threats.

- **To prevent identity theft:**

No matter whether you are an organization or an individual, your identity is valuable. If you log into an unsecured network, your identity can become visible to third-parties.

To avoid such a situation, you should secure your network.

To protect shared data:

When it comes to a business, special precautions should be taken to protect shared data. And, network security is one of the best ways to do so. Network security can be applied with different restrictions on different computers depending on the types of files they handle.

To stabilize the network connection:

In an unrestricted, unprotected network, network activity can become too heavy. Intense traffic can lead to an unstable computer network. Eventually, the entire network will become vulnerable to various external attacks.

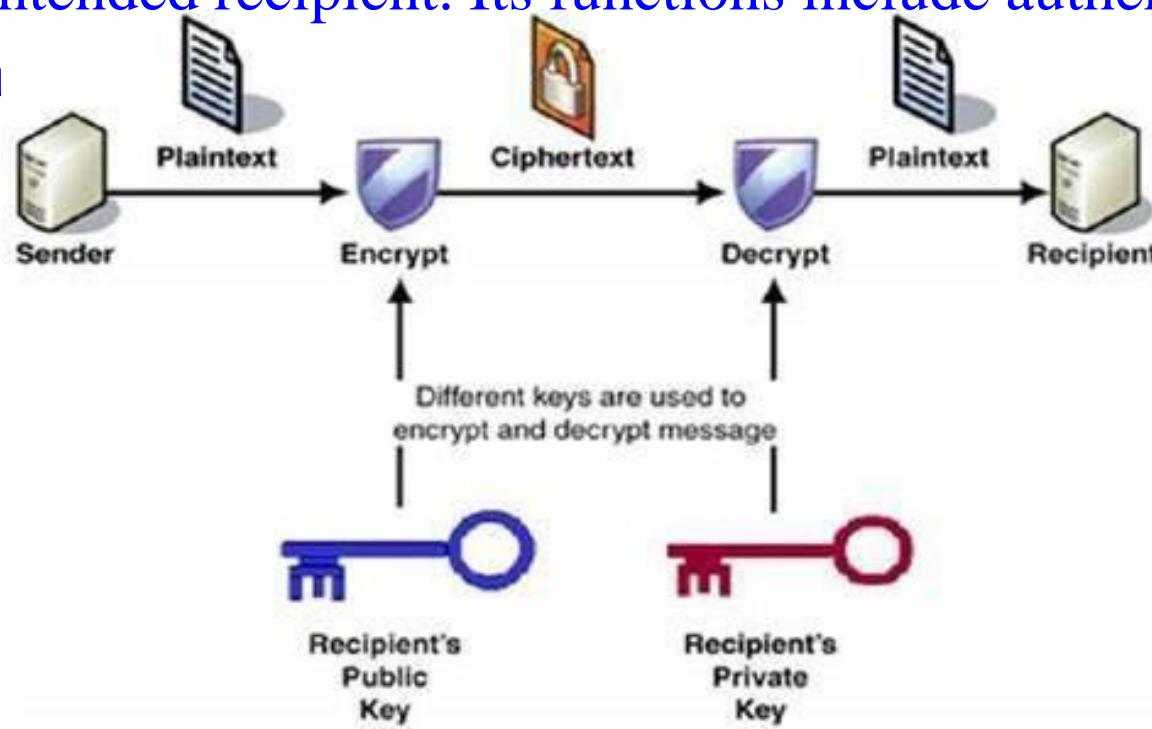
❖ Policies, Standards, Guidelines & Procedures:

- ❑ Part of the management of any security program is determining and defining how security will be maintained in the organization.
- ❑ **Policies:** Intended to be a set of overarching principles, they do not have to be long or complicated.
- ❑ **Standards:** Outline a set of minimum requirements which must be met when commissioning a new asset. For example, the minimum requirements for locking down the Windows operating system; or a standard used to assess eligibility for security clearance.
- ❑ **Guidelines:** Intended to outline best practice - they are not mandatory, but help employees follow the rules while allowing for flexibility and common sense in different scenarios.
- ❑ **Procedures:** These are how the policies should be enacted in the

❖ Security Methods:

1. Cryptography: Cryptography, as name suggests, is generally study of methods like encryption. Its main objective is to provide methods simply to secure and protect information and communications using encryption and related techniques.

- It simply allows one to store sensitive information or transmit it across insecure networks so that it cannot be read or accessed by anyone except intended recipient. Its functions include authentication, nonrepudiation, and integrity.



Security Methods:

2. Encryption: Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called *cryptography*.

- In computing, unencrypted data is also known as *plaintext*, and encrypted data is called *ciphertext*. The formulas used to encode and decode messages are called *encryption algorithms*, or *ciphers*.
- To be effective, a cipher includes a variable as part of the algorithm. The variable, which is called a *key*, is what makes a cipher's output unique. When an encrypted message is caught by an unauthorized person, the intruder has to guess which cipher and what keys or variables the sender used to encrypt the message. The time and difficulty of guessing this information is what makes encryption such a

Security Methods:

- Historically, it was used by militaries and governments. In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

3. Authentication: Authentication is the process of recognizing or identifying a user's identity whether it is true, real, or not. It's simply a verification of claim whether you are who you say you are or not.

- There are many authentication methods available nowadays like password authentication that includes using a password, physical authentication that includes the scannable card or smart card or digital certificate, biometric authentication that includes signatures and fingerprints, or visual identification, OTP and many more.
- Authentication technology provides access control for

Security Principles – CIA Model

- In present day scenario security of the system is the sole priority of any organization. The main aim of any organization is to protect their data from attackers. In cryptography, attacks are of two types such as Passive attacks and Active attacks.
- Passive attacks are those that retrieve information from the system without affecting the system resources while active attacks are those that retrieve system information and make changes to the system resources and their operations.
- The Principles of Security can be classified as follows:
 1. Confidentiality
 2. Integrity
 3. Availability



CIA Model _ 1. Confidentiality:

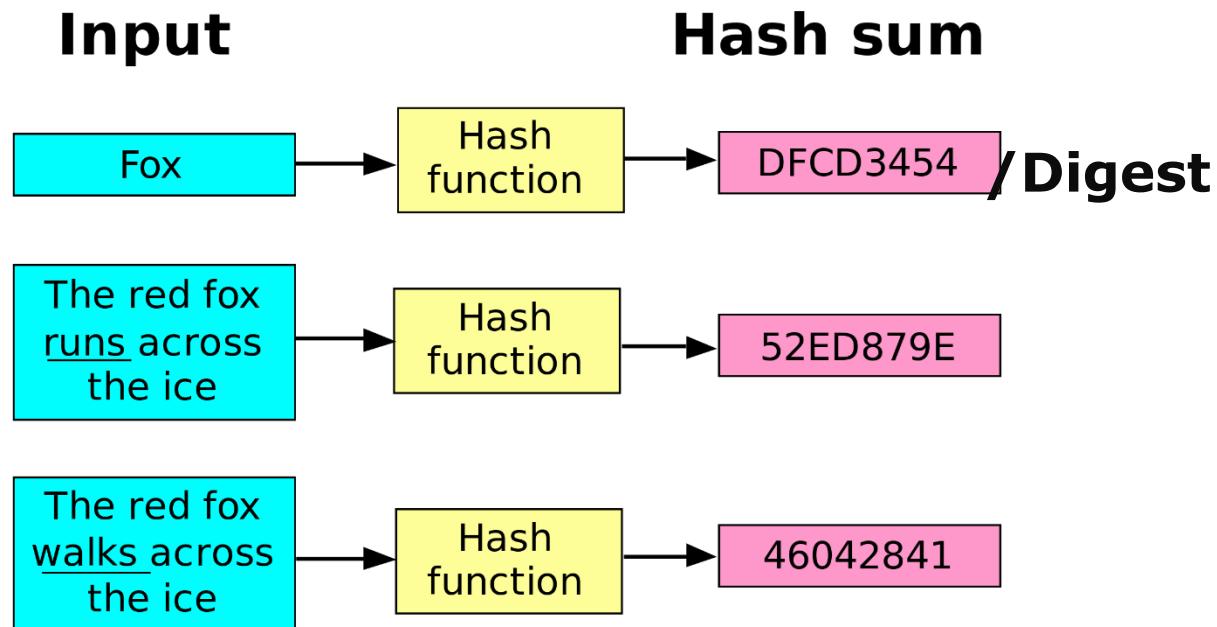
- ❑ Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals.
- ❑ The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it.
- ❑ Encryption standards include **AES**(Advanced Encryption Standard) and **DES** (Data Encryption Standard). Another way to protect your data is through a VPN tunnel. VPN

2. Integrity:

- The next thing to talk about is integrity. Well, the idea here is to make sure that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function.
- We have two common types: SHA (Secure Hash Algorithm) and MD5(Message Direct 5). Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1. There are also other SHA methods that we could use like SHA-0, SHA-2, SHA-3.

Integrity:

- Let's assume Host 'A' wants to send data to Host 'B' maintaining integrity. A hash function will run over the data and produce an arbitrary hash value **H1** which is then attached to the data. When Host 'B' receives the packet, it runs the same hash function over the data which gives a hash value **H2**. Now, if **H1 = H2**, this means that the data's integrity has been maintained and the contents were not modified.



3. Availability:

- The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.
- This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network.
- Attacks such as DoS (Daniel-of-Service) may render a network unavailable as the resources of the network get exhausted.
- The main goal of the availability is specifies that to reduce

Assignments:

- 1) What is network security? What are the fundamentals of network security? Explain briefly.
- 2) Describe requirements / need of network Security.
- 3) Express following terms:
 - i. Policies
 - ii. Standards
 - iii. Procedures
 - iv. Baselines
 - v. Guidelines
- 4) Explain various security methods.
- 5) Describe in details: Security Principles – CIA Model



Basics of Internet Connection & Sharing

Contents...

- ❖ **Basics of Internet**
- ❖ **How Internet is connect with Computer**
- ❖ **Technology related Internet**
 - ❑ Dial-Up Technology
 - ❑ ISDN Network Technique
 - ❑ Lease Line Technique
- ❖ **VPN**
 - ❑ Types of VPN
 - ❑ Use of VPN
 - ❑ VPN Protocols
 - ❑ PPTP
 - ❑ L2TP
 - ❑ IPsec
- ❖ **Proxy Server, Firewall**

❖ Basics of Internet:

- ❑ The Internet is a global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news and opinions. According to Internet World Stats, as of December 31, 2011 there was an estimated 2,267,233,742 Internet users worldwide. This represents 32.7% of the world's population.
- ❑ Internet is a system that interconnects the different computer systems across the world. It uses the Internet protocol suite to link devices located in different corners of the world.
- ❑ The Internet system carries an extensive range of information resources and services including World Wide Web (WWW), telephony, electronic mail, etc. It uses standard internet protocols, such as TCP/IP and HTTP, etc.

History of Internet:

- The first development was the introduction of host-to-host network interactions. This was first observed in ARPANET in 1969. It was developed by Advanced Research Projects Agency (APRA) of the Department of Defence, U.S.
- Next step was commercialising the usage and making the transistors and transmitters fit in smaller devices for convenient Internet usage for the general public. This was introduced in the 1970s.
- Moving forward, satellites and wireless communication was the main target. Defence Advanced Research Projects Agency (formerly ARPA), supported satellite-based radio packets for mobile usage of networks.
- The next was the development of TCP. This enabled different machines and networks across the world to assemble data packets. It was in the 1980s that the TCP/IP approach was adapted by researchers and technologists.
- In 1993, the web browser was introduced, which followed the point-and-click approach and is now a widely used operation for Internet users.
- The late 1990s was the time when thousands of Internet Service Providers has taken up the

Basics of Internet:

- ❖ **Features of Internet**
- **Accessibility:** An Internet is a global service and accessible to all. Today, people located in a remote part of an island or interior of Africa can also use Internet.
- **Easy to Use:** The software, which is used to access the Internet (web browser), is designed very simple; therefore, it can be easily learned and used. It is easy to develop.
- **Interaction with Other Media:** Internet service has a high degree of interaction with other media. For example, News and other magazine, publishing houses have extended their business with the help of Internet services.
- **Low Cost:** The development and maintenance cost of Internet service are comparatively low.
- **Extension of Existing IT Technology:** This facilitates the sharing of IT technology by multiple users in organizations and even facilitates other trading partners to use.
- **Flexibility of Communication:** Communication through Internet is flexible enough. It facilitates communication through text, voice, and video too. These services can be

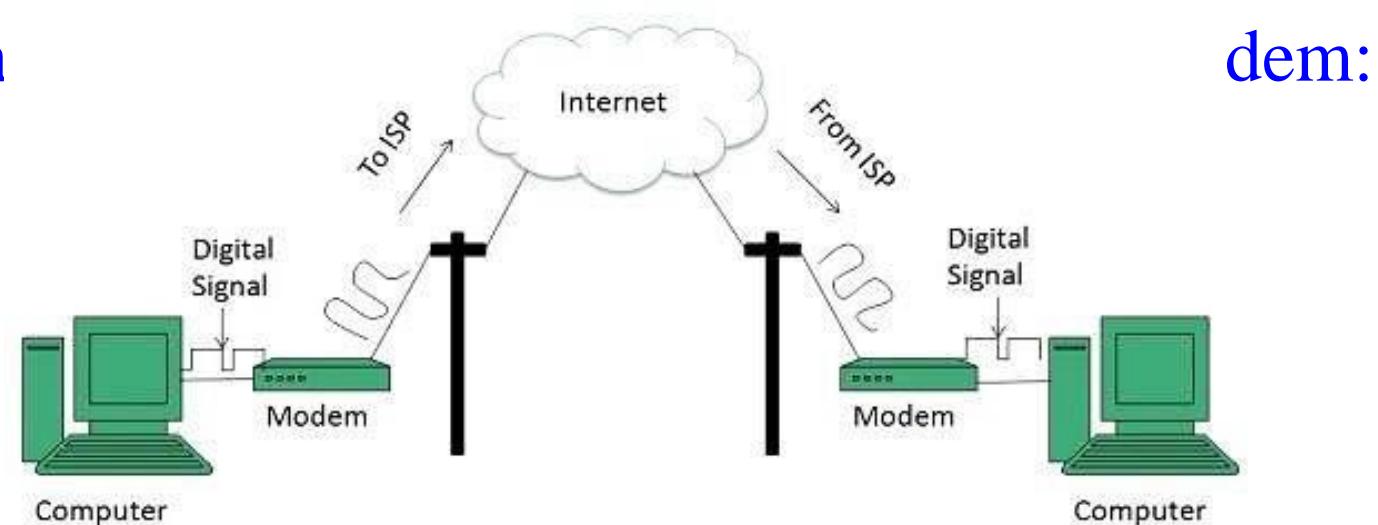
availed at both organizational and individual levels.

How Internet is Connect with Computers:

- The very first requirement for any computer to connect to the internet is the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol is used by computers.
- A network interface card (NIC) is required for a computer in order to connect to the Internet as well as other computers on a network. The NIC is on one end of a network connection that connects a computer to the Internet and other computers, while a cable modem, DSL modem, router, or switch is on the other end.
- **ISP(Internet Service Provider):** These guidelines apply to ISPs or companies that provide Internet access and connectivity. ISP serves as a pipeline between your computer and the rest of the world's computers that are linked to the Internet. TCP/IP protocols are used by the ISP to establish computer-to-computer connections and to send data between them. An Internet service provider (ISP) assigns your computer or network an IP address, which is a unique address that allows your computer or network to interact over the Internet.

❖ Technology related Internet

- **Dial-up Connection:** Dial-up connection uses telephone line to connect PC to the internet. It requires a modem to setup dial-up connection. This modem works as an interface between PC and the telephone line.
- There is also a communication program that instructs the modem to make a call to specific number provided by an ISP.
- Dial-up connection uses either of the following protocols:
 - Serial Line Internet Protocol (SLIP)
 - Point to Point Protocol (PPP)
- The following diagram illustrates a dial-up connection to the Internet.



Technology related Internet:

- **ISDN:** ISDN is acronym of **Integrated Services Digital Network**. It establishes the connection using the phone lines which carry digital signals instead of analog signals.
- ISDN is a circuit-switched telephone network system, but it also provides access to packet-switched networks that allows digital transmission of voice and data. This results in potentially better voice or data quality than an analog phone can provide. It provides a packet-switched connection for data in increments of 64 kilobit/s. It provided a maximum of 128 kbit/s bandwidth in both upstream and downstream directions.

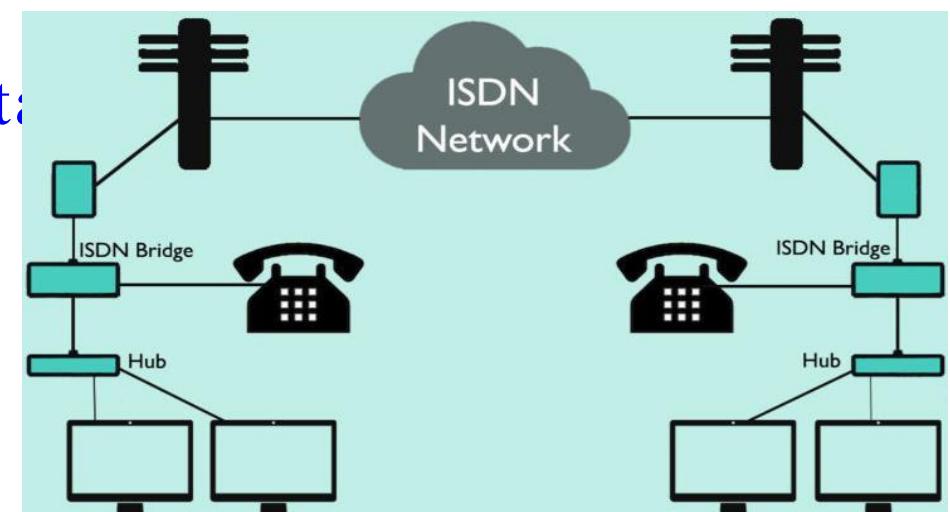
□ **Advantages:**

- ISDN channels have a reliable connection.
- ISDN is used to facilitate the user with multiple digital connections.

- It has faster data transfer rate.

□ **Disadvantages:**

- ISDN lines costlier than the other telephone system.



- It requires specialized digital devices.

Technology related Internet:

- A leased line is a dedicated communication channel that interconnects two or more sites. This is a service contract between a customer and a provider. It acts as a dedicated tunnel from one point to the other where data can continuously flow for a fixed monthly fee or rent, hence the name. Leased lines are used for Internet, data and even telephone services. They are typically run on fiber optic cables to provide large bandwidth and speed.
- Leased line is not really a dedicated physical connection, but a reserved circuit between two designated points that is open at all times.
- This is unlike traditional telephone services, which reuse the same circuit through switching. They are typically rented by large companies to connect two or more sites that need constant fast connection. These lines are leased by large telecommunication companies and are generally quite expensive. The alternative to this is to use the public switched networks.

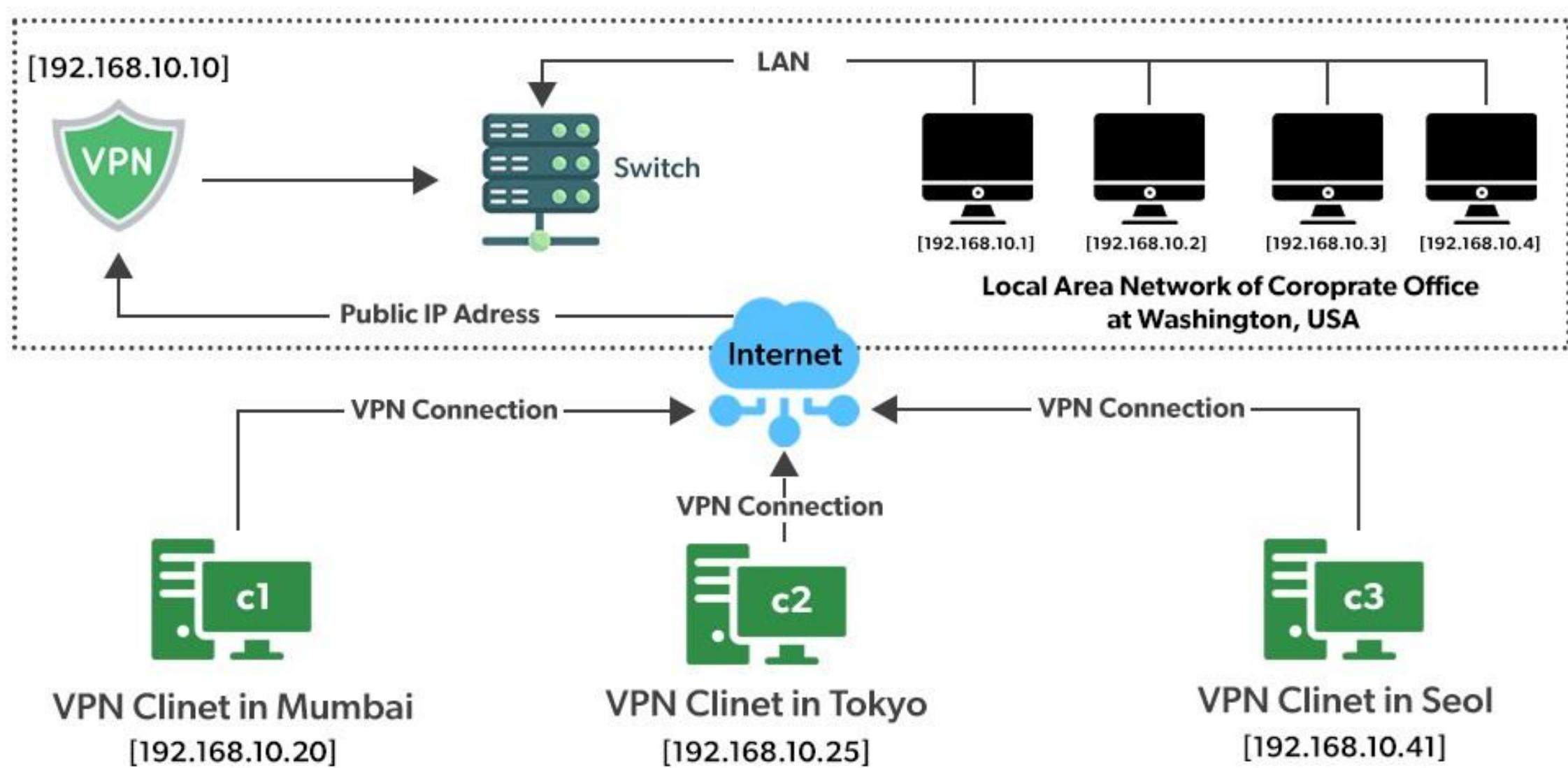
❖ VPN

- VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual “private network” i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.
- For Ex: Think of a situation where corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan. The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job. VPN lets us overcome this issue in an effective manner.

VPN:

- All 100 hundred computers of the corporate office at Washington are connected to the VPN server(which is a well-configured server containing a public IP address and a switch to connect all computers present in the local network i.e. in US head office).
- The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.
- Thus person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
- So this is the inbuilt way of extending the local network even across the geographical borders of the country.

VPN:



Types of VPN:

- **Remote Access VPN:** Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely.
- The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.
- An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network.
- Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

Types of VPN:

- **Site to Site VPN:** A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.
- **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.
- In Site-to-site VPN one router acts as a VPN Client and another router as a VPN Server as it is based on Router-to-Router communication. When the authentication is validated between the two routers only then the communication starts.

□ Use of VPN:

- **1. Safety and Security:** The first and the most important reason people use VPN is its safety feature. It provides an encrypted tunnel for transferring data to and from your device and the host site. This removes all chances of spying and snooping on your data. Even your own internet service provider (ISP) can't access your data or track your activities.
- **2. Anonymity / No Identity:** Another crucial reason that people choose to use a VPN is because it respects and preserves your anonymity. VPN allows its users to explore the internet from different location servers. This way all the traffic is directed to and from the server, and your location as well as identity remain anonymous even to the host site.
- **3. Breaking Geo-Restrictions:** The Internet provides endless sources of entertainment and infotainment but unfortunately, these sources are not accessible for all. Most of the content on the internet is geo-restricted. This means that the content is available only for users living in certain geographical locations while

❖ VPN Protocols:

- **Internet Protocol Security (IPSec):** Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection. IPSec runs in 2 modes:
 - (i) Transport mode: to encrypt the message in the data packet.
 - (ii) Tunneling mode: encrypts the whole data packet.
- **Point-to-Point Tunneling Protocol (PPTP):** PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.
- **Layer 2 Tunneling Protocol (L2TP):** L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol

VPN Protocols:

- ❑ **Internet Protocol Security (IPSec):** Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection.
- ❑ **Layer 2 Tunneling Protocol (L2TP):** It is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.

Point-to-Point Tunneling Protocol (PPTP):

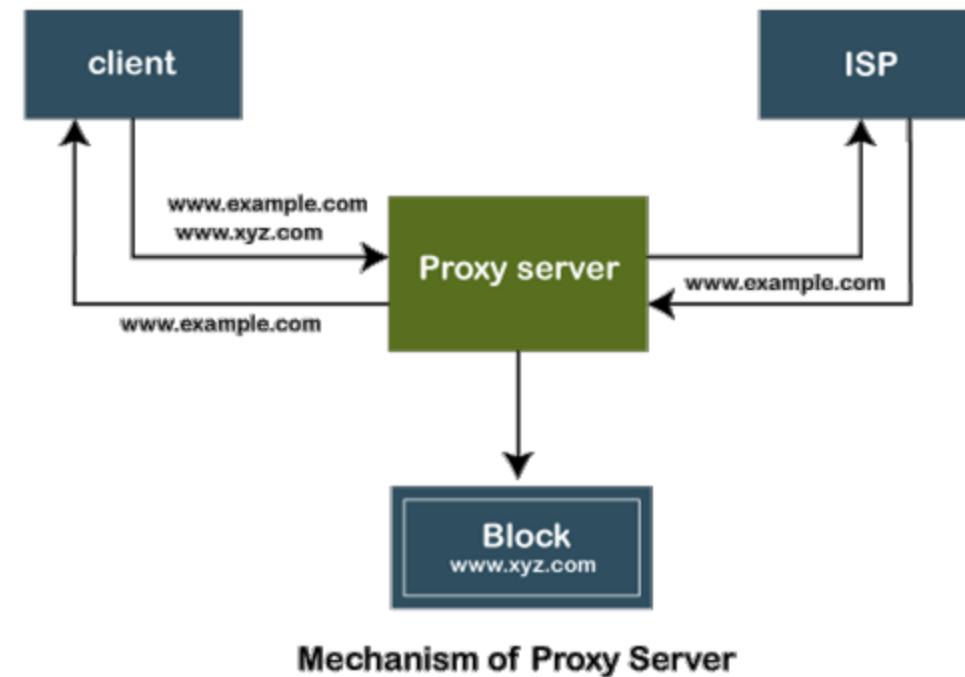
PPTP generates a tunnel and quarantines the data packet. PPTP is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also

used on Mac and Linux apart from Windows.

❖ **Proxy Server:**

- Every computer that is connected to the network has an IP address that identifies the device uniquely. Similarly, the **proxy server** is a computer on the network that has its own IP address. But sometimes, we want to access those websites or servers that are restricted and we do not want to show our identity (IP address). In such a scenario, the **proxy server** comes into existence. We can achieve the same by using the **proxy server**.
- The **proxy server** is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server. It works as a gateway between the end-user and the internet. It has its own IP address. It separates the client system and web server from the global network.
- In other words, we can say that the proxy server allows us to access any websites with a different IP address. It plays an intermediary role between users and targeted websites or servers. It collects and provides information related to user

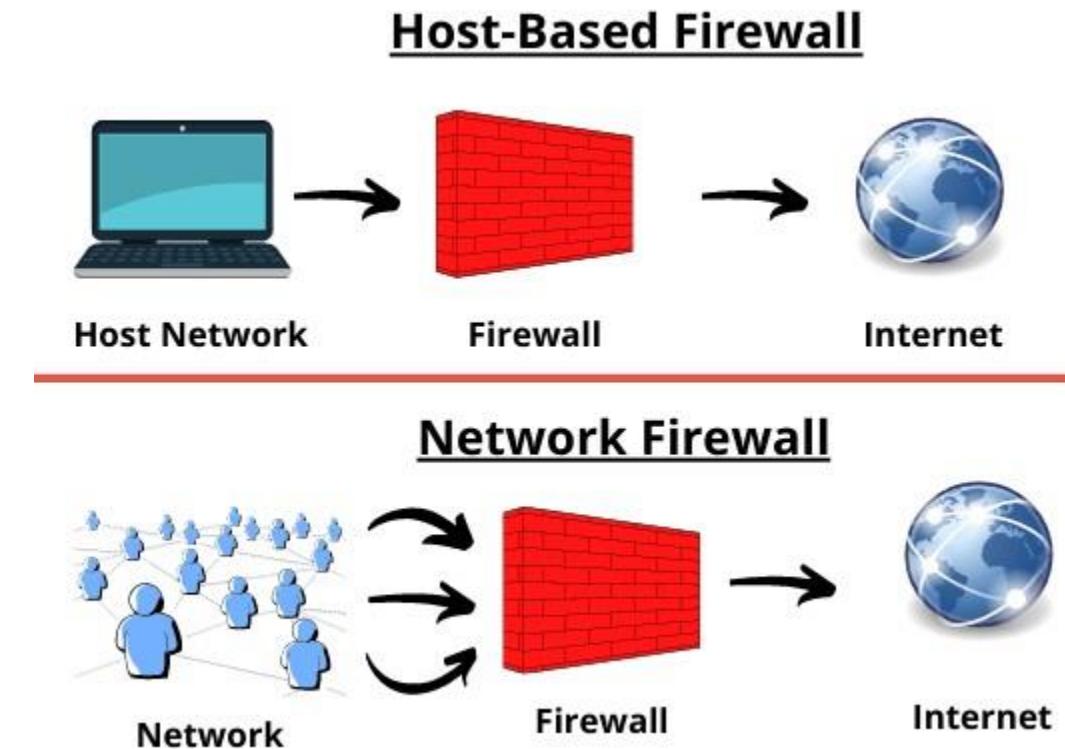
- There are two main purposes of proxy server:
- To keep the system behind it anonymous.
- To speed up access to a resource through caching.



❖ Firewall:

- A firewall is a network security device, either hardware or software-based.
- Firewall monitors all incoming and outgoing traffic (of Data Packets) and based on a defined set of security rules (Protocols) it accepts, rejects or drops that specific traffic (Data Packets).
- **Accept** : allow the traffic
Reject : block the traffic but reply with an “unreachable error”
Drop : block the traffic with no reply
- A firewall establishes a barrier between secured internal networks and outside unsecure or untrusted network, such as the Internet.
- Firewall not only provide security from outsiders but also monitors which type of packets are going outside of the particular computer or network. It means firewall can also block the access of such untrusted or unsecure and restricted IP.
- We can also set a rule in firewall for not having access to some potentially

- **For Ex:** Firewall acts as gatekeeper or security guard that is always stayed at our door step to protect us from the visit of unknown and unauthorized persons to whom we have some security threats. The guard allows to enter the persons only who are mentioned in the list of those who are potentially safe for us.
- Firewall can be a software or hardware or a firmware. Firewall can be implemented in individual host or entire network.
- Generally firewall acts a software in almost all genuine operating system now a days. It can be implemented as a hardware or firmware before the router to protect entire network for additional security.

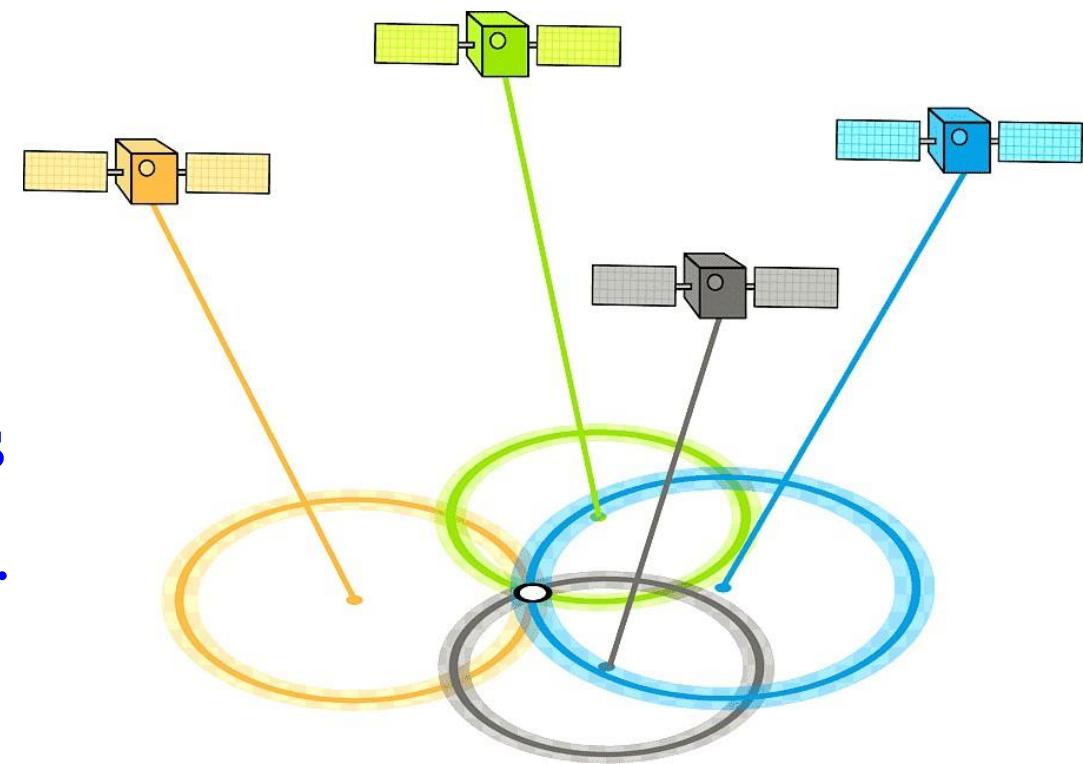


❖ GPS (Global Positioning System):

- The GPS (Global Positioning System) is a group of 31 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to locate or identify their geographic location.
- The location accuracy is anywhere from 100 to 10 meters for most equipment and within one meter with special military-approved equipment. GPS equipment is widely used in science and has now become sufficiently low-cost so that almost anyone can own a GPS receiver.
- The GPS was owned and operated by the U.S. Department of Defense but now is available worldwide.
- Each four satellites orbiting at 13,000 miles (20,000 km) above Earth and traveling at a speed of 8,700 mph (14,000 km/h).
- While we only need three satellites to produce a location on earth's surface, a fourth satellite is often used to validate the information from the other three. The

□ How GPS Works?

- GPS works through a technique called trilateration. Used to calculate location, velocity and elevation, trilateration collects signals from satellites to output location information.
- Once the receiver receives the signal from at least three satellites, the receiver then points its location using trilateration process. A GPS requires at least 3 satellites to calculate 2-D position(latitude and longitude on a map). In this case, the GPS receiver assumes that it is located at mean sea level. However, it requires at least 4 satellites to find receivers 3-D position(latitude, longitude, and altitude).



❖ GPRS (General Packet Radio Service):

- ❑ GPRS stands for General Packet Radio Service. It is a packet oriented wireless data communication service for mobile communications on 2G and 3G cellular communication systems. It is non-voice, high speed packet switching technology intended for GSM networks.
- ❑ To enable GPRS on a GSM or TDMA network, we are required to add two core modules: the Gateway GPRS Service Node (GGSN) and the Serving GPRS Service Node (SGSN).
- ❑ GPRS can be used to provide connections on the basis of internet protocols that support a wide variety of enterprises as well as commercial applications.

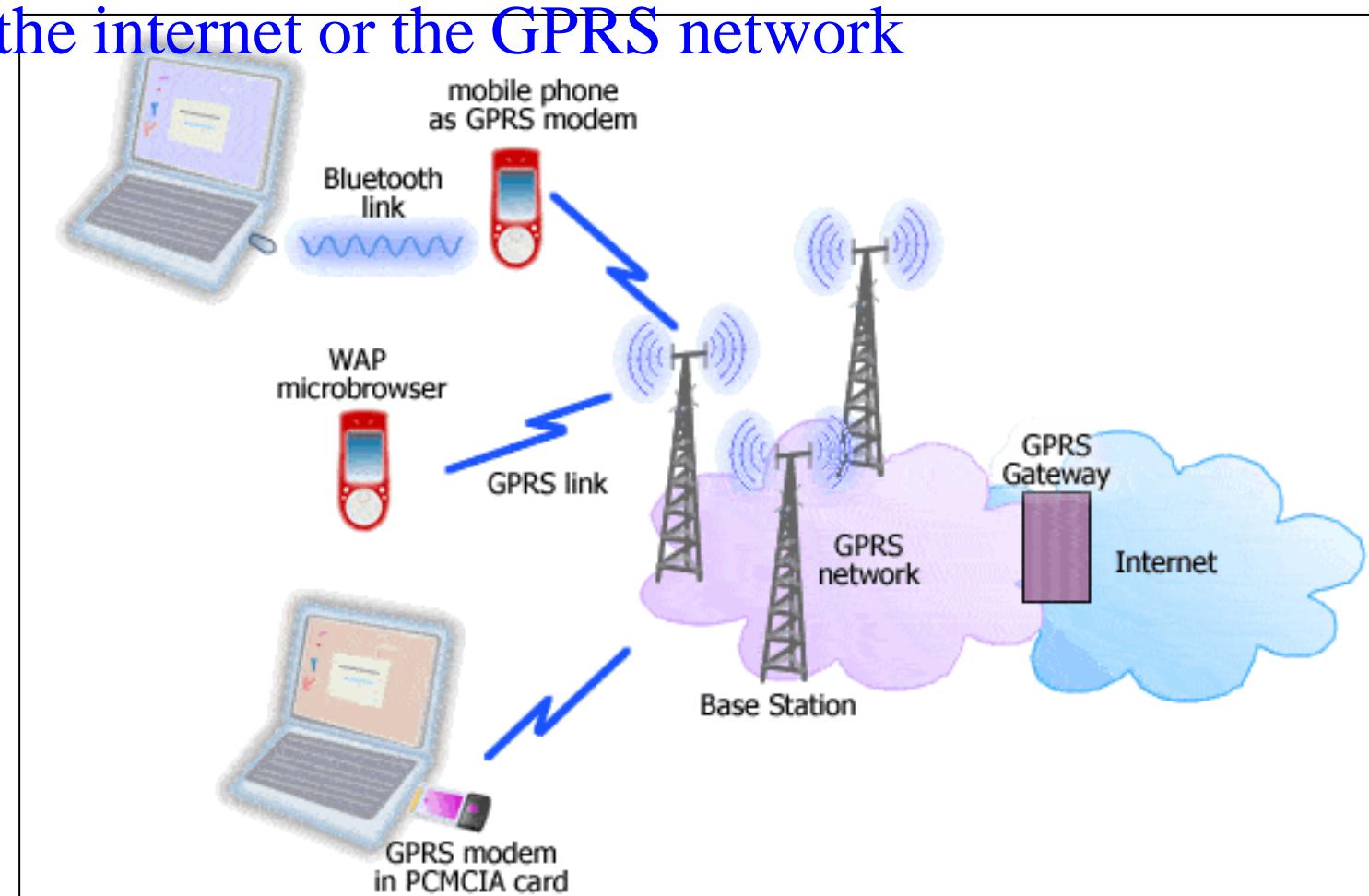
❑ Benefits of GPRS:

- ❑ It provides higher data transfer speed than fixed telecommunication networks. Its optimum speed is 171.2 kbps. Three time quicker than fixed-telecommunication.
- ❑ It provides instant connection and immediate data transfer.

❑ What is needed to use GPRS?

- ❑ An application with a GPRS modem
- ❑ A GSM/GPRS network
- ❑ A SIM card with GPRS service
- ❑ A remote station with access to the internet or the GPRS network

❑ GPRS is considered as 2.5G technology because it is more advanced than standard 2G digital technology, but does not meet the requirements of 3G technology.



❖ CCTV (Closed-Circuit Television) Technology:

- CCTV (closed-circuit television) is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.
- “Closed-circuit” means broadcasts are usually transmitted to a limited (closed) number of monitors, unlike “regular” TV, which is broadcast to the public at large. CCTV networks are commonly used to detect and prevent criminal activities, and record traffic violations, but they have other uses also.
- CCTV technology was first developed in 1942 by German scientists Walter Bruch to monitor the launch of V2 rockets. It was later used by American scientists during the testing of the atomic bomb.
- CCTV works by the cameras taking a constant sequence of images that are then transmitted by cable or wirelessly to the recording device and then on to the display monitor, which enables an individual to see the sequence of images as video footage.

Assignments:

- 1) What is Internet? How Internet is connect with Computer?
- 2) Explain Technologies related to the Internet.
- 3) What is VPN? Explain types and uses of VPN.
- 4) Explain available three protocols of VPN.
- 5) What is Proxy Server? How it is differ from Firewall?
- 6) Explain in details GPS and GPRS.
- 7) Describe CCTV Technology.
- 8) Differentiate VPN and Firewall.
- 9) Differentiate ISDN and Dial-up Connection.