

COMPUTER NETWORKS

By

Er. Khushbu Kumari Sarraf

COMMUNICATION

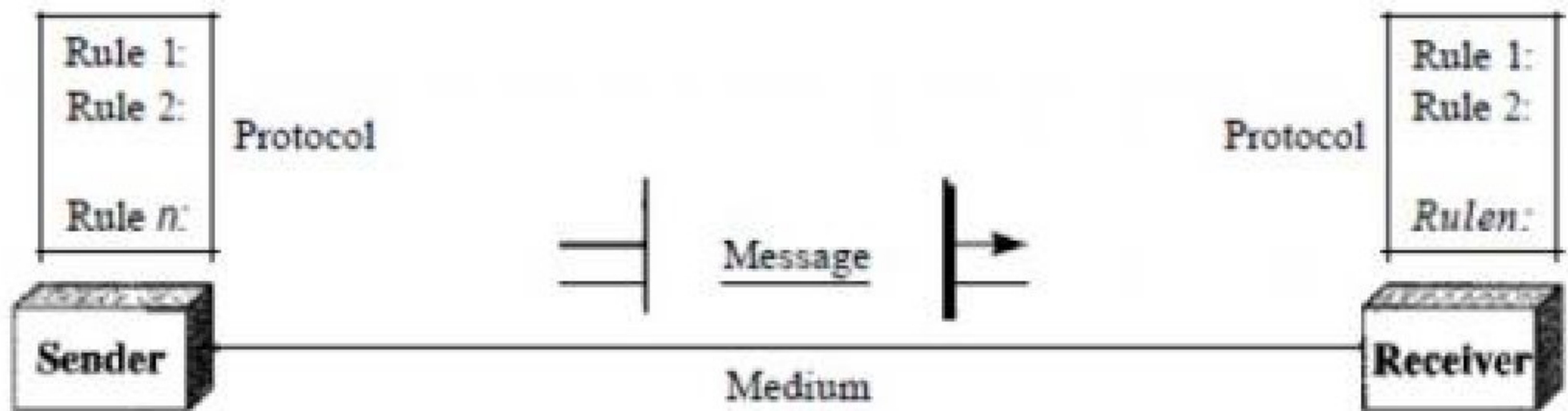
- Communication is the process of establishing connection or link between two points for information exchange.

OR

- Communication is simply the basic process of exchanging information.
- Typical example of communication system are line telephony and line telegraphy, radio telephony and radio telegraphy, radio broadcasting, point-to-point communication and mobile communication, computer communication, radar communication, television broadcasting, radio telemetry, radio aids to navigation, radio aids to aircraft landing etc.

A Basic Communication Model:

A data communications system has five components.



A Basic Communication Model:

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

Computer Networks

- A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels. The computers on a network may be linked through cables, telephone lines, radio waves, satellites etc.
- Computer Network uses distributed processing in which task is divided among several computers. Instead, a single computer handles an entire task, each separate computer handles a subset.
- A popular example of a computer network is the Internet, which allows millions of users to share information.

Computer Network



Network Criteria

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

- **Performance:** Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.
- **Reliability:** Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.
- **Security:** Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Every Network Includes:

1. At least two computers that have something to share.
2. A cable or wireless pathway, called **Transmission Media**, for computers to signal each other.
3. Rules, called **Protocols**, so that computers can use the unified principle of data communication.
4. Networking Interface Cards (NIC)

Advantages of Computer Network

- Sharing resources:** hardware resources such as processor, storage devices, printers, scanner, etc. can be shared among us using computer network. It helps to minimize the operational cost of an organization.
- Faster and cheaper communication:** communication in modern days has become very faster and cheaper to send information to a long distance through network.
- Centralized control:** all network resources such as computers, printer file , database , etc can be managed and controlled by a central connecting computer also known as the server.
- Backup and recovery:** server is used to keep data as backup. It maintains backup of all individual computer information.
- Remote and mobile access:** a remote user can access resources from the distance using computer network.

Disadvantages of Computer Network

- Expensive:** In order to install computer network, we require some extra cost to purchase networking devices such as hubs, switch, cables, etc.
- Security problems:** network security is the most challenging job for network administrator in order to protect network resources from authorized users and physical destructions.
- Needs technical person:** it is very difficult to install and operate good computer network.

Uses of Computer Network

Information and Resource Sharing

Computer networks allow organizations having units which are placed apart from each other, to share information in a very effective manner. Programs and software in any computer can be accessed by other computers linked to the network. It also allows sharing of hardware equipment, like printers and scanners among varied users.

Retrieving Remote Information

Through computer networks, users can retrieve remote information on a variety of topics. The information is stored in remote databases to which the user gains access through information systems like the World Wide Web.

Speedy Interpersonal Communication

Computer networks have increased the speed and volume of communication like never before. Electronic Mail (email) is extensively used for sending texts, documents, images, and videos across the globe. Online communications have increased by manifold times through social networking services.

E-Commerce

Computer networks have paved way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.

Uses of Computer Network

Highly Reliable Systems

Computer networks allow systems to be distributed in nature, by the virtue of which data is stored in multiple sources. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.

Cost-Effective Systems

Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to set up expensive mainframes for computation and storage. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose.

VoIP

VoIP or Voice over Internet protocol has revolutionized telecommunication systems. Through this, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.

Interactive entertainment

Interactive entertainment includes:

- Multiuser real-time simulation games.

- Video on demand.

Participation in programs likes quiz, contest, discussions etc.

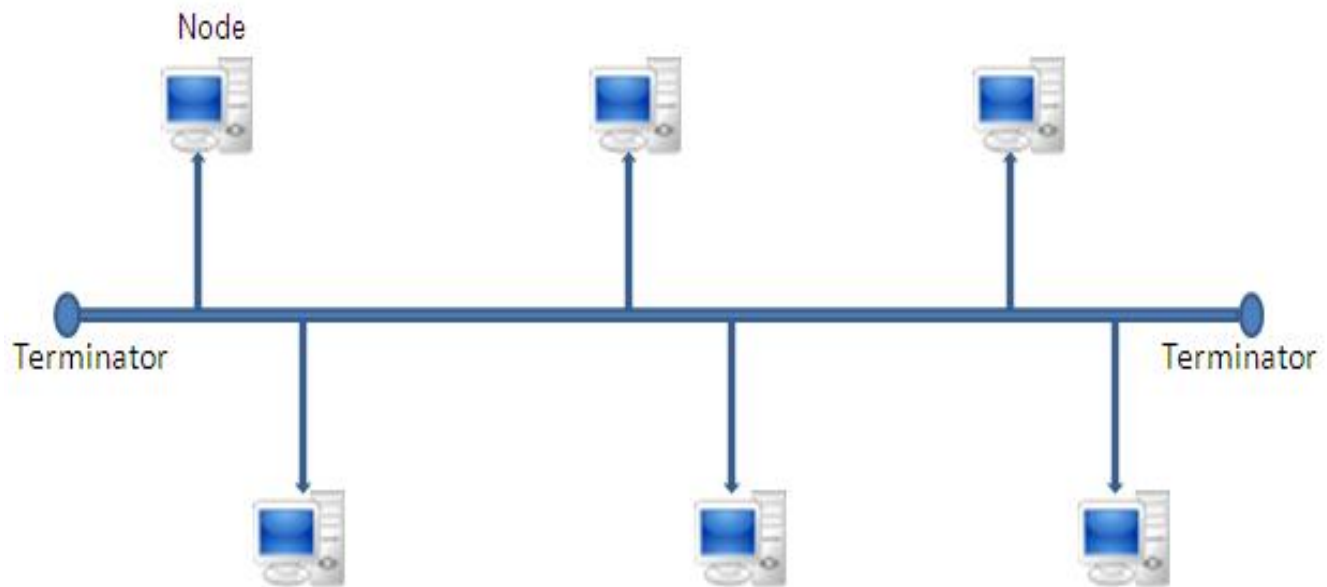
Network Topologies/ architecture:

A network topology is the physical arrangement of computers, cables and other components on a network. The type of topology you use affect the speed and performance of the computer network. The commonly used physical network topologies are;

- Bus Topology
- Ring Topology
- Star Topology
- Mesh Topology
- Tree Topology
- Hybrid Topology

Bus Topology

In a bus topology, all of the computers in a network are attached to a continuous cable or segment, that connects them in a linear format. It uses a common cable or backbone to connect all the nodes is called as Bus. In this topology, a packet or data is transmitted to all network adapter on that segment. Ethernet networks require a terminator at both ends of the bus. The purpose of the terminator is to absorb signals so that they do not reflect back down the line.



Bus Topology

Advantages:

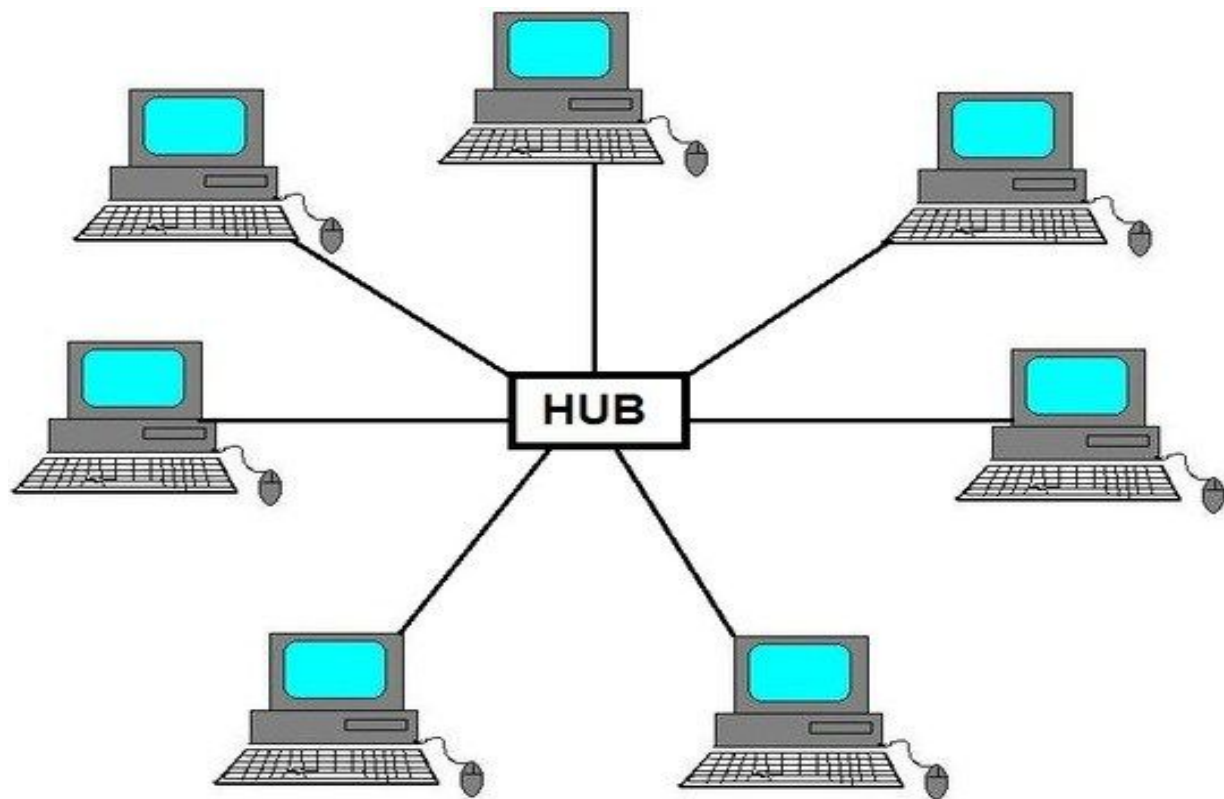
- Bus topology is simple, reliable (in very small network), easy to use and easy to understand.
- It is less expensive.
- It is easy to add a new node in the network.

Disadvantages:

- Heavy network traffic can slow a bus considerably.
- It is difficult to troubleshoot.
- If problems occurs on the backbone, the entire network will go down.

Star Topology:

In a star topology, all cables runs from the computer to a central location, where they are all connected by a device called a hub or switch. Each nodes on a star topology must be located relatively close to the hub.



Star Topology:

Advantages:

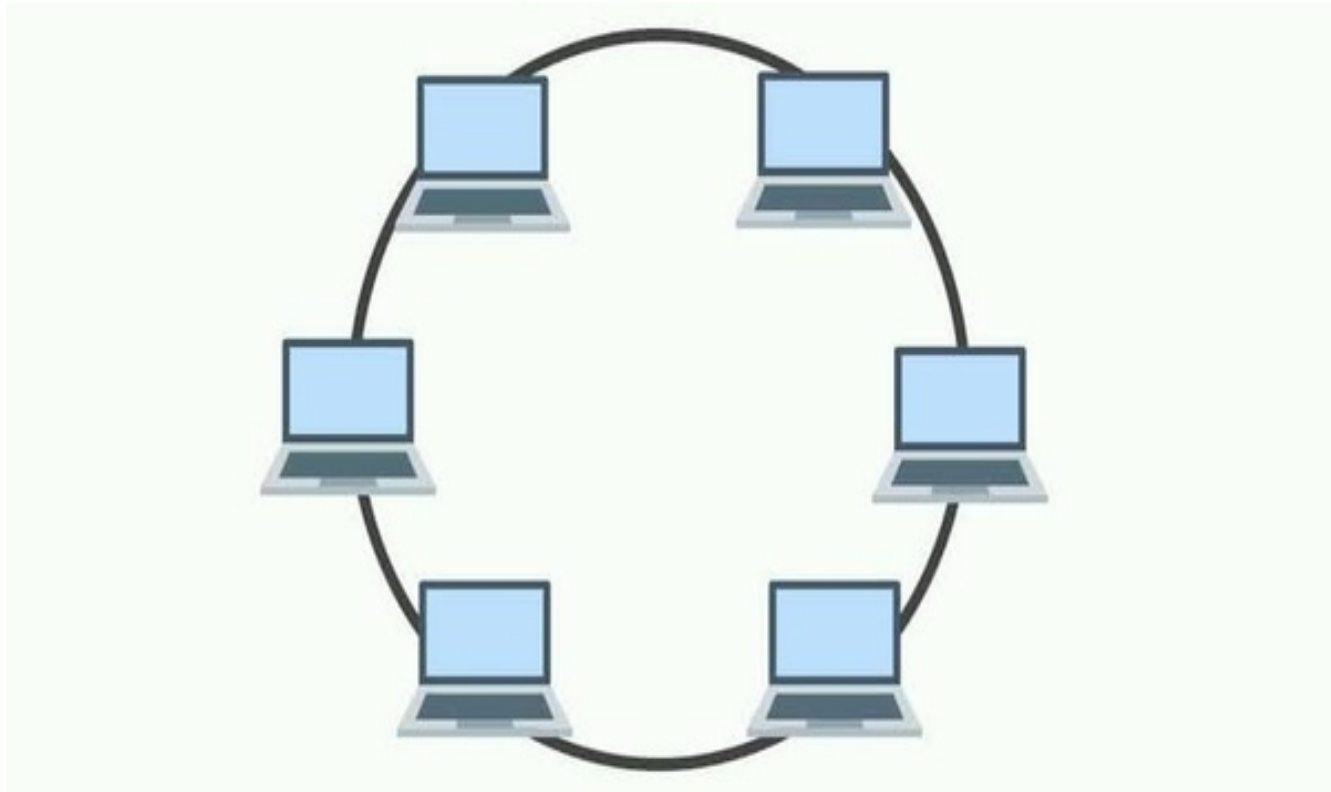
- It is easy to set up and configure.
- It is easy to modify and add new computers to a star topology without disturbing the rest of the network.
- Single computer failure does not necessarily bring down the whole star network.
- It is easy to detect the errors in star topology

Disadvantages:

- If the central device fails, the whole network stops.
- It costs more to cable a star topology because all network cable must be pulled to central point (hub).

Ring Topology:

In a ring topology, each computer is connected to the next computer with the last one connected to the first. The ring topology provides equal access for all computers on the network. The information on a ring network travels in one direction either clockwise or anti clockwise direction.



Ring Topology:

Advantages:

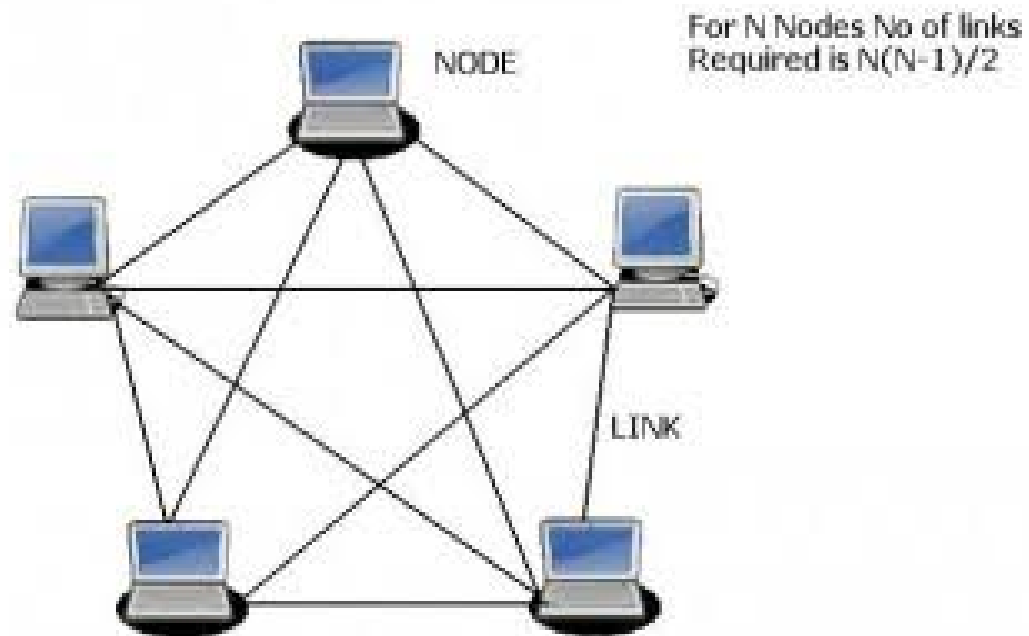
- Ring topology is easy to setup and reconfigure.
- Each computer is given equal opportunity to access the network resources.
- Single cable connects between the nodes.

Disadvantages:

- Failure of one computer on the ring can affect the entire network.
- Adding or removing computers disturbs the networks.
- It is difficult to troubleshoot in a ring topology.

Mesh Topology:

In a mesh topology, each node is linked to other through intermediate nodes with redundant paths. All nodes are connected directly to one another, which helps fast communication between nodes.



Mesh Topology:

Advantages:

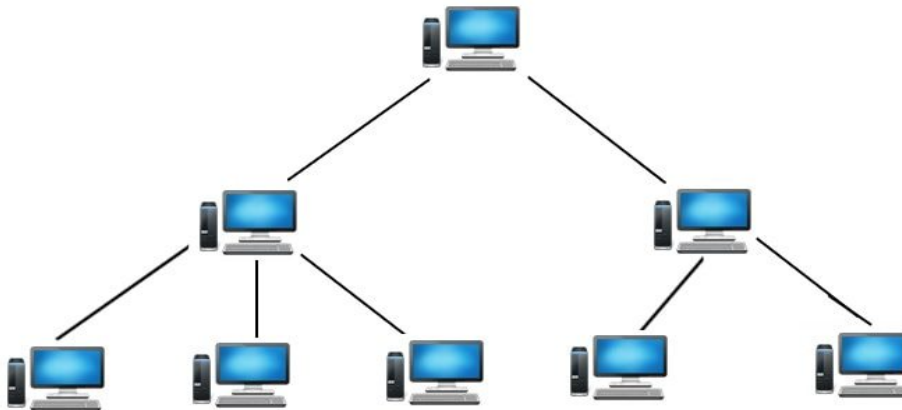
- The mesh topology is fault tolerance.
- It is easy to troubleshoot.

Disadvantages:

- Difficult to installation and reconfigure
- It is Expensive.

Tree Topology

Tree Topology is a topology which is having a tree structure in which all the computer are connected like the branches which are connected with the tree. A tree topology is a combination of a star network topology and a bus topology. In tree topology, nodes of the underlying bus network topology are replaced with a complete star topology.



Tree Topology:

Advantages:

- The leaf nodes can add one or more nodes in the hierarchical chain, this topology provides high scalability.
- Tree topology provides easy maintenance and easy fault identification can be done.

Disadvantages:

- Requires large number of cables compared to star and ring topology.
- The establishment cost increases as well.
- If the bulk of nodes are added in this network, then the maintenance will become complicated.

Hybrid Topology

Hybrid topology is a combination of more than two topologies. In computer networking, a network structure that contains more than two topologies is known as hybrid topology. It inherits the advantages and disadvantages of included topologies.

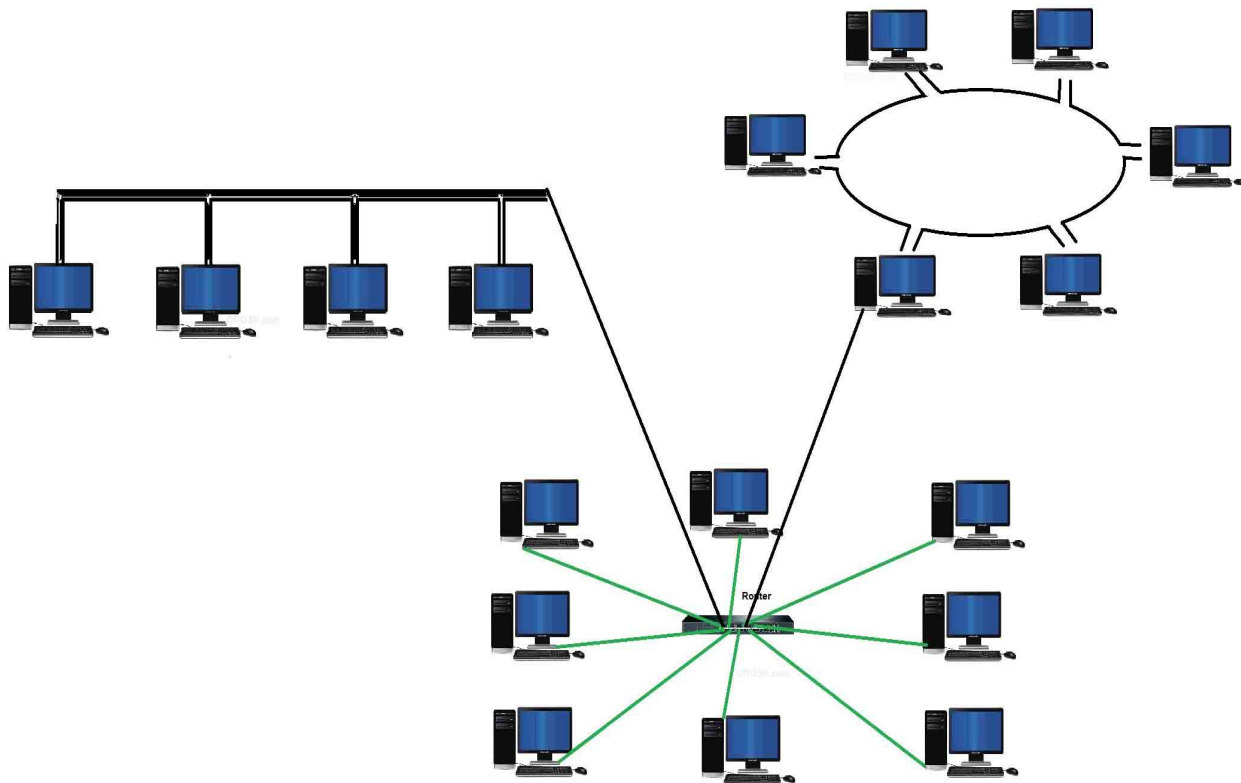
Hybrid Topology:

•Advantages:

- This type of topology combines the benefits of different types of topologies in one topology.
- Can be modified as per requirement.
- It is very reliable.
- Error detecting and trouble shooting is easy.
- It is used for create large network.

Disadvantages:

- It is a type of network expensive.
- Design of a hybrid network is very complex.
- There is change hardware in order to connect topology with another topology.
- Installation is a difficult process.



Network Types:

- Computer network is broadly classified into three types
 1. Local Area Network (LAN),
 2. Metropolitan Area Network (MAN), and
 3. Wide Area Network (WAN).
- The different network types are distinguished from each other based on the following characteristics:
 1. Size of the network
 2. Transmission Technology
 3. Networking Topology
- The size of the network refers to the area over which the network is spread.
- Transmission technology refers to the transmission media used to connect computers on the network and the transmission protocols used for connecting.
- Network topology refers to the arrangement of computers on the network or the shape of the network.

Local Area Network

A local area network (LAN) refers to a combination of computer hardware and transmission media that is relatively small. Normally, LAN is entirely contained within a school, college, building etc. LANs is typically comprised of only one transmission media type such as coaxial cable or twisted pair cable but never both. The features of LAN are;

- It covers short geographical area.
- LANs are characterized by comparatively high speed communication.
- LAN uses only one kinds of cable.
- Complete ownership by single organization.

Network Types:

Local Area Networks (LAN):

Characteristics of LAN:

- LANs are private networks, not subject to external control

- Simple and better performance

- Work in a restricted geographical area

Advantages:

- Resource sharing

- Software applications sharing

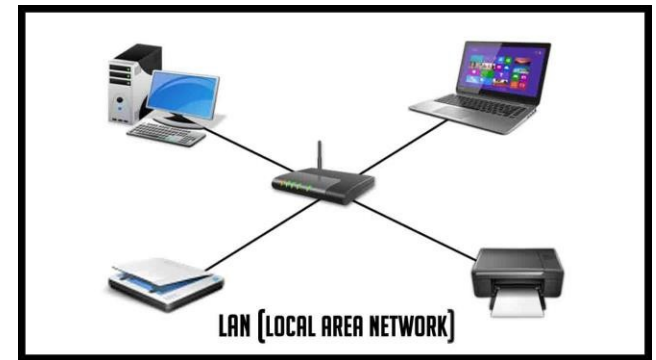
- Easy and Cheap communication

- Data Security

Disadvantages:

- Internet sharing

- Restricted to local area



Network Types:

Local Area Networks (LAN):

Characteristics of LAN:

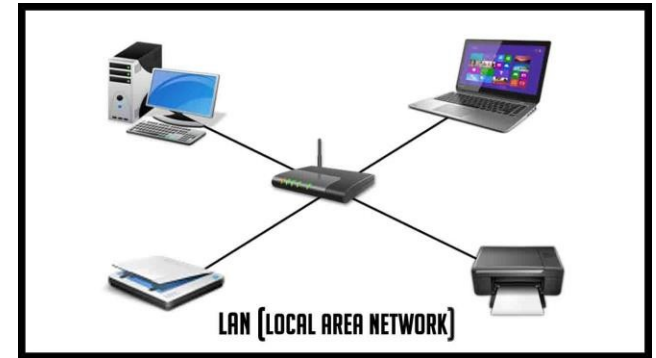
- LANs are private networks, not subject to external control
- Simple and better performance
- Work in a restricted geographical area

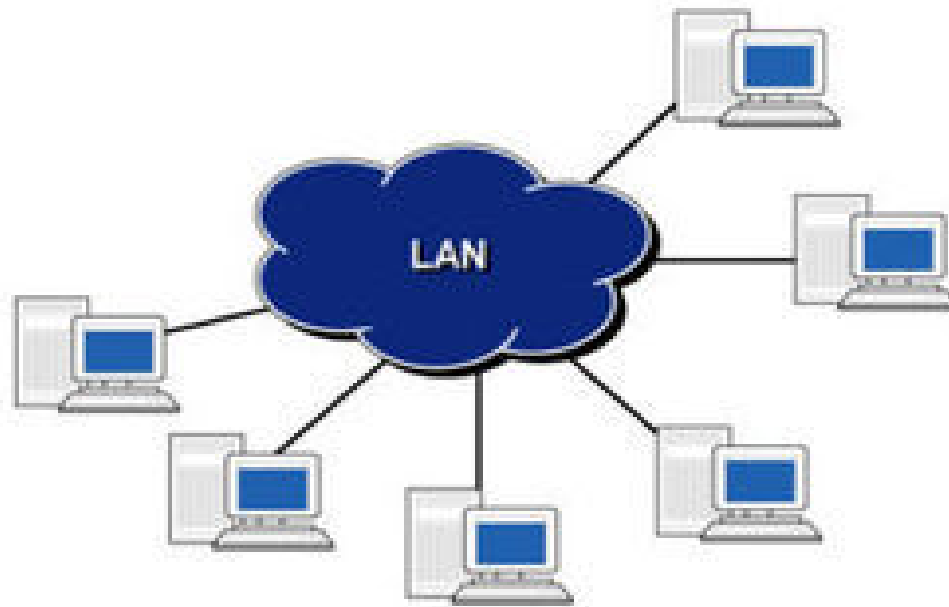
Advantages:

- Resource sharing
- Software applications sharing
- Easy and Cheap communication
- Data Security
- Internet sharing

Disadvantages

- Restricted to local area





Metropolitan Area Network:

- A Metropolitan Area Network (MAN) is a network that is larger than a LAN. It is called metropolitan since it normally covers the area of city. Different hardware and transmission media are often used in MAN because they don't require complete access to locations between the network sites. The features of the MAN are;
 - It covers large geographical area with respect to LAN.
 - MANs typically used when you need to connect dissimilar system within a single metropolitan.
 - It is owned by single or multiple organizations.
 - It uses private or public connection mediums.

Network Types:

Metropolitan Area Network (MAN):

A metropolitan area network, or MAN, covers a city. A MAN is a computer network that interconnects users with computer resources in a geographical area or region larger than that covered by a LAN. It can be an interconnection between several LANs by bridging them with backbone lines.

Characteristics:

- Generally, covers towns and cities (up to 50km)

- Transmission medium used for MAN is optical fiber, coaxial cable etc.

- Data rates adequate for distributed computing applications

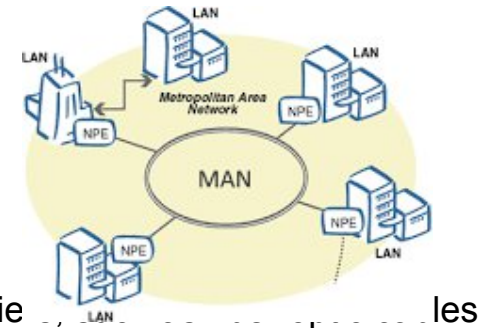
Advantages

- Extremely efficient and provide fast communication via high-speed carrier

- Good backbone for larger networks and provides greater access to WAN

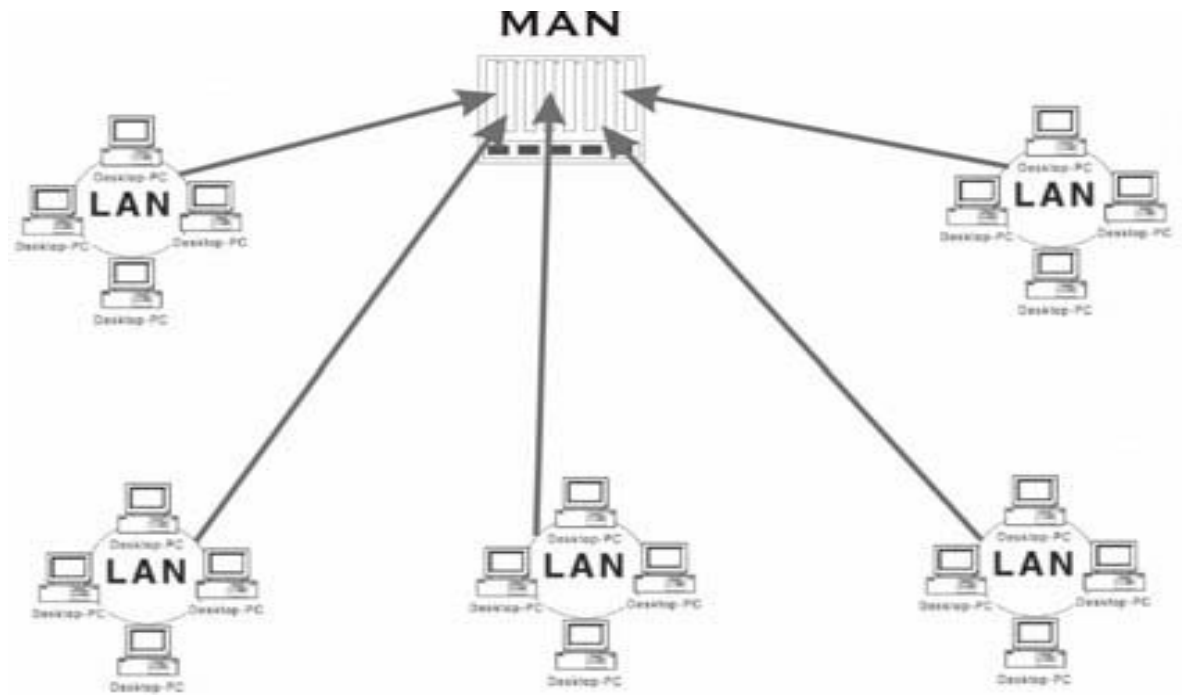
Disadvantages

- Complex, more cabling required and expensive



Network Types:

The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses. At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only. Cable television is not the only MAN. Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as IEEE 802.16.



Wide Area Network (WAN):

A Wide Area Network is a network of connecting two or more computers generally across a wide geographical area such as cities, districts and countries. WANs interconnect LANs which may be at the opposite side of a country or located around the world. It uses telephone lines, communication satellite and other long range communication links to connect the computers and network. Internet is an example of WAN. The characteristics of WAN are:

- It covers a large geographical area.
- Transmission cost is high
- Transmission error is higher than LAN
- It is owned by multiple organizations.
- It uses public connections mediums such as telephone lines, wireless technology etc.

Wide Area Network (WAN):

Characteristics

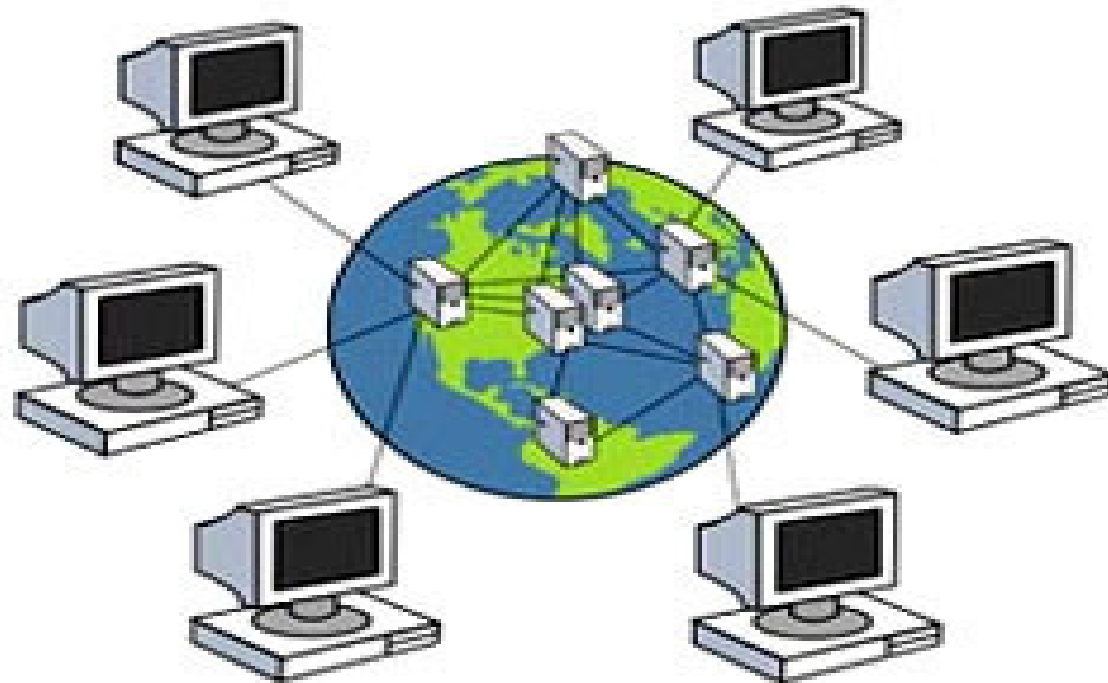
- Covers large distances (states, countries, continents)
- Communication medium used are satellite, public telephone networks which are connected by routers

Advantages

- Covers large geographical area
- Shares software and resources with connecting workstations
- Information can be exchanged to anyone else worldwide in the network

Disadvantages

- Data security
- Network is very complex and management is difficult
- As size increases, the networks become more expensive



Difference Between the types of Computer network

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

Different types of Computer network

Campus Area Network (CAN)

- A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area. A CAN is smaller than a wide area network (WAN) or metropolitan area network (MAN).
- A CAN is also known as a corporate area network (CAN).
- In most cases, CANs own shared network devices and data exchange media.
- CAN benefits are as follows:
 - Cost-effective
 - Wireless, versus cable
 - Multi departmental network access
 - Single shared data transfer rate (DTR)

Different types of Computer network

Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.

Different types of Computer network

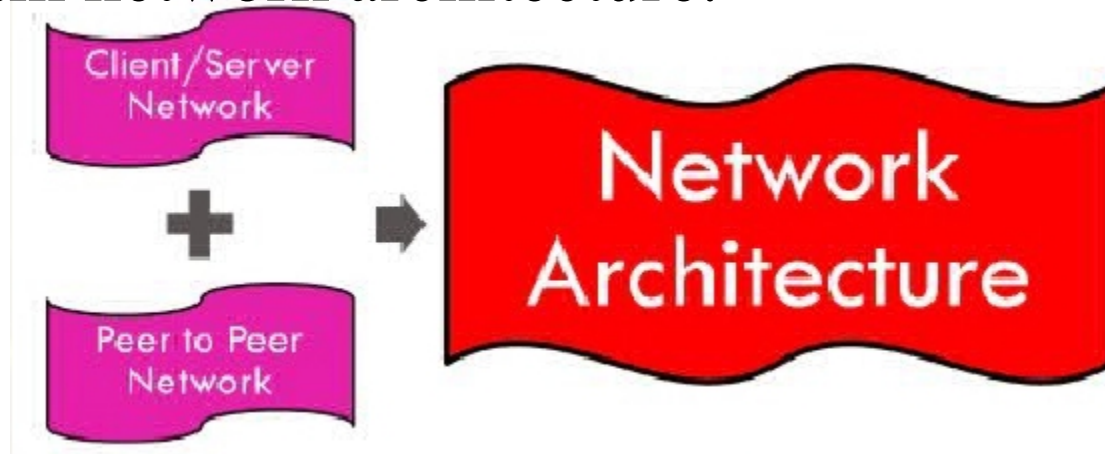
Personal Area Network (PAN)

PAN (Personal Area Network) is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

- It is mostly personal devices network equipped within a limited area.
- Allows you to handle the interconnection of IT devices at the surrounding of a single user.
- PAN includes mobile devices, tablet, and laptop.
- It can be wirelessly connected to the internet called WPAN.
- Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

Network Architecture

- **Network Architecture** is the over all **design of a computer** network that describes how a computer network is configured and what strategies are being used.
- It also know as **network model** or **network design**.
- Two main network architecture:



Network Architecutre

Network is the collection of computers, software and hardware that are all connected to each other to help their users work together. A network connects computers by means of cabling systems, specialized software and devices that manage data traffic. A network enables users to share files and resources, such as printers as well as send messages electronically to each other. Computer network falls under two types:

- Client/Server Network
- Peer to peer Network

Client/Server Network:

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.

Client/Server Network:

Advantages:

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources

Disadvantages:

- Require expensive, more powerful hardware for the server machine.
- Has a single point of failure. User data is unavailable when the server is down.
- Requires expensive specialized network administrative and operational software.
- Requires a professional administrator.

Peer-to-Peer Network:

- Network computers act as equal partners, or peers. Each computer can take on the client function or the server function. Computer A may request for a file from computer B, which then sends the file to Computer A. Computer A acts like the client and Computer B acts like the server. At a later time, Computer A and B may reverse roles.
- Individual users control their own resources. The users may decide to share certain files with other users.
- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.

Peer-to-Peer Network:

Advantages:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages:

- Less secure.
- Doesn't scale well to large networks and administration becomes unmanageable.
- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.

Protocols:

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

Syntax. 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. 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? For example, does an address identify the route to be taken or the final destination of the message?

Timing. 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 :

It provides guidelines to manufacturers, vendor, government agencies and other service providers to ensure the kind of interconnectivity necessary in today's market place and in international communication. It is important to follow Standards which are created by various Standard Organization like IEEE , ISO , ANSI etc.

Types of Standards :

Standards are of two types :

- De Facto Standard.
- De Jure Standard.

Standards

De Facto Standard : De facto" means "**in fact**" or "**in practice.**"

These are standards that are widely used and accepted in practice, even though they may not be officially approved by a formal standards organization.

Characteristics:

- Widely adopted by users or companies.
- Becomes a standard through market dominance or common usage.
- May later become a formal (de jure) standard.

Examples:

- **TCP/IP:** Became the dominant networking protocol before being standardized by IETF.
- **PDF (Portable Document Format):** Created by Adobe and widely used before becoming an ISO standard.
- **Microsoft Office file formats (.doc, .xls):** Commonly used before being standardized

Standards

De Jure Standard : De jure" means "**by law**" or "**by regulation.**"

These are standards that are officially approved and recognized by standardization bodies.

Characteristics:

- Approved by national or international organizations.
- Legally recognized.
- Often more formal and documented.

Examples:

- OSI Model (by ISO):** A reference model for how applications communicate over a network.
- IEEE 802.11:** Standard for wireless LAN (Wi-Fi).
- HTML (by W3C):** Standard for web page structure and content.

Connection-Oriented and Connectionless Network Service

- Data communication is a telecommunication network to send and receive data between two or more computers over the same or different network. There are two ways to establish a connection before sending data from one device to another, that are **Connection-Oriented** and **Connectionless Service**.
- Connection-oriented service involves the creation and termination of the connection for sending the data between two or more devices.
- In contrast, connectionless service does not require establishing any connection and termination process for transferring the data over a network.

Connection-Oriented	Connectionless
It is designed and developed based on the telephone system.	It is service based on the postal system.
It is used to create an end to end connection between the senders to the receiver before transmitting the data over the same or different network.	It is used to transfer the data packets between senders to the receiver without creating any connection.
It requires authentication before transmitting the data packets to the receiver.	It does not require authentication before transferring data packets.
All data packets are received in the same order as those sent by the sender.	Not all data packets are received in the same order as those sent by the sender.
It is a more reliable connection service because it guarantees data packets transfer from one end to the other end with a connection.	It is not a reliable connection service because it does not guarantee the transfer of data packets from one end to another for establishing a connection.
Transmission Control Protocol (TCP) is an example of a connection-oriented service.	User Datagram Protocol (UDP) is an examples of connectionless service.

Connection-Oriented vs Connectionless



Connection-Oriented Network Service

A connection-oriented service is a network service that was designed and developed after the telephone system. A connection-oriented service is used to create an end to end connection between the sender and the receiver before transmitting the data over the same or different networks. In connection-oriented service, packets are transmitted to the receiver in the same order the sender has sent them. It uses a handshake method that creates a connection between the user and sender for transmitting the data over the network. Hence it is also known as a reliable network service.

Connectionless Network Services

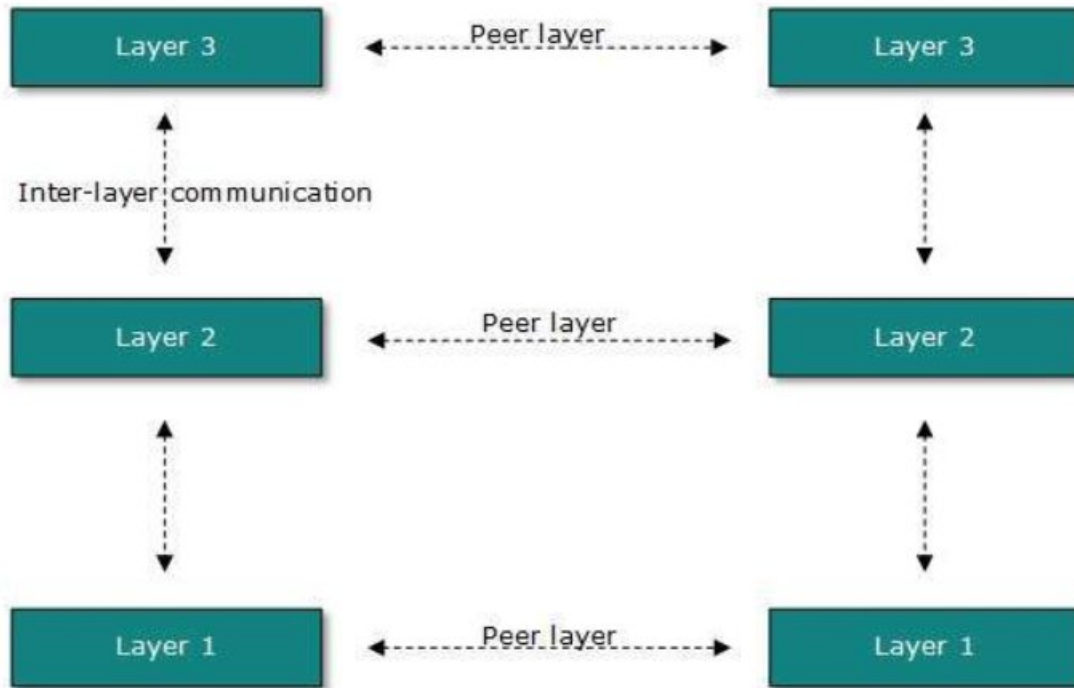
A connection is similar to a **postal system**, in which each letter takes along different route paths from the source to the destination address. Connectionless service is used in the network system to transfer data from one end to another end without creating any connection. So it does not require establishing a connection before sending the data from the sender to the receiver. It is not a reliable network service because it does not guarantee the transfer of data packets to the receiver, and data packets can be received in any order to the receiver. Therefore we can say that the data packet does not follow a **defined** path. In connectionless service, the transmitted data packet is not received by the receiver due to network congestion, and the data may be lost.

Layered Architecture

In layered architecture of Network Model, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.

In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the-top most layer, it is passed on to the layer below it for further processing. The lower layer does the same thing; it processes the task and passes on to lower layer. If the task is initiated by lower most layer, then the reverse path is taken.

Layered Architecture



Every layer clubs together all procedures, protocols, and methods which it requires to execute its piece of task.

Layered Architecture

Why Layered architecture?

1. To make the design process easy by breaking unmanageable tasks into several smaller and manageable tasks (by divide-and-conquer approach).
2. Modularity and clear interfaces in layered architecture help different parts of a network system work together, even if they are made by different companies. This makes networks more flexible, compatible, and easier to manage.
3. Ensure independence of layers, so that implementation of each layer can be changed or modified without affecting other layers.
4. Each layer can be analyzed and tested independently of all other layers.

Reference Model

There are basically two reference model:

- OSI reference model
- TCP/IP reference model

Open System Interconnection (OSI) Reference Model

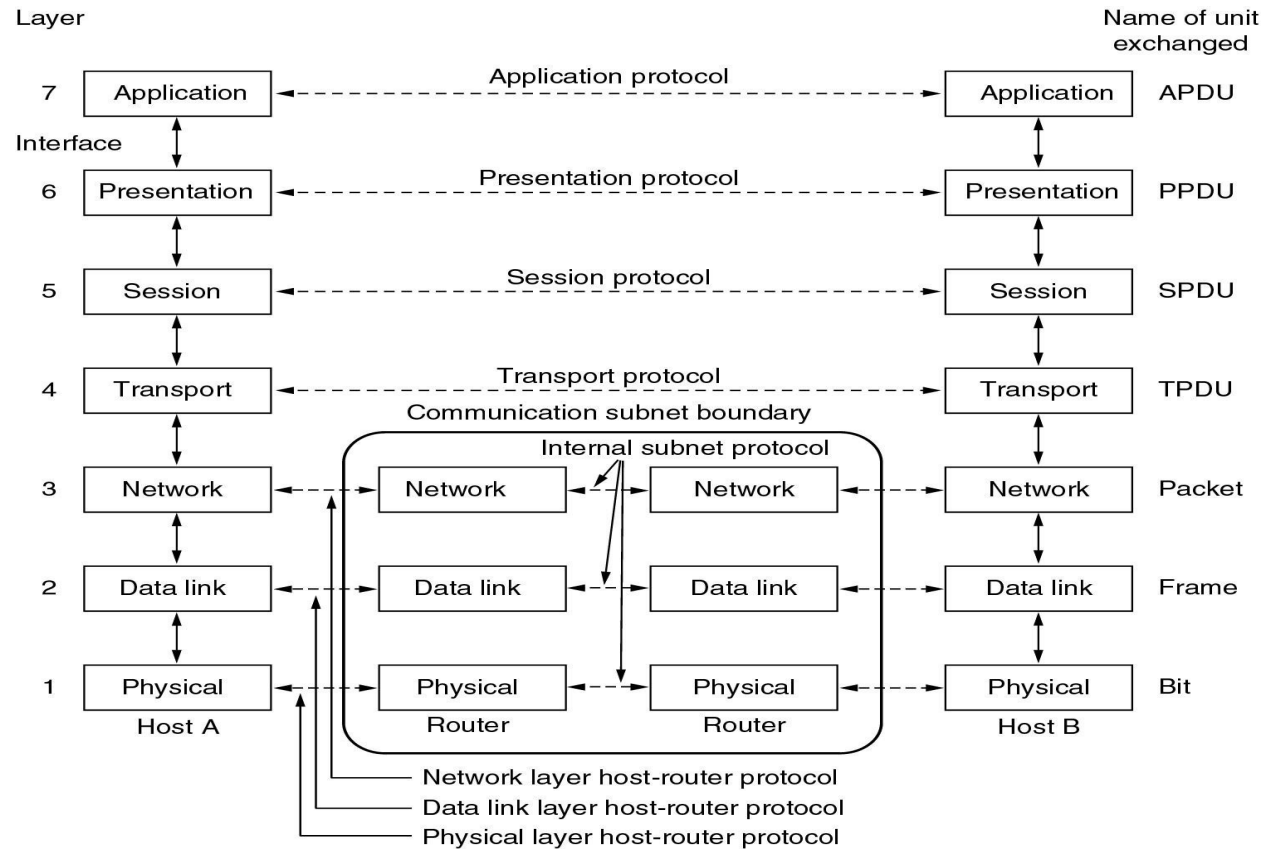
- The OSI reference model is a framework that is used to understand how information travels throughout a network.
- The OSI reference model explains how packets travel through the various layers to another device on a network, even if the sender and destination have different types of network media.

Open System Interconnection (OSI) Reference Model

In the OSI reference model, there are seven numbered layers, each of which illustrates a particular network function.

- **Physical Layer**
- **Data Link Layer**
- **Network Layer**
- **Transport Layer**
- **Session Layer**
- **Presentation Layer**
- **Application Layer**

Open System Interconnection (OSI) Reference Model



Physical Layer (Layer 1)

- Concern with data transmission
- Wires and their specification
- Connector for the system to connect
- Voltage (voltage at which the binary data is being assign and (transmitted))
- Data rate (rate at which bit is transmit)
- Protocol Data Unit(PDU): bps

Data Link Layer (Layer 2)

- There is a direct link control on the network
- Provide reliable data transfer over the link
- Physical addressing
- Error notification and flow control
- Protocol Data Unit(PDU): Frame

Network Link Layer (Layer 3)

- Network addressing
- Best path determination
- Data transmission between the subnet
- Protocol Data Unit(PDU): Packet

Transport Link Layer (Layer 4)

- Segmentation and Reassembly
- Process are addressed
- Reliable data transfer between the host
- Establish connection between the host
- Flow control and congestion control
- Error detection and recovery
- Protocol Data Unit (PDU): Segment / Datagram

Session Link Layer (Layer 5)

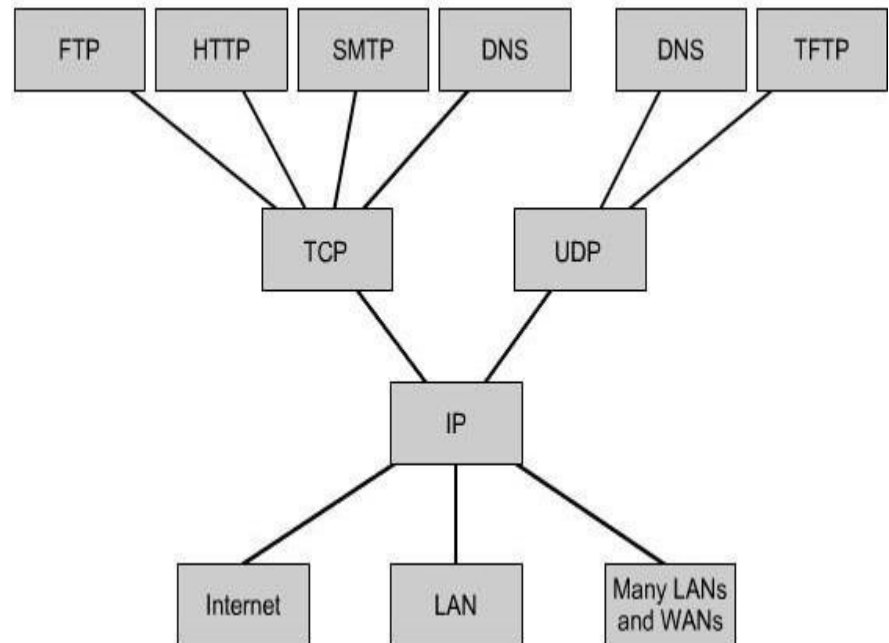
- Maintain the session of the user
- Token management
- Track all the event through the use
- Establish and terminate session
- Protocol Data Unit (PDU): Data

Presentation Link Layer (Layer 6)

- Data representation
- Ensure the data is read able by the application
- Format of data
- Data structure selection
- Data transfer syntax and semantics
- eg. ASCII, UNICODE etc
- Protocol Data Unit (PDU): Data

Application Link Layer (Layer 7)

- Application for the user for network use
- Provide the different network services to the user
- Email, www, ftp, http, smtp etc.
- Protocol Data Unit (PDU): Data



Relationship of Services to Protocols

Services

- A service is a set of operations (primitives) that one layer offers to the layer above it.
- It defines what functions or tasks a layer will perform for the layer above.
- It describes what the layer does, but not how it is done internally.
- The service is about the interface between two adjacent layers:
- The lower layer acts as a service provider.
- The upper layer acts as a service user.

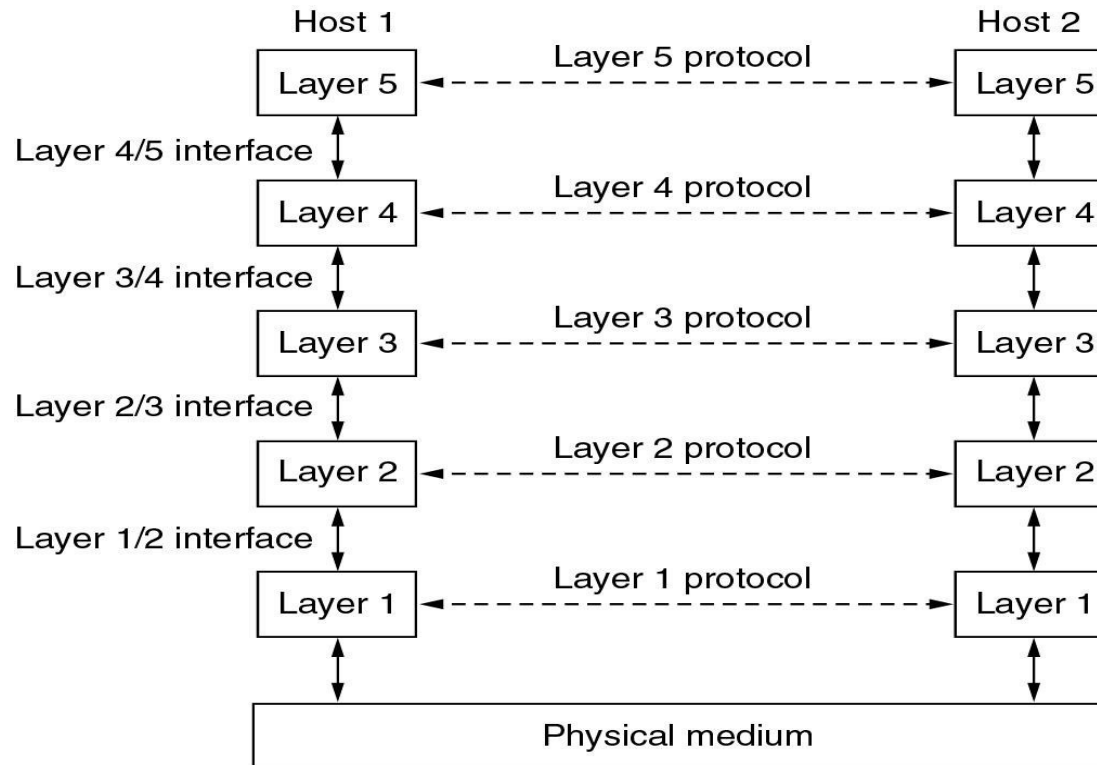
Protocol

- A protocol is a set of rules and conventions used by peer entities at the same layer on different machines.
- It defines how data is formatted, transmitted, and understood between these peer entities.
- Protocols are used to implement the services that a layer promises.
- Protocols govern the actual communication between devices (like how packets are structured and exchanged).

Relationship of Services to Protocols

Service	Protocol
Set of operations provided to the upper layer	Rules for communication between peer entities
What the layer does	How the layer does it
Interface between adjacent layers	Communication between entities at the same layer
File transfer service, error checking service	TCP protocol, HTTP protocol

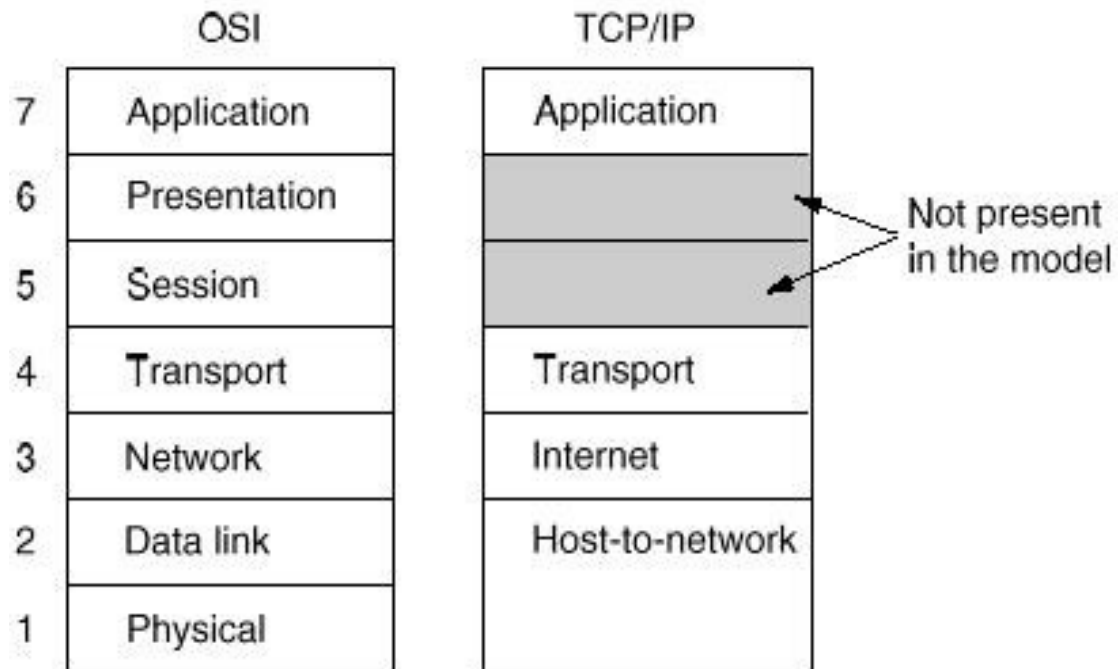
Relationship of Services to Protocols



TCP/IP Model

- TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.
- TCP/IP was developed as an open standard. This meant that anyone was free to use TCP/IP. This helped speed up the development of TCP/IP as a standard.
- **The TCP/IP model has the following four layers:**
 - **Application layer**
 - **Transport layer**
 - **Internet layer**
 - **Network access layer /Host-to-network layer**

TCP/IP Model



TCP/IP Model

Network Access Layer

- The lowest layer of the TCP/IP protocol hierarchy.
- It defines how to use the network to transmit an IP datagram. Unlike higher-level protocols, Network Access Layer protocols must know the details of the underlying network (its packet structure, addressing, etc.) to correctly format the data being transmitted to comply with the network constraints.
- The TCP/IP Network Access Layer can encompass the functions of all three lower layers of the OSI reference Model (Physical, Data Link and Network layers).
- As new hardware technologies appear, new Network Access protocols must be developed so that TCP/IP networks can use the new hardware. Consequently, there are many access protocols - one for each physical network standard.

TCP/IP Model

Internet layer

- Provides services that are roughly equivalent to the OSI Network layer.
- The primary concern of the protocol at this layer is to manage the connections across networks as information is passed from source to destination.
- The Internet Protocol (IP) is the primary protocol at this layer of the TCP/IP model.

Transport layer

- It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer.
- Two end-to-end transport protocols have been defined here: TCP and UDP

TCP/IP Model

Application Layer

- Includes the OSI Session, Presentation and Application layers.
- An application is any process that occurs above the Transport Layer. This includes all of the processes that involve user interaction. The application determines the presentation of the data and controls the session.
- There are numerous application layer protocols in TCP/IP, including Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) used for e-mail, Hyper Text Transfer Protocol (HTTP) used for the World-Wide-Web, and File Transfer Protocol (FTP).
- Most application layer protocols are associated with one or more port number.

Similarities between OSI Model & TCP/IP Model

- Both have layered architecture.
- Layers provide similar functionalities.
- Both are protocol stack.
- Both are reference models.

Difference between OSI Model & TCP/IP Model

OSI Model	TCP/IP Model
It has 7 layers	It has 4 layers
In OSI model the transport layer guarantees the delivery of packets.	In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
It is reference model.	It is implemented model.
OSI model has a separate Presentation layer and Session layer.	TCP/IP does not have a separate Presentation layer or Session layer.
Transport Layer is Connection Oriented.	Transport Layer is both Connection Oriented and Connection less.
It is a theoretical model which is used for computing system.	It is a client server model used for transmission of data over the internet.

Internet

A network is a group of connected communicating devices such as computers printers and other devices.

The internet is a globally connected network system that uses TCP/IP to transmit data via various types of media. Simply, internet is a means of connecting a computer to any other computer anywhere in the world via dedicated routers and servers.

Internet is a network of global exchanges – including private, public, business, academic and government networks and is made up of many wide and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the internet because it is continually changing-new networks are being added, existing networks are adding addresses and networks of defunct companies are being removed. Most end users nowadays use the Internet services of Internet Service providers (ISPs).

Internet Service Provider (ISP):

Internet service provider (ISP), company that provides [Internet](#) connections and services to individuals and organizations. In addition to providing access to the Internet, ISPs may also provide [software](#) packages (such as [browsers](#)), [e-mail](#) accounts, and a personal [Web site](#) or home page. ISPs can host Web sites for businesses and can also build the Web sites themselves. ISPs are all connected to each other through network access points, public network facilities on the Internet [backbone](#).

An Internet service provider (ISP) is a company that provides web access to both businesses and consumers.

ISPs may also provide other services such as email services, domain registration, web hosting, and browser services.

An ISP is considered to be an information service provider, storage service provider, Internet network service provider (INSP), or a mix of all of them.

An **INSP** is a company or organization that provides **internet backbone services** or network infrastructure that connects various ISPs.

Backbone Network:

A backbone or core is a part of a computer network which interconnects pieces of various networks, providing a path for the exchange of information between different LANs or subnetworks.

A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than the networks connected to it.

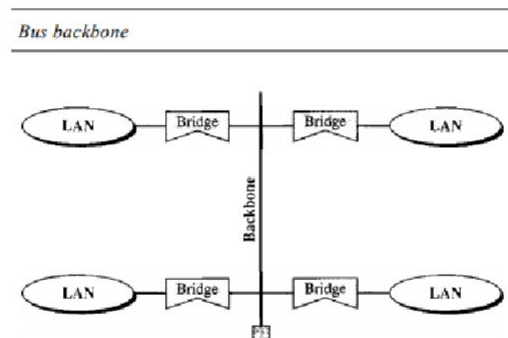
In a backbone network, no station is directly connected to the backbone; the stations are part of a LAN and the backbone connects the LANs.

The backbone is itself a LAN that uses a LAN protocol such as Ethernet; each connection to the backbone is itself another LAN. Although many different architectures can be used for a backbone, we discuss only the two most common: the bus and the star.

Backbone Network:

Bus Backbone:

In a bus backbone, the topology of the backbone is a bus. Bus backbones are normally used as a distribution backbone to connect different buildings in an organization. Each building can comprise either a single LAN or another backbone (normally a star backbone). A good example of a bus backbone is one that connects single- or multiple-floor buildings on a campus. Each single-floor building usually has a single LAN. Each multiple-floor building has a backbone (usually a star) that connects each LAN on a floor. A bus backbone can interconnect these LANs and backbone



Backbone Network:

Star Backbone:

In a star backbone, sometimes called a collapsed or switched backbone, the topology of the backbone is a star. In this configuration, the backbone is just one switch that connects the LANs. Star backbones are mostly used as a distribution backbone inside a building. In a multi-floor building, we usually find one LAN that serves each particular floor. A star backbone connects these LANs. The backbone network, which is just a switch, can be installed in the basement or the first floor, and separate cables can run from the switch to each LAN. In the following configuration, the switch does the job of the backbone and at the same time connects the LANs

