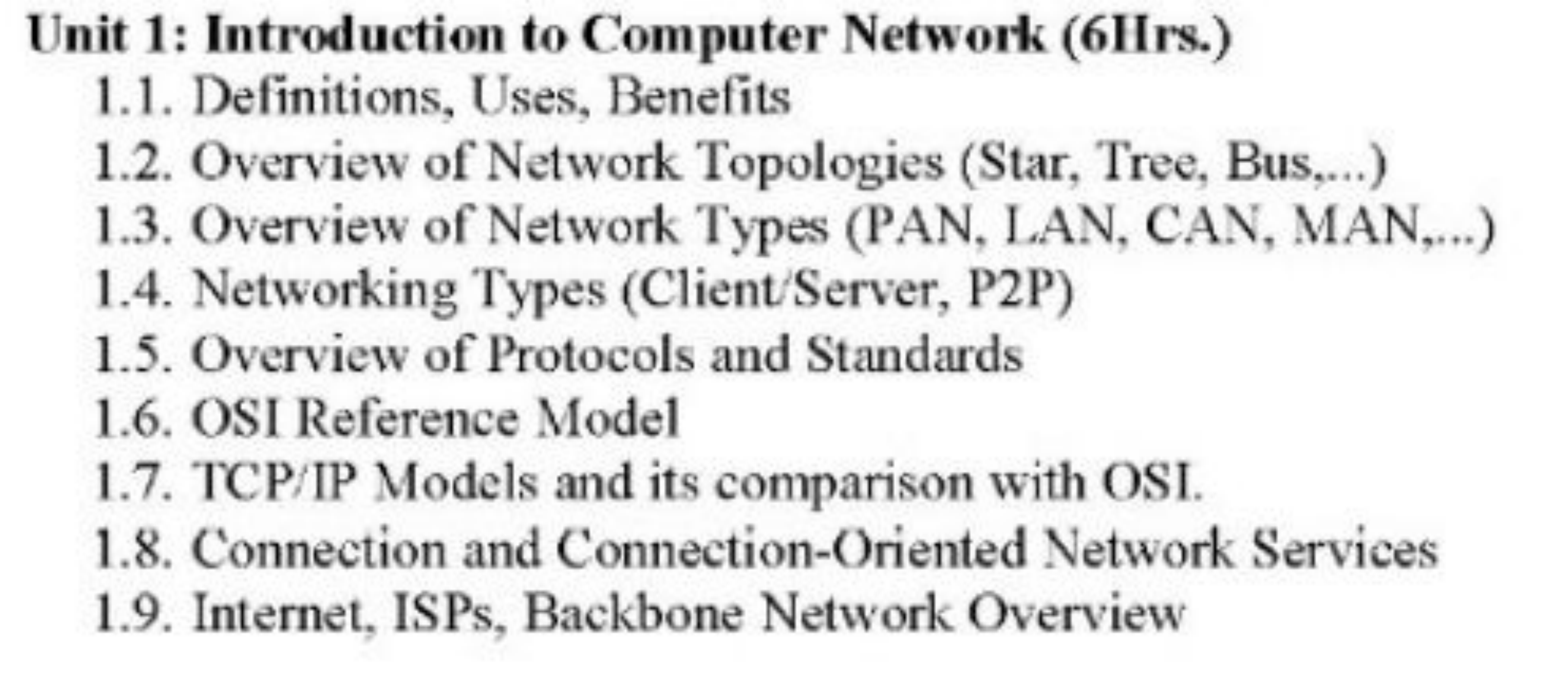
CHAPTER 1: INTRODUCTION TO COMPUTER NETWORK

ANKU JAISWAL(ASSISTANT PROFESSOR, IOE, PULCHOWK CAMPUS)

TOPIC CONTENT

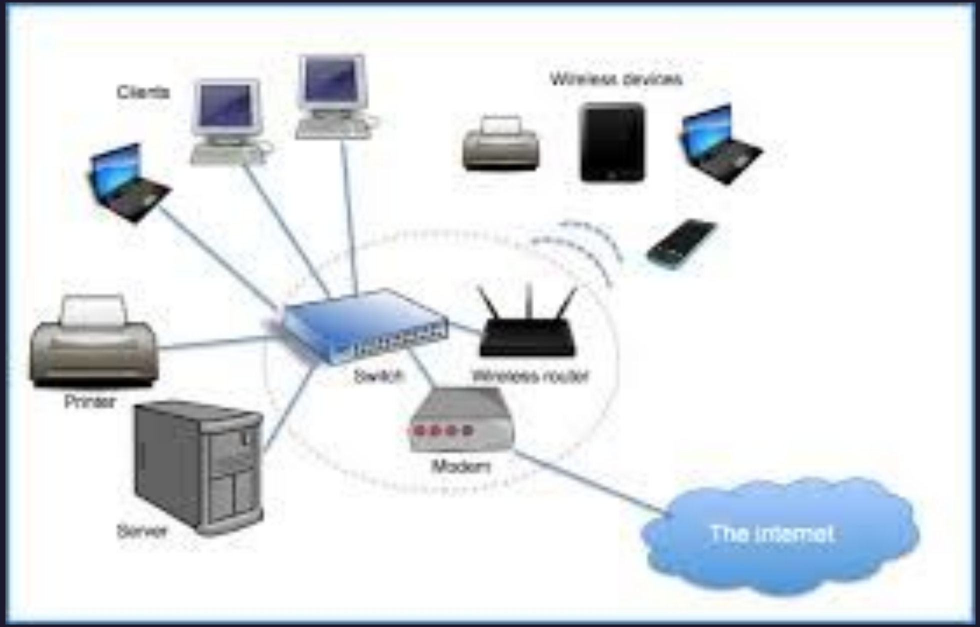


Unit 1: Introduction to Computer Network (6Hrs.)

1.1. Definitions, Uses, Benefits
1.2. Overview of Network Topologies (Star, Tree, Bus,...)
1.3. Overview of Network Types (PAN, LAN, CAN, MAN,...)
1.4. Networking Types (Client/Server, P2P)
1.5. Overview of Protocols and Standards
1.6. OSI Reference Model
1.7. TCP/IP Models and its comparison with OSI.
1.8. Connection and Connection-Oriented Network Services
1.9. Internet, ISPs, Backbone Network Overview

DEFINITIONS, USES, BENEFITS

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



USES

- Facilitate communication via email, video conferencing, instant messaging, etc.
- Enable multiple users to share a single hardware device like a printer or scanner
- Enable file sharing across the network
- Allow for the sharing of software or operating programs on remote systems
- Make information easier to access and maintain among network users

Benefits

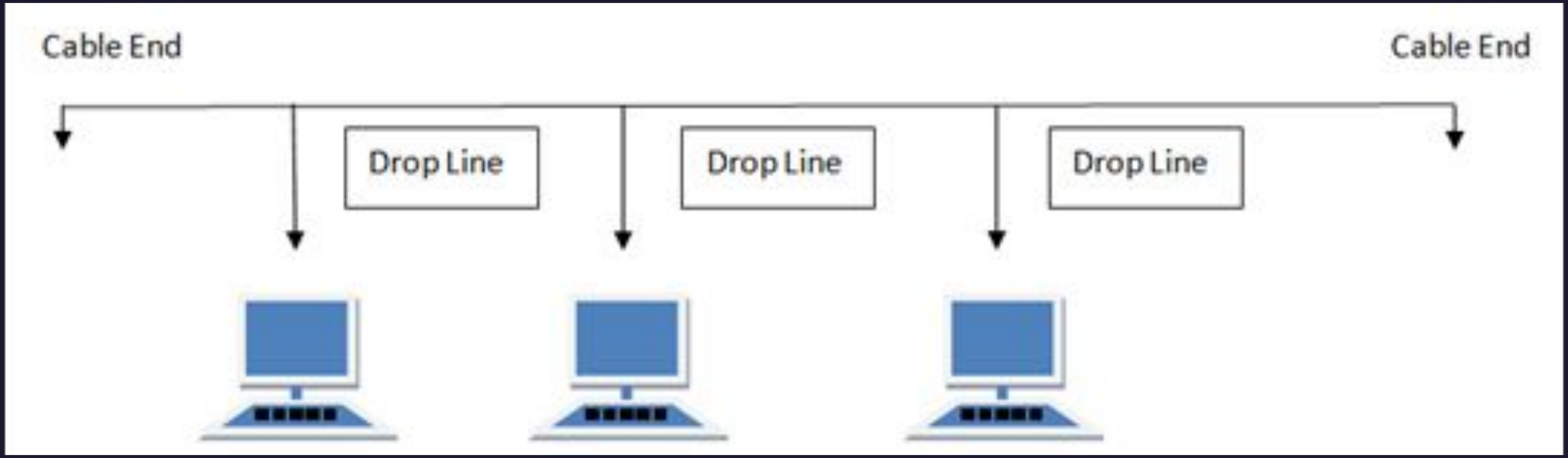
- Resource sharing.
- For providing high reliability.
- To save money.
- It can provide a powerful communication medium.
- Access to remote information
- Person to person communication
- Interactive entertainment.

OVERVIEW OF NETWORK TOPOLOGIES MESH, STAR, TREE, BUS

- Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.



Features of Bus Topology

- It transmits data only in one direction.
- Every device is connected to a single cable

Advantages of Bus Topology

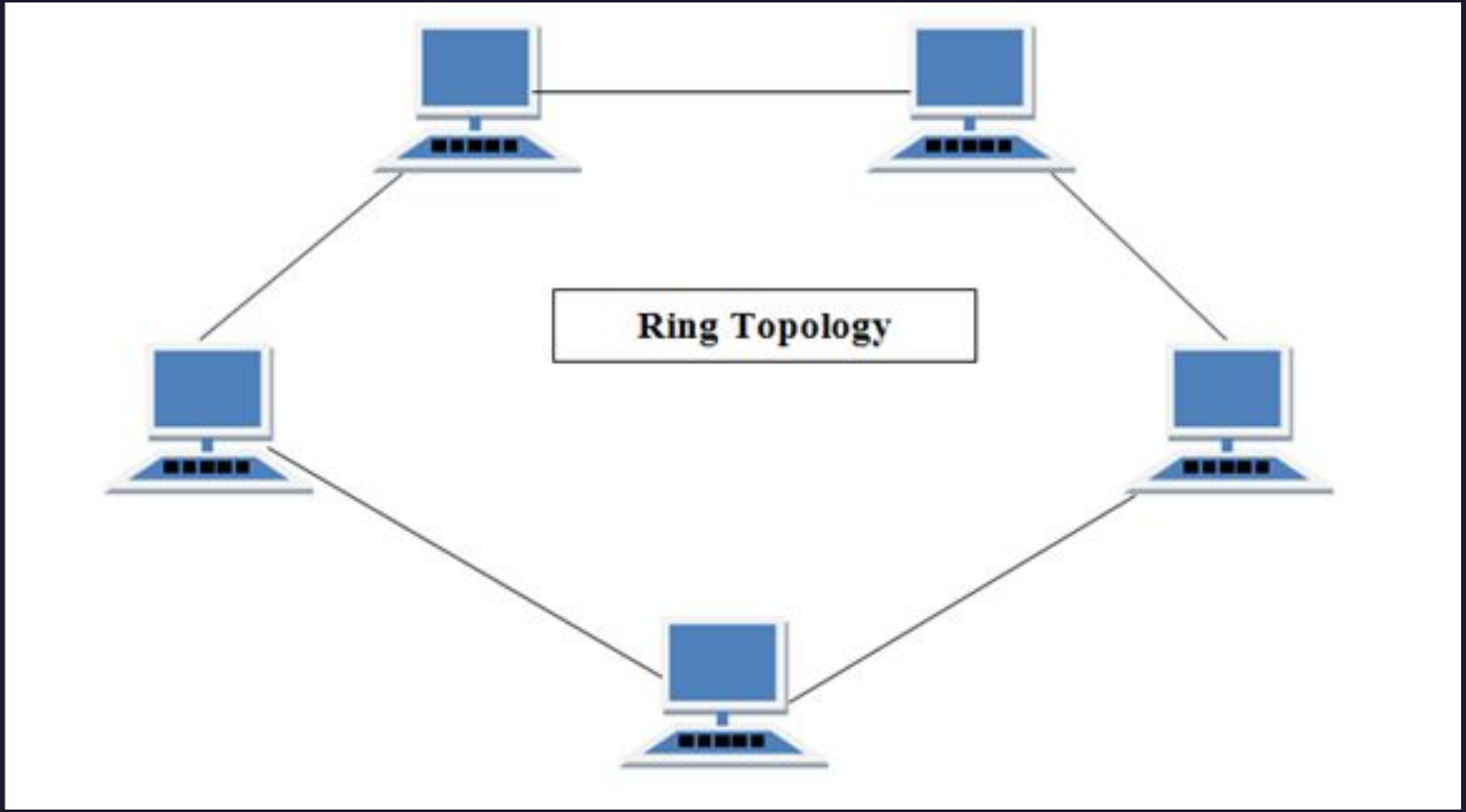
- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

RING Topology

- It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.



Features of Ring Topology

- A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

- The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

- In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.

- Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

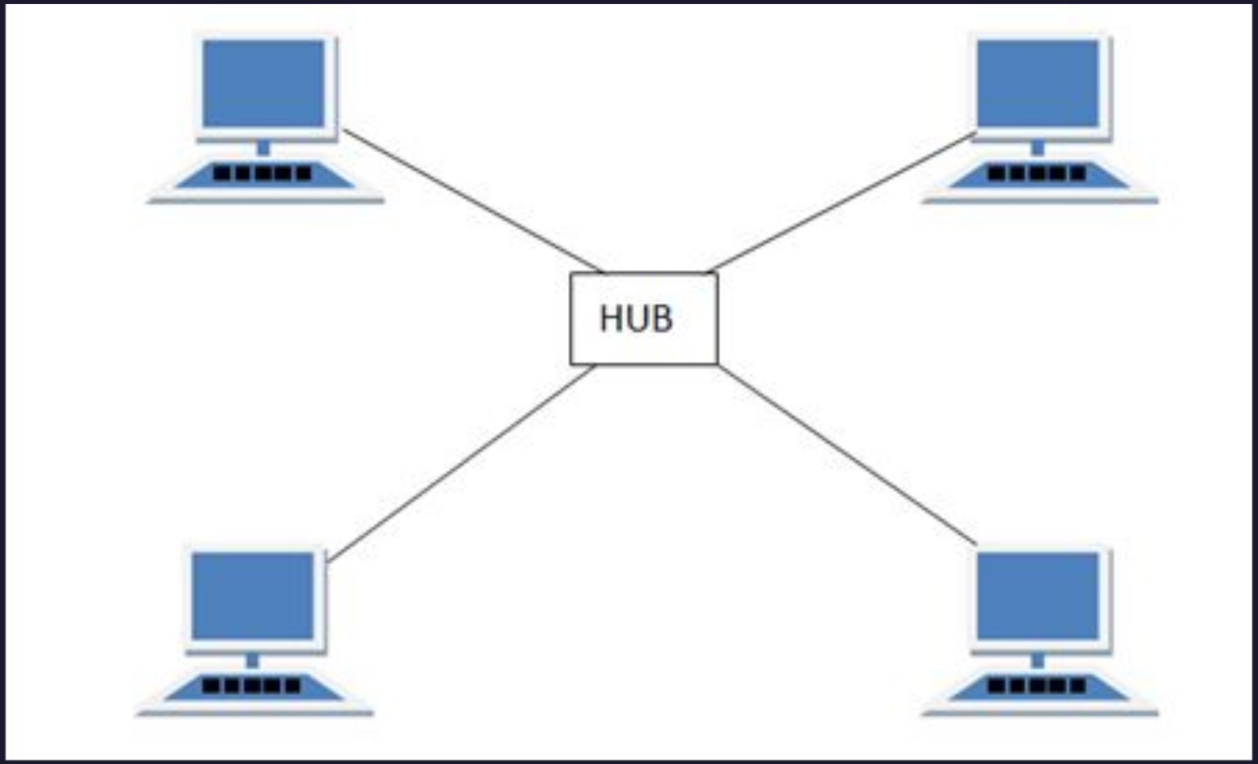
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand

Disadvantages of Ring Topology

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

STAR Topology

- In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

- Every node has its own dedicated connection to the hub.
- Hub acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

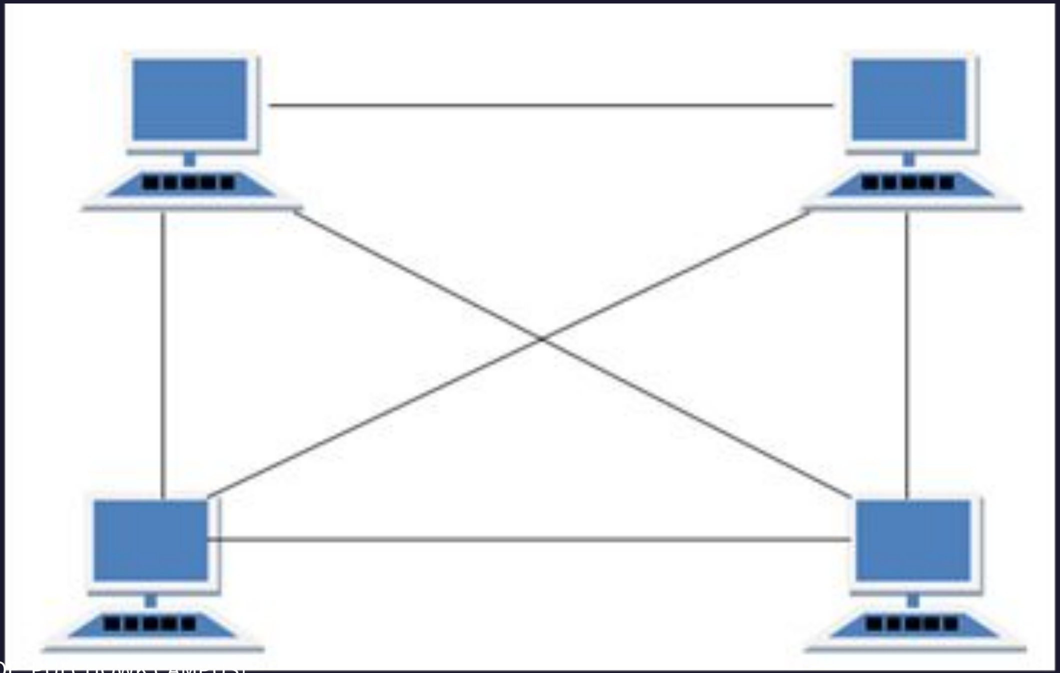
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity

MESH Topology

- It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.
- There are two techniques to transmit data over the Mesh topology, they are :
- Routing
- Flooding



Features of Mesh Topology

- Fully connected.
- Robust.
- Not flexible.

Advantages of Mesh Topology

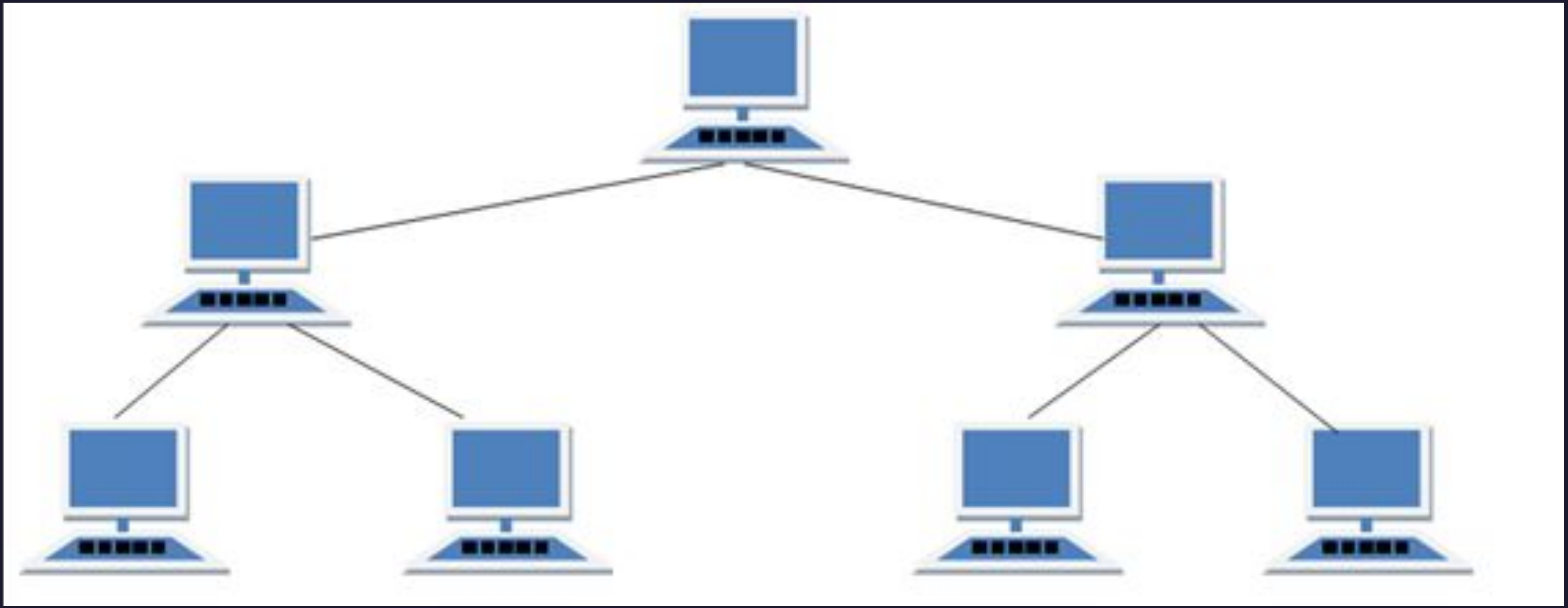
- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages of Mesh Topology

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

TREE Topology

- It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

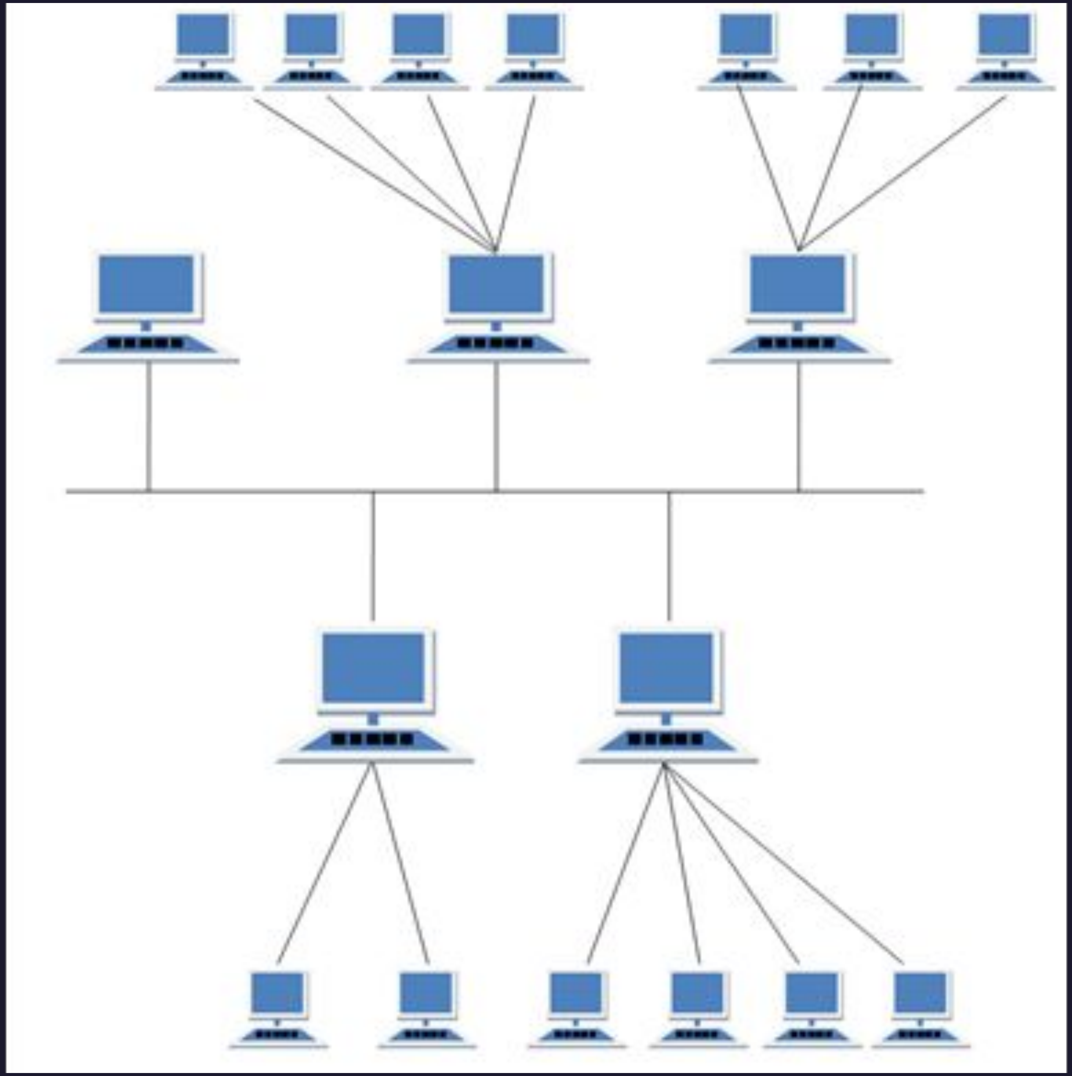
- Ideal if workstations are located in groups.
- Used in Wide Area Network.

Advantages of Tree Topology

- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages of Tree Topology

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails, network fails.



HYBRID Topology

- It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

Features of Hybrid Topology

- It is a combination of two or topologies
- Inherits the advantages and disadvantages of the topologies included

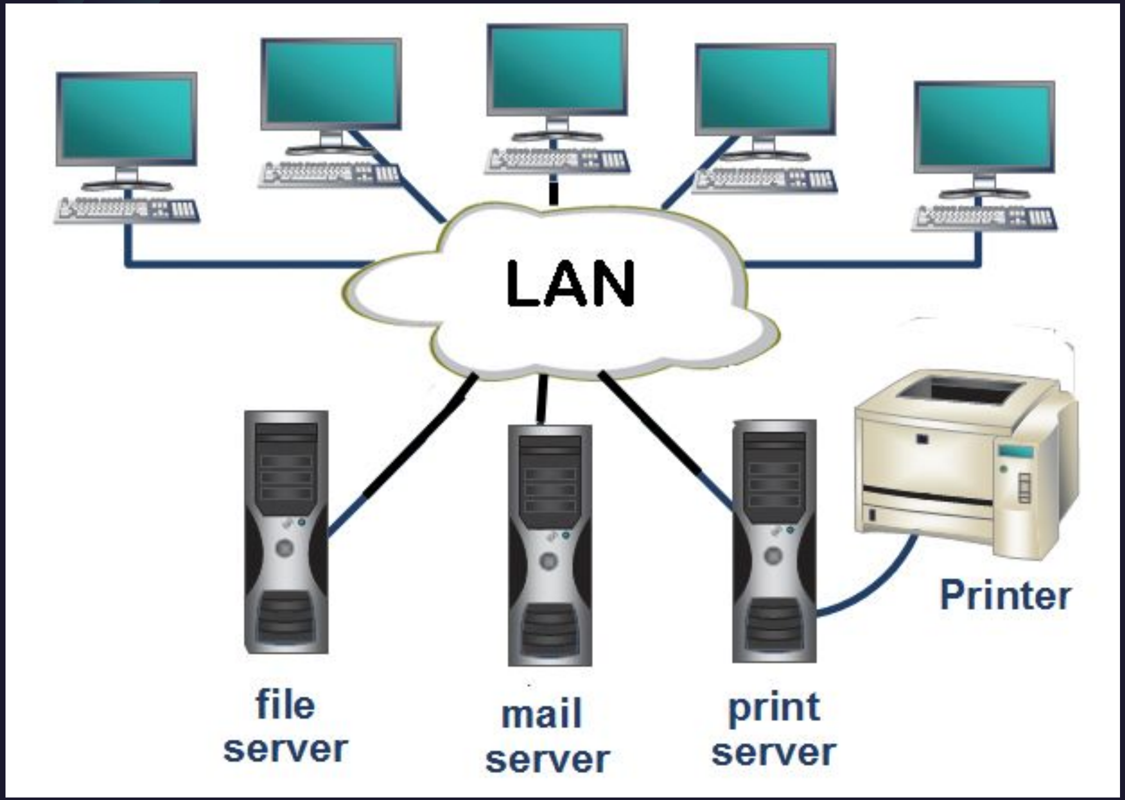
Advantages of Hybrid Topology

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

OVERVIEW OF NETWORK TYPES LAN, PAN, CAN, MAN, WAN



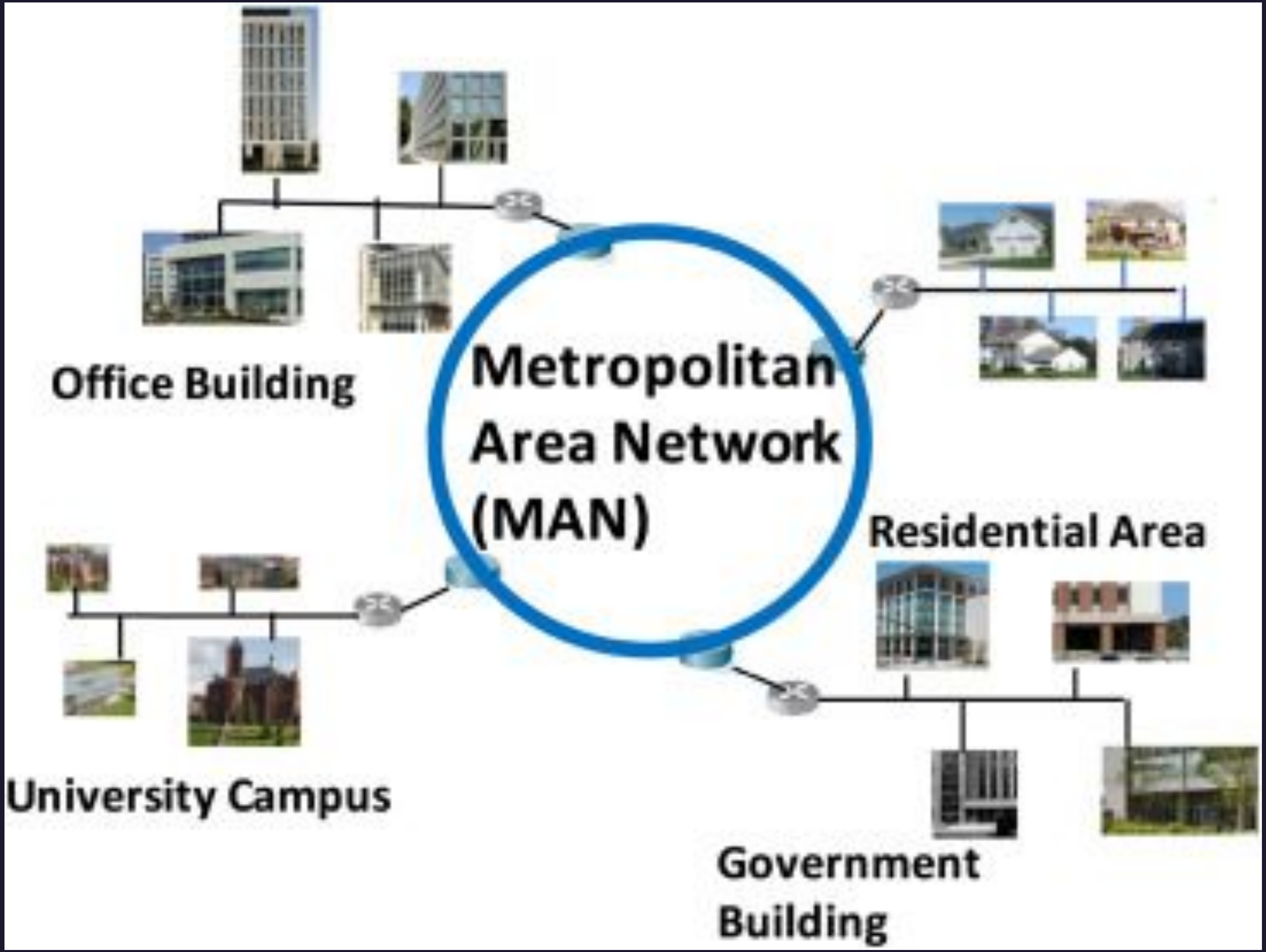
LAN

- A local-area network (LAN) is a computer network that spans a relatively small area.
- Most often, a LAN is confined to a single room, building or group of buildings;
- however, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

- This is the abbreviation for Local Area Network which is when there are multiple computers and peripheral devices connected to a campus or in an office or other room.
- They are sharing a common connection that has 10-100 Mbps data transmission speed and are connected by Ethernet cables, usually running on high-speed internet connection.
- LAN computer terminals may be physically connected using cables or setup wireless, thus called WLAN.
- LAN is less expensive than WAN or MAN.

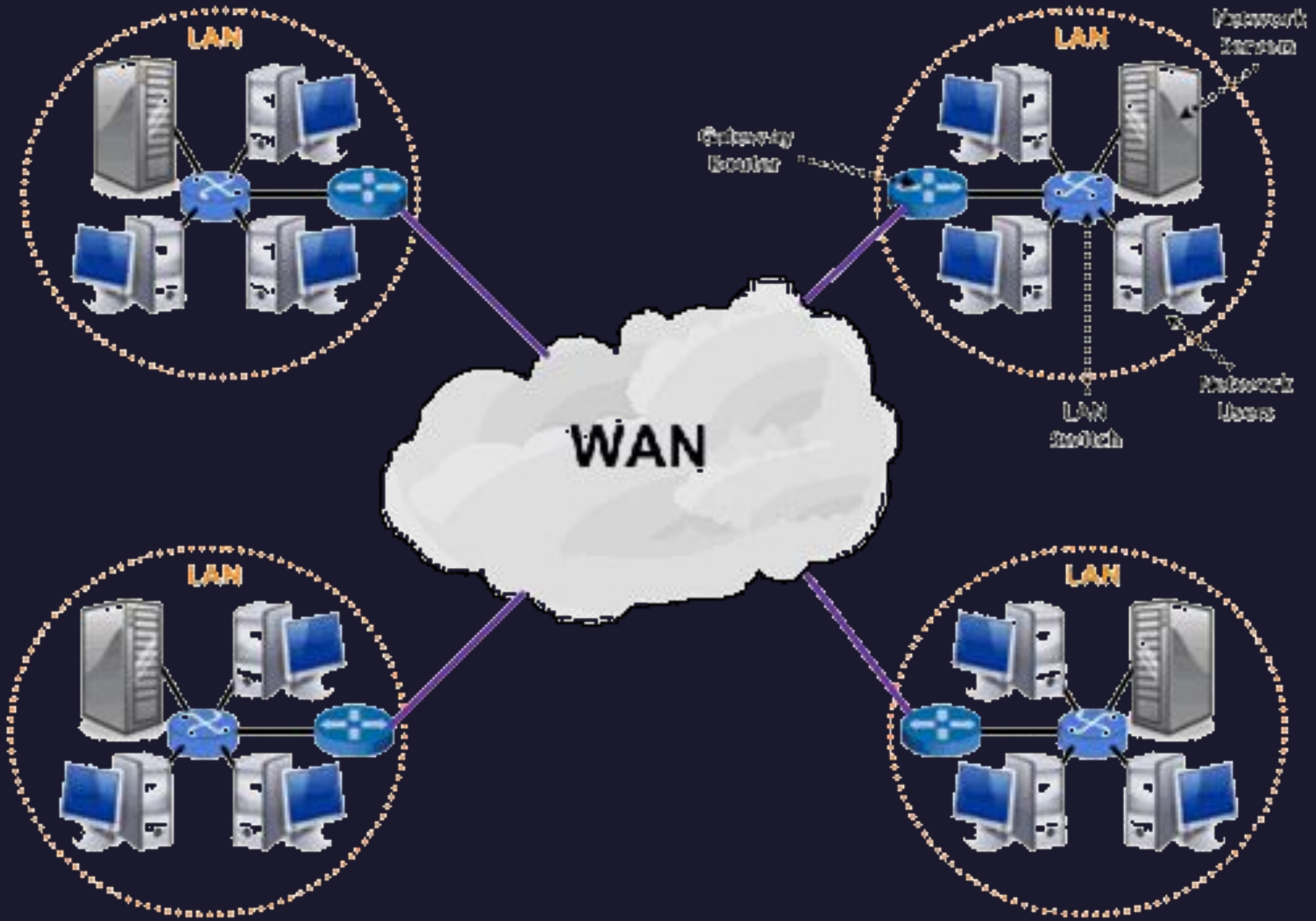
MAN

- MAN is the abbreviation for Metropolitan Area Network and bigger than LAN network.
- It connects computer users that are in a specific geographical area.
- An example of MAN is a large university.
- MAN’s data transmission speed is 5-10Mbps, which is faster and more expensive than LAN but slower and smaller than WAN.


Office Building
Metropolitan Area Network (MAN)
Residential Area
University Campus
Government Building

WAN

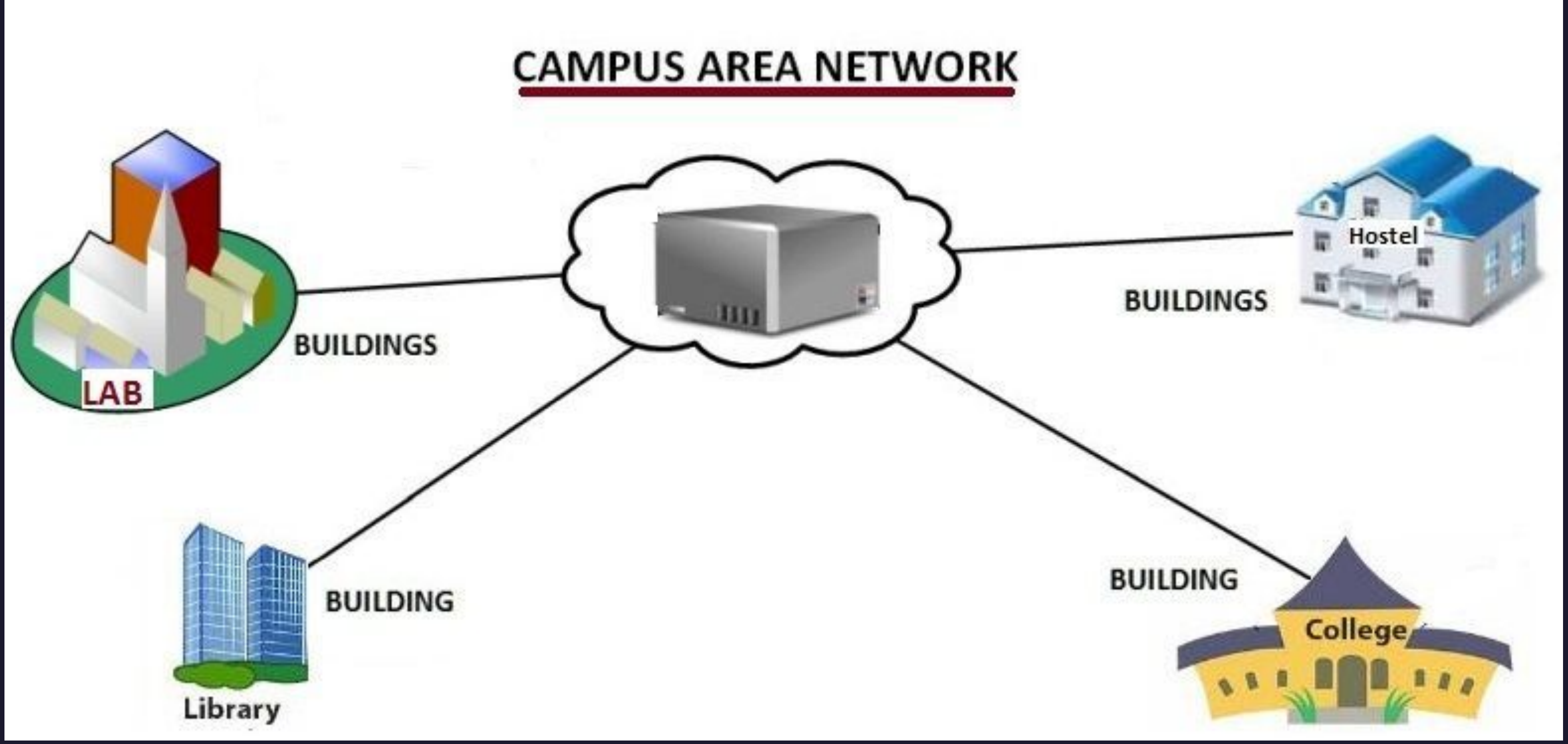
- A WAN connects more than one LAN and is used for larger geographical areas.
- WANs are similar to a banking system, where hundreds of branches in different cities are connected with each other in order to share their official data.
- A WAN works in a similar fashion to a LAN, just on a larger scale.
- TCP/IP is the protocol used for a WAN in combination with devices such as routers, switches, firewalls and modems.


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

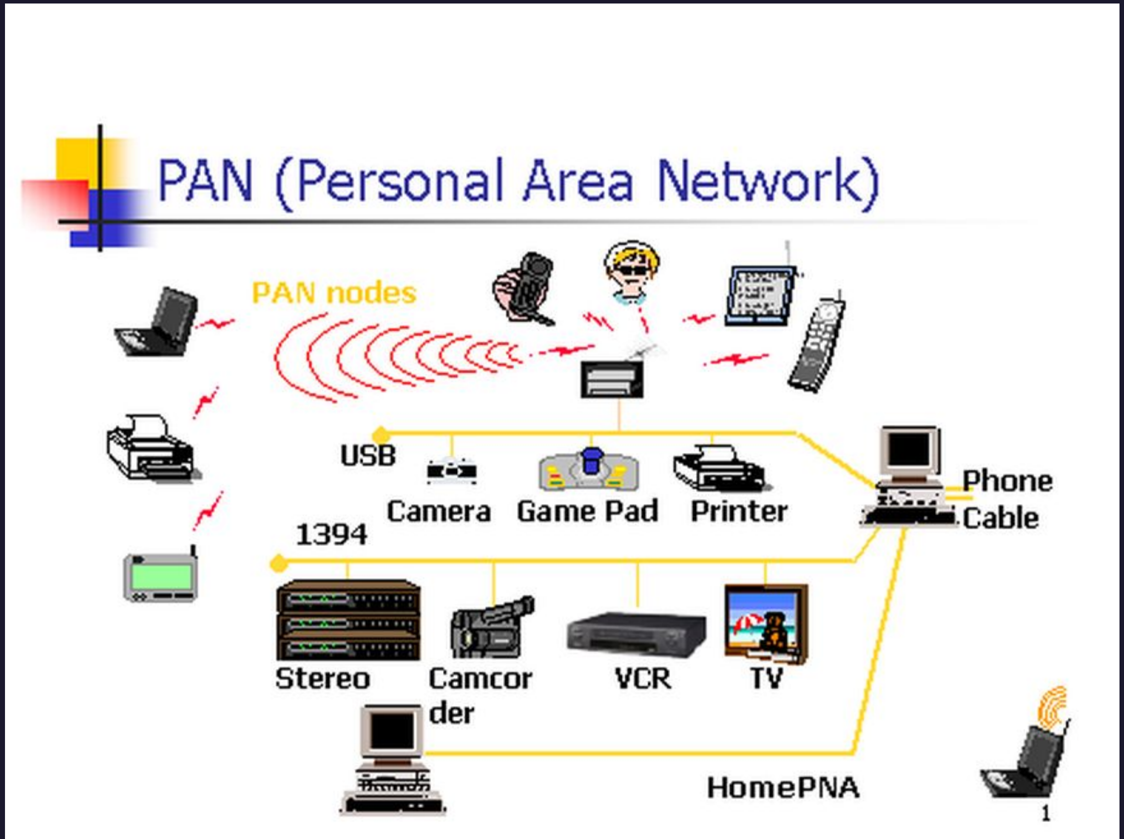
- This is the abbreviation forWide Area Network and is the biggest network which can interconnect networks around the world.
- Companies such as Microsoft or other worldwide organizations utilize WAN connection between their various branches by communicating via microwave satellites.
- WAN has a data transmission speed of 256Kbps to 2Mbps, offering a faster speed than LAN or MAN.
- WAN is used to connect LANs that are not in the same area and is more expensive than LAN or MAN.

CAN

- Stands for "**Campus Area Network**."
- A **CAN** is a **network** that covers an educational or corporate campus.
- **Examples** include elementary schools, university campuses, and corporate buildings.
- A **campus area network** is larger than a local area **network** LAN since it may span multiple buildings within a specific area.
- **Example** of the **CAN** is the **networking** between school, library and hostel. School management **can** access to library and hostel
- For **example**, the campus **network can** used for an office or industrial park, in a public place like a supermarket with an entertainment center, even on a farm.
- CAN has a data transmission speed of 40Kbps to 1Mbps,


CAMPUS AREA NETWORK
LAB
BUILDINGS
Hostel
BUILDINGS
Library
BUILDING
BUILDING
College

- **PAN**
- A personal area network (PAN) is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters.
- For example, a person traveling with a laptop, a personal digital assistant (PDA), and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology.
- Typically, this kind of personal area network could also be interconnected without wires to the Internet or other networks.

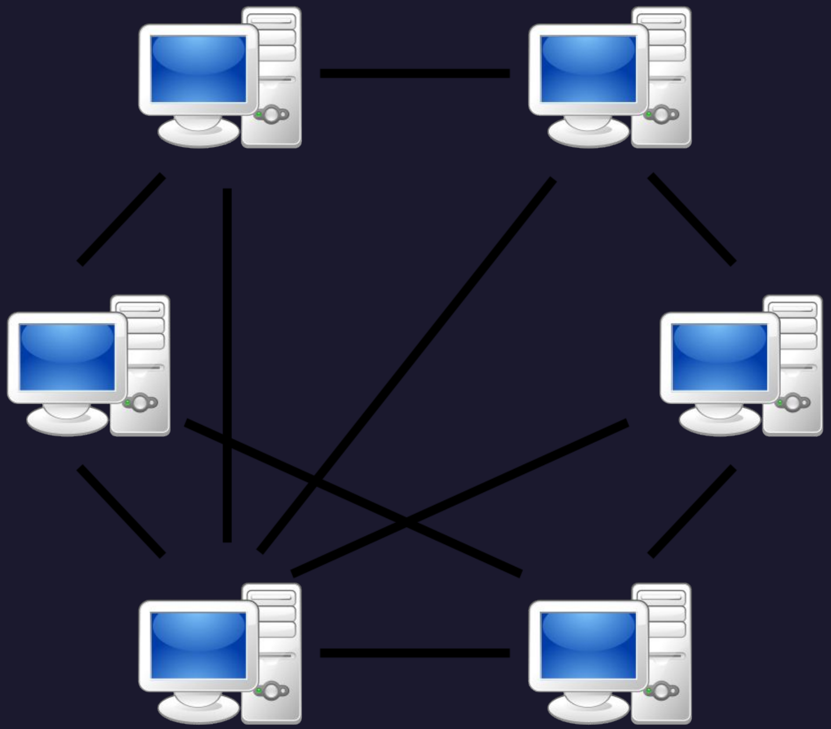


PAN (Personal Area Network)

NETWORKING TYPES

P2P model

- Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session.
- Unlike the client/server model, in which the client makes a service request and the server fulfills the request, the P2P network model allows each node to function as both a client and server.
- In its simplest form, a peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server computer.
- Most P2P programs are focused on media sharing.



The different characteristics of peer to peer networks are as follows:

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

Some advantages of peer to peer computing are as follows:

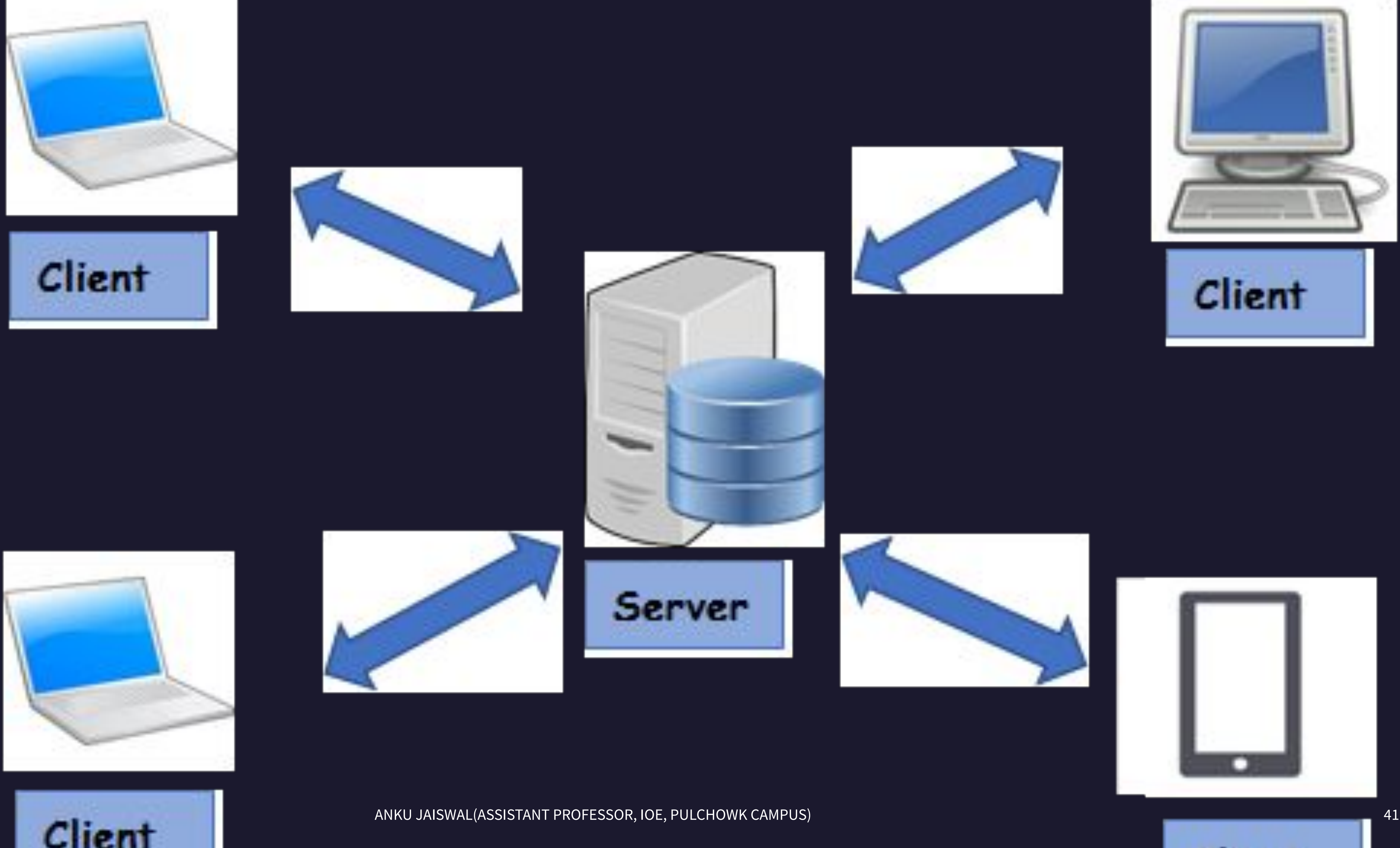
- Each computer in the peer to peer network manages itself. So, the network is quite easy to set up and maintain.
- In the client server network, the server handles all the requests of the clients. This provision is not required in peer to peer computing and the cost of the server is saved.
- It is easy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

Some disadvantages of peer to peer computing are as follows:

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

Client-Server Model

- Client-server architecture (client/server) is a network architecture in which each computer or process on the network is either a *client* or a *server*.
- Servers are powerful computers or processes dedicated to managing disk drives (*file servers*), printers (*print servers*), or network traffic (network servers).
- Clients are PCs or workstations on which users run applications.
- Clients rely on servers for resources, such as files, devices, and even processing power.


Client
Client
Server
Client

The salient points for client server computing are as follows:

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

The different advantages of client server computing are:

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

The different disadvantages of client server computing are:

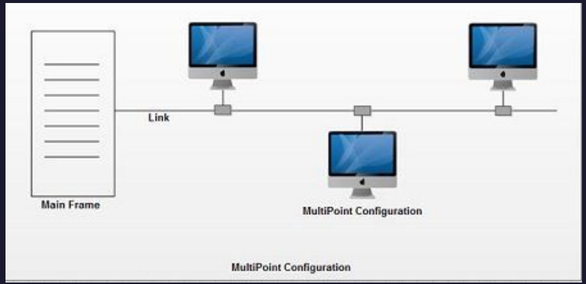
- If all the clients simultaneously request data from the server, it may get overloaded. This may lead to congestion in the network.
- If the server fails for any reason, then none of the requests of the clients can be fulfilled. This leads of failure of the client server network.
- The cost of setting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

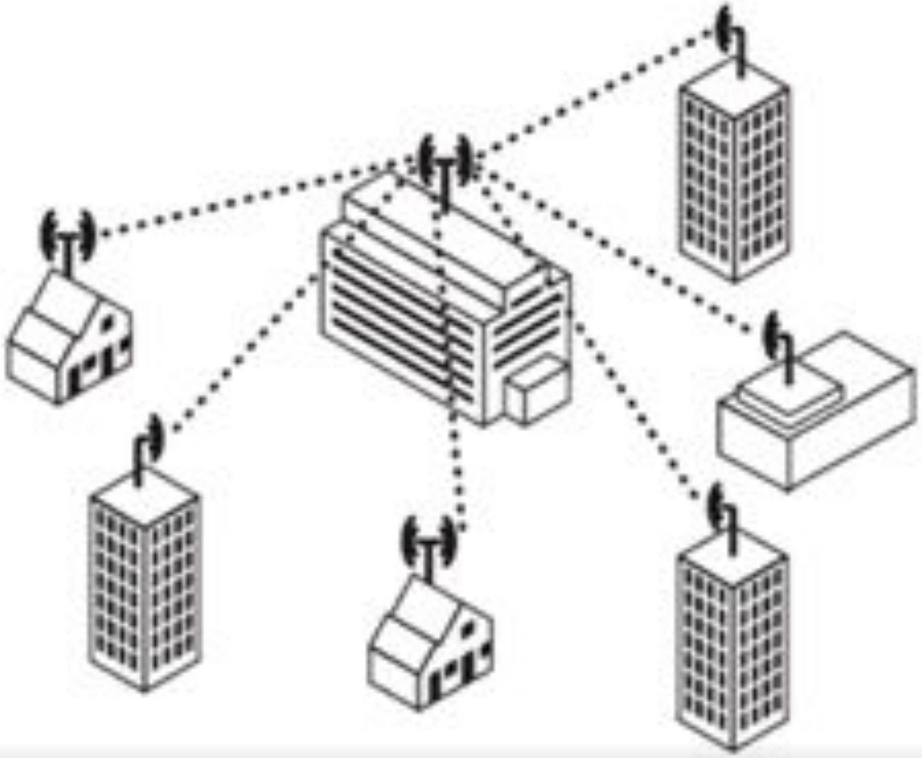
The major differences between client server computing and peer to peer computing are as follows:

- In client server computing, a server is a central node that services many client nodes. On the other hand, in a peer to peer system, the nodes collectively use their resources and communicate with each other.
- In client server computing the server is the one that communicates with the other nodes. In peer to peer to computing, all the nodes are equal and share data with each other directly.
- Client Server computing is believed to be a subcategory of the peer to peer computing.

Multipoint Model

- More than two specific devices share a single link. Multipoint topology is based on “sharing”. In this type of topology, each node on a network has only one connection.
- Bus Topology is a common example of Multipoint Topology.





Instead of using point-to-point topology such as a mesh, LANs typically use a multipoint topology. The key to a multipoint topology can be summed up in a single word: sharing.

Instead of a separate connection and cable being connected to every other computer on a network, with a multipoint topology, each computer on the network has just one connection. This connection is attached to a single cable that is shared by all other devices on the network. All transmissions are sent and received across one cable.

OVERVIEW OF PROTOCOLS AND STANDARDS

Protocol: Syntax, Semantics, Timing

- Protocol is a set of rules that governs communication. The key elements of protocol are syntax, semantics and timing.
- **Syntax:**
  Syntax refers the structure and format of the information data.
- The term syntax refers to the structure or format of the data, meaning the order in which they are presented.
- For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

- **Semantics:**
  Semantics refers to the meaning of each section of bits.

- **It identify the route to be taken or the final destination of the message.**

- The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?

- **Timing:**
  Timing refers to two characteristics: when data should be sent and how fast it should be sent.
- The term timing refers to two characteristics: when data should be sent and how fast they can be sent.
- For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

- **Standards:** Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes.

- Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

- Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

- **De facto:** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

- **De jure:** Those standards that have been legislated by an officially recognized body are de jure standards.

Standards Organizations

- Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees

- While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

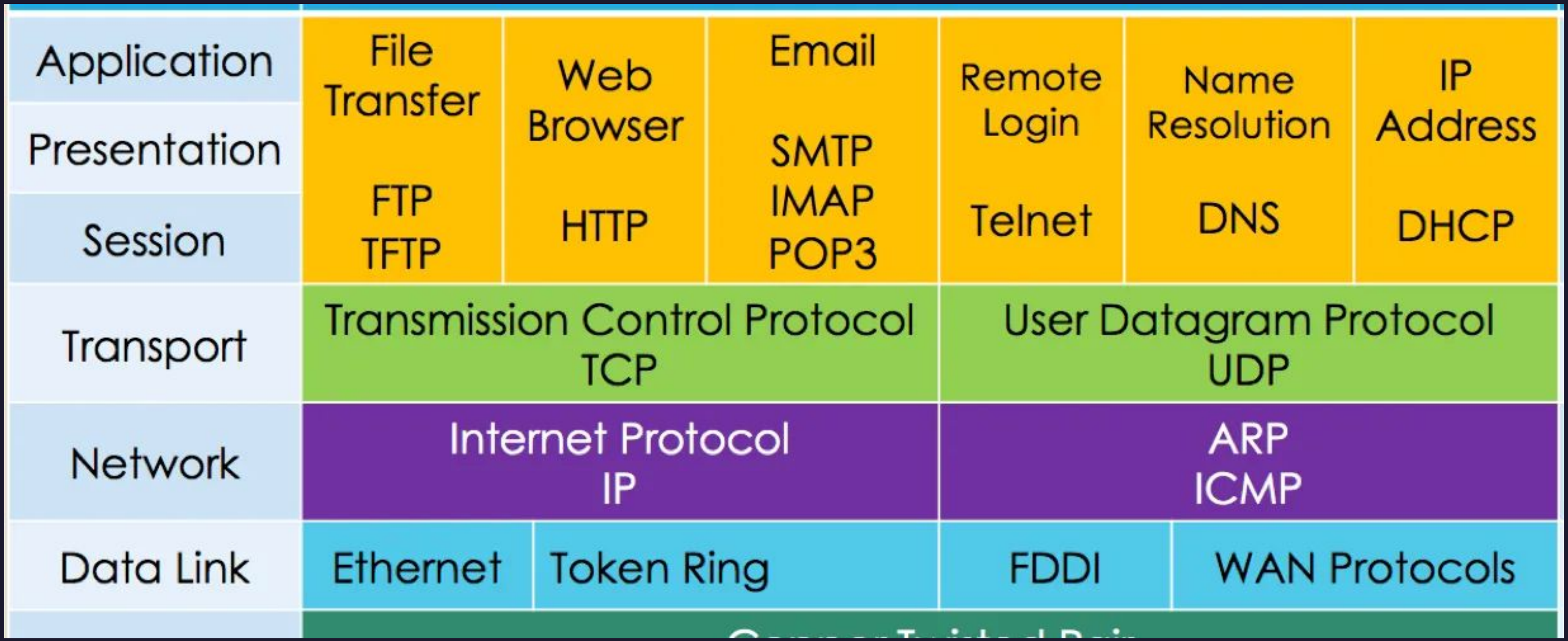
Some Standards

- International Standards Organization (ISO)
- makes standards for many different activities
- American National Standards Institute (ANSI)
- US representative to ISO
- Consultative Committee for International Telephony and Telegraphy (CCITT)
- one part of the UN agency International Telecommunications Union

- concerned with telephone and data communication services
- US representative is the State Department
- National Institute of Standards and Technology (NIST)
- standards body for US government purchases
- Institute of Electrical and Electronics Engineers (IEEE)
- key standards for LANs
- Internet Engineering Task Force (IETF)

Network Protocol

- A **network protocol** is an established set of rules that determine how data is transmitted between different devices in the same **network**.
- Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.

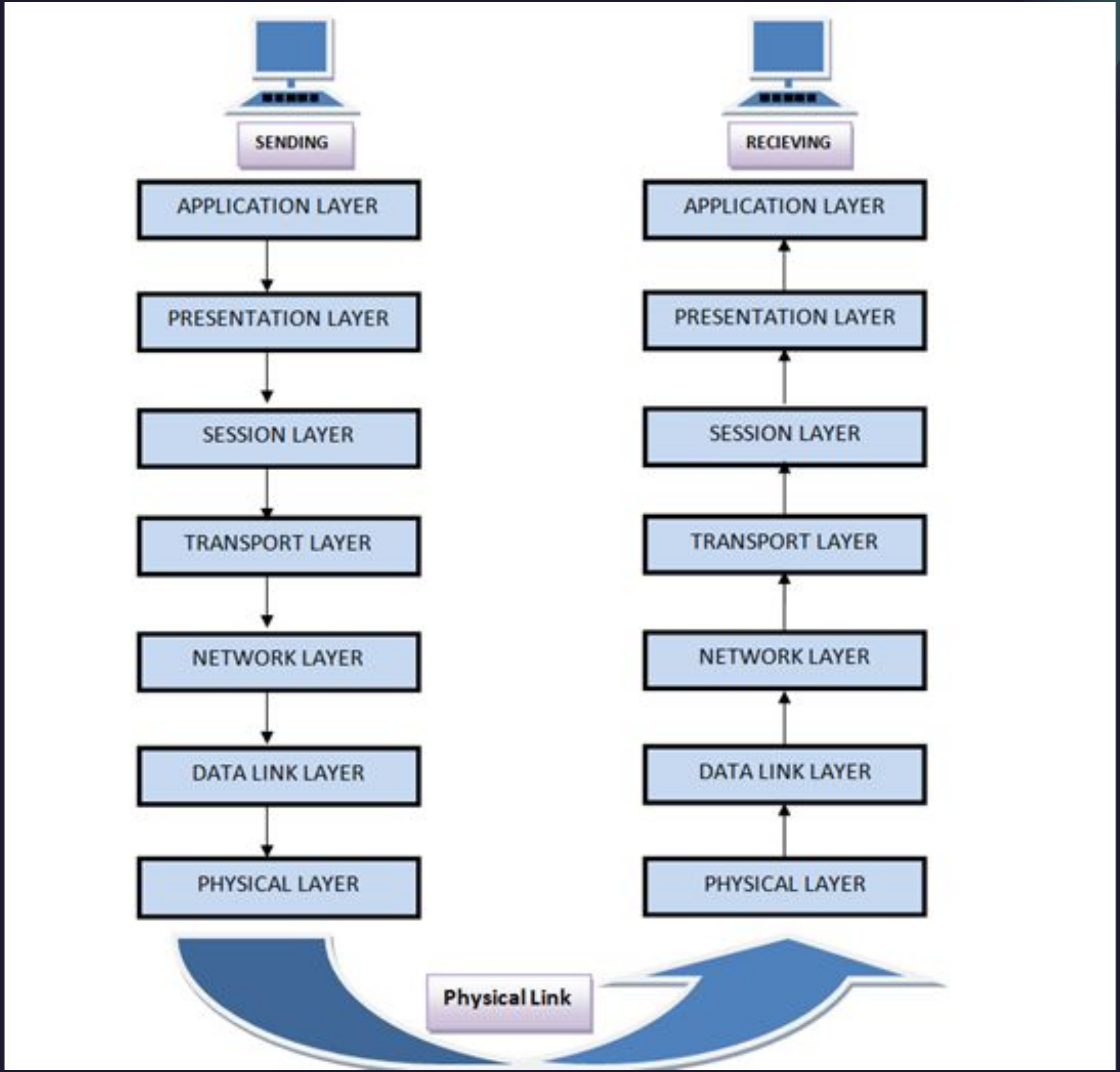


Application	File Transfer FTP TFTP	Web Browser HTTP	Email SMTP IMAP POP3	Remote Login Telnet	Name Resolution DNS	IP Address DHCP
Presentation						
Session						
Transport	Transmission Control Protocol TCP			User Datagram Protocol UDP		
Network	Internet Protocol IP			ARP ICMP		
Data Link	Ethernet	Token Ring		FDDI	WAN Protocols	
	Copper Twisted Pair					

OSI REFERENCE MODEL

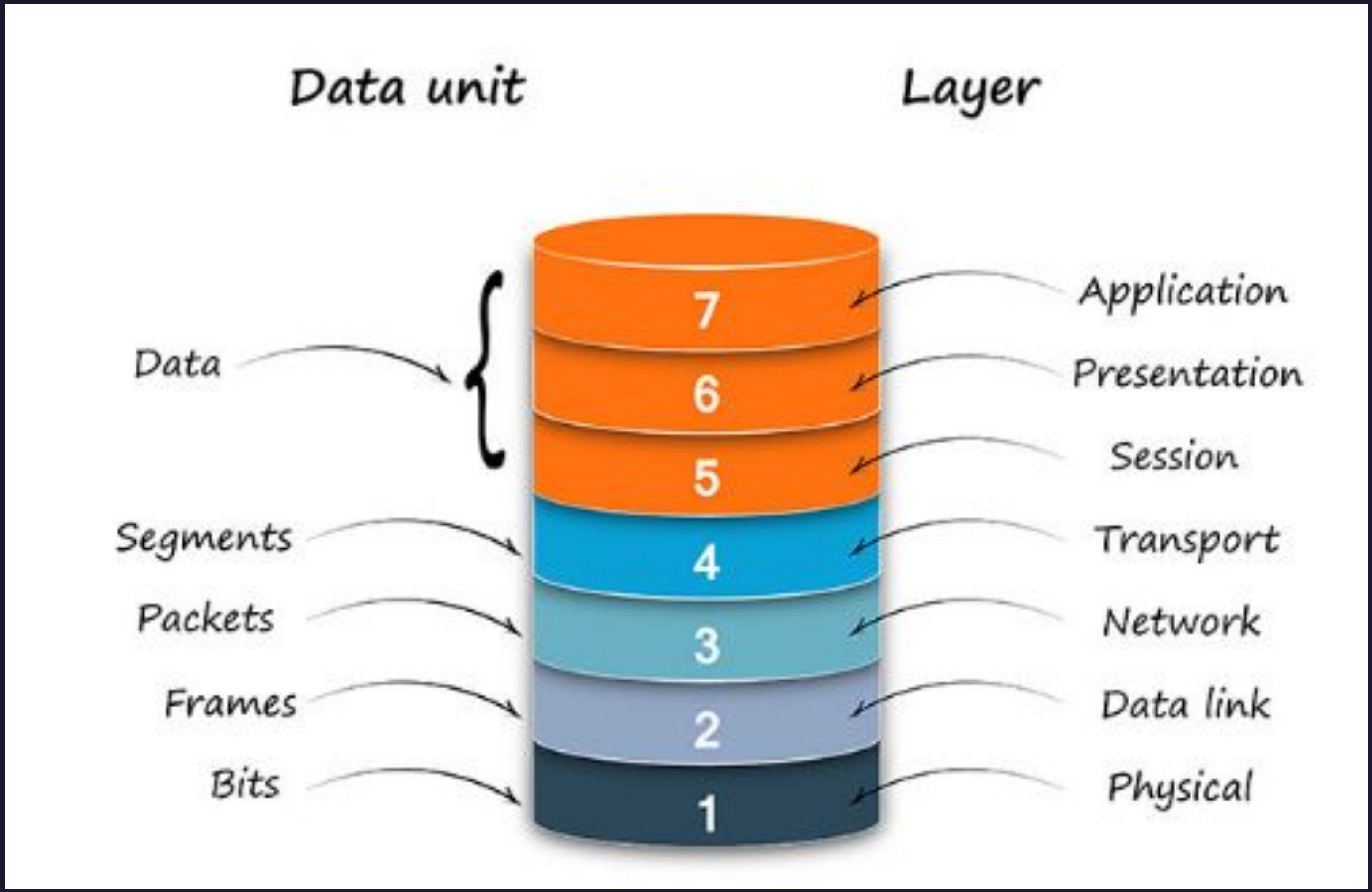
- There are many users who use computer network and are located all over the world.
- To ensure national and worldwide data communication ISO (ISO stands for International Organization of Standardization.) developed this model.
- This is called a model for open system interconnection (OSI) and is normally called as OSI model.
- OSI model architecture consists of seven layers.

OSI REFERENCE MODEL



- **Please Do Not Throw Sushi and Pizza Away. (PDNTSPA).**
-

Data Forms in Each Layer



Layer 1: The Physical Layer:

- It is the lowest layer of the OSI Model.
- It activates, maintains and deactivates the physical connection.
- It is responsible for transmission and reception of the unstructured raw data over network.
- Voltages and data rates needed for transmission is defined in the physical layer.
- It converts the digital/analog bits into electrical signal or optical signals.
- Data encoding is also done in this layer.

Layer 2: Data Link Layer:

- Data link layer synchronizes the information which is to be transmitted over the physical layer.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- Transmitting and receiving data frames sequentially is managed by this layer.
- This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
- This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

Layer 3: The Network Layer:

- It routes the signal through different channels from one node to other.
- It acts as a network controller. It manages the Subnet traffic.
- It decides by which route data should take.
- It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Layer 4: Transport Layer:

- It decides if data transmission should be on parallel path or single path.
- Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
- It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
- Transport layer can be very complex, depending upon the network requirements.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer:

- Session layer manages and synchronize the conversation between two different applications.
- Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Layer 6: The Presentation Layer:

- Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
- While receiving the data, presentation layer transforms the data to be ready for the application layer.
- Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
- It performs Data compression, Data encryption, Data conversion etc.

Layer 7: Application Layer:

- It is the topmost layer.
- Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
- This layer mainly holds application programs to act upon the received and to be sent data

Merits of OSI reference model:

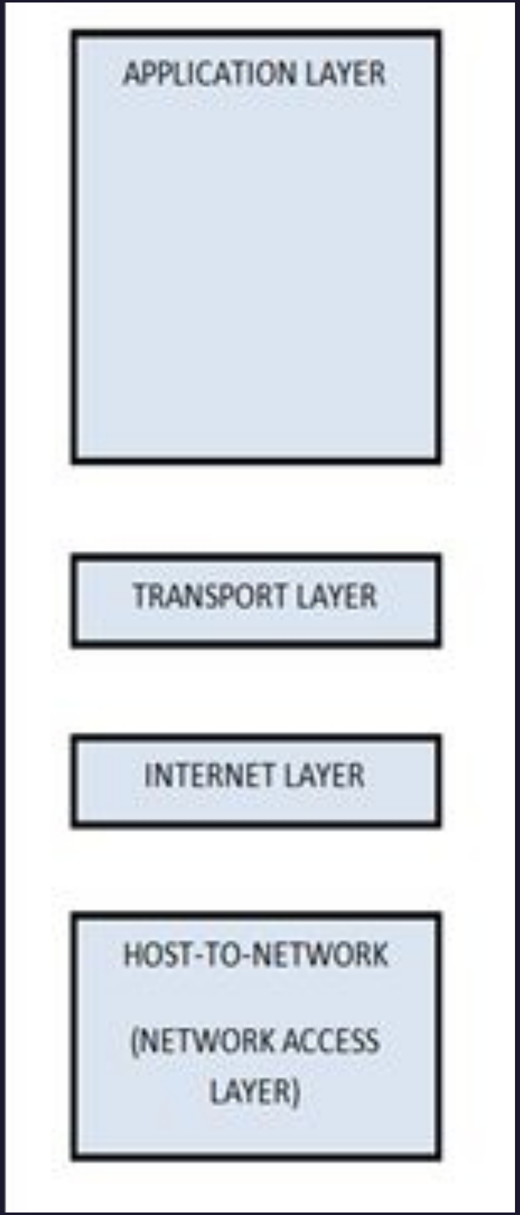
- OSI model distinguishes well between the services, interfaces and protocols.
- Protocols of OSI model are very well hidden.
- Protocols can be replaced by new protocols as technology changes.
- Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model:

- Model was devised before the invention of protocols.
- Fitting of protocols is tedious task.
- It is just used as a reference model.

TCP/IP REFERENCE MODEL

- TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.



The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.
- The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Layer 1: Host-to-network Layer

- Lowest layer of the all.
- Protocol is used to connect to the host, so that the packets can be sent over it.
- Varies from host to host and network to network.

Layer 2: Internet layer

- It is the layer which holds the whole architecture together.
- It helps the packet to travel independently to the destination.
- Order in which packets are received is different from the way they are sent.
- IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

- It decides if data transmission should be on parallel path or single path.
- Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
- The applications can read and write to the transport layer.
- Transport layer adds header information to the data.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

- The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

- TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.

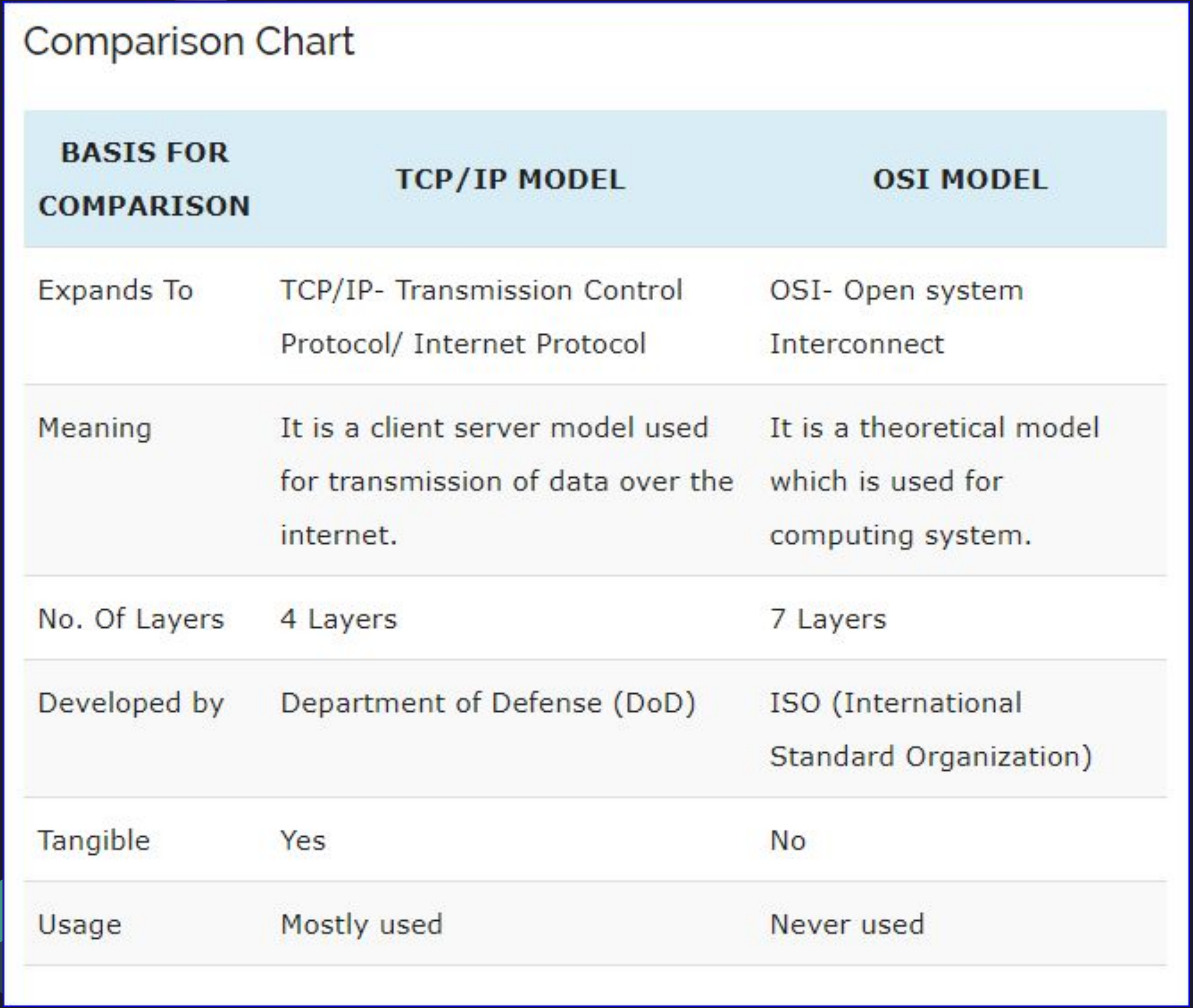
- FTP (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.

- SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.

- DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

Merits of TCP/IP model

- It operated independently.
- It is scalable.
- Client/server architecture.
- Supports a number of routing protocols.
- Can be used to establish a connection between two computers.



Comparison Chart

BASIS FOR COMPARISON	TCP/IP MODEL	OSI MODEL
Expands To	TCP/IP- Transmission Control Protocol/ Internet Protocol	OSI- Open system Interconnect
Meaning	It is a client server model used for transmission of data over the internet.	It is a theoretical model which is used for computing system.
No. Of Layers	4 Layers	7 Layers
Developed by	Department of Defense (DoD)	ISO (International Standard Organization)
Tangible	Yes	No
Usage	Mostly used	Never used

CONNECTION ORIENTED AND CONNECTIONLESS SERVICES

CONNECTION ORIENTED SERVICES

- There is a sequence of operation to be followed by the users of connection oriented service. These are :
- Connection is established
- Information is sent
- Connection is released
- In connection oriented service we have to establish a connection before starting the communication. When connection is established we send the message or the information and then we release the connection.
- Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

- **CONNECTION LESS SERVICES**
- It is similar to the postal services, as it carries the full address where the message (letter) is to be carried.
- Each message is routed independently from source to destination.
- The order of message sent can be different from the order received.
- In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this.
- Example of Connectionless service is UDP (User Datagram Protocol) protocol.

DIFFERENCE BETWEEN CONNECTION ORIENTED SERVICE AND CONNECTIONLESS SERVICE

- In connection oriented service authentication is needed while connectionless service does not need any authentication.
- Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs connectionless service protocol does not guarantees a delivery.
- Connection oriented service is more reliable than connectionless service.
- Connection oriented service interface is stream based and connectionless is message based.

SEE PDF FOR THESE CONTENT:

INTERNET
ISPS
BACKBONE NETWORK OVERVIEW
BUS BACKBONE
STAR BACKBONE
CONNECTING REMOTE LANS