

Computer Networks (CS303)

Assignment - 1

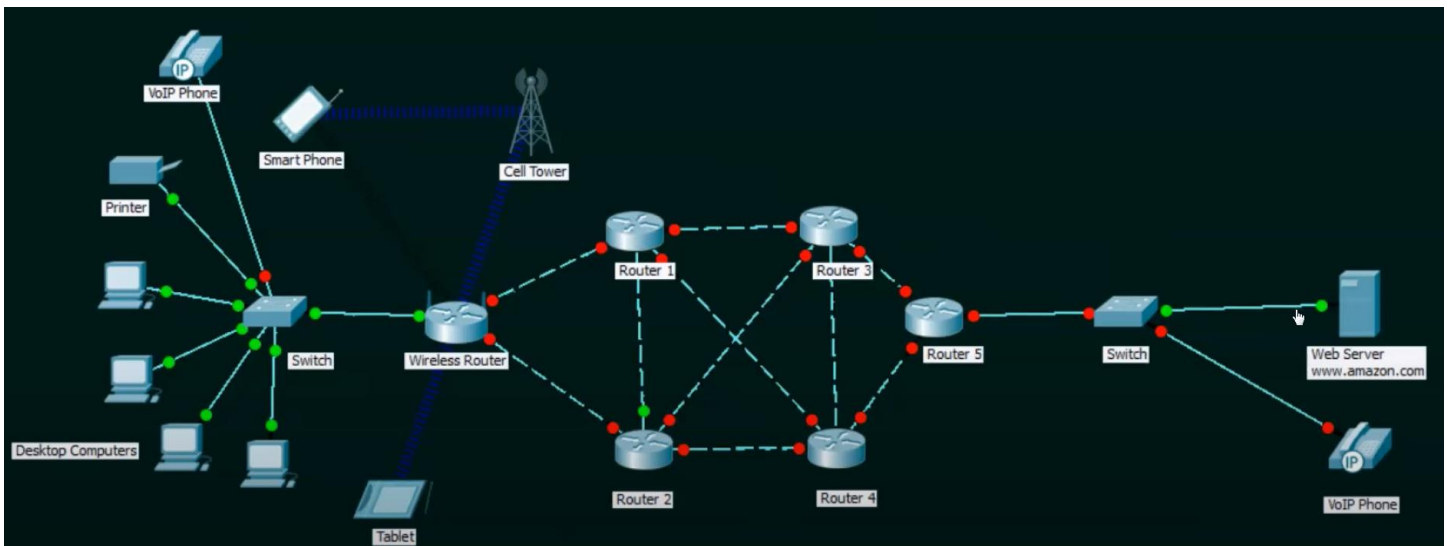
U19CS012

1.) Do Analysis and Understand the Concepts of Networking (Basics).

a.) What is a Computer Network?

An interconnection of multiple devices, also known as **hosts**, that are connected using multiple paths for the purpose of sending/receiving data or media.

Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as **Network devices** and include things such as routers, switches, hubs, and bridges.



BASIC CHARACTERISTICS OF COMPUTER NETWORK

▪ **Fault Tolerance**

The ability to:

1. Continue working despite failures
2. Ensure no loss of service

▪ **Scalability**

The ability to:

1. Grow based on the needs
2. Have good performance after growth

▪ **Quality of Service (QOS)**

The ability to:

1. Set Priorities
2. Manage data traffic to reduce data loss, delay etc.

▪ **Security**

The ability to prevent:

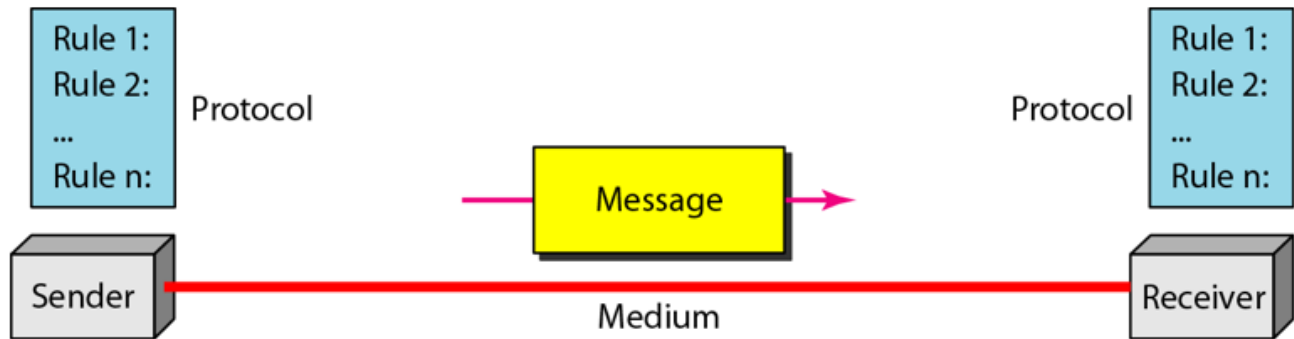
- Unauthorized access
- Misuse
- Forgery

The ability to provide:

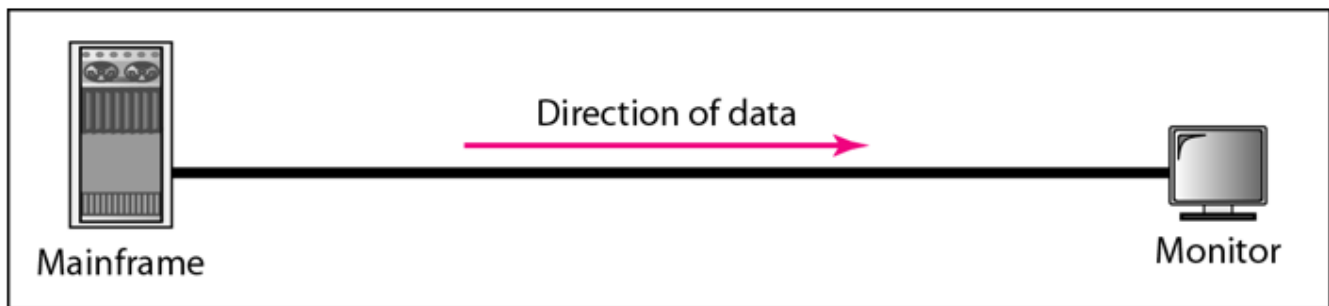
- Confidentiality
- Integrity
- Availability

DATA COMMUNICATION

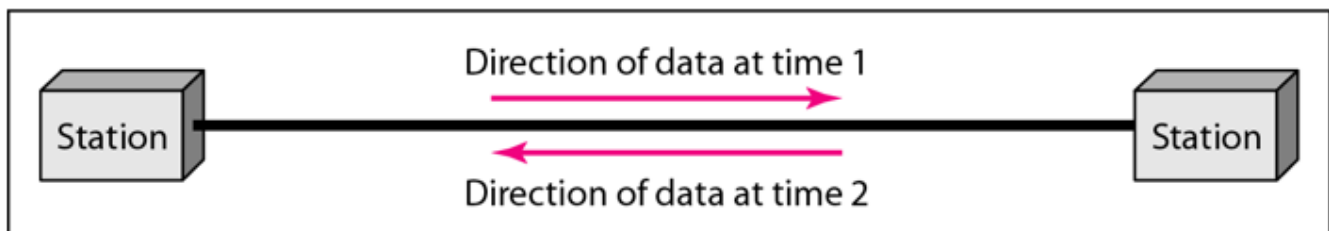
- Data communications are the exchange of data between two nodes via some form of link (transmission medium) such as a cable.



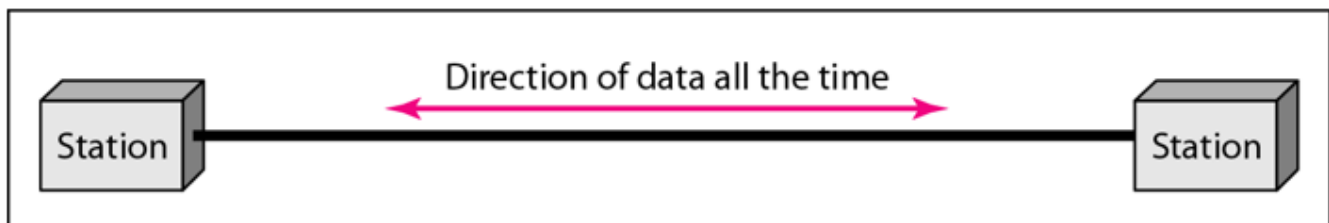
DATA FLOW



a. Simplex



b. Half-duplex



c. Full-duplex

DATA FLOW — SIMPLEX

- Communication is always unidirectional.
- One device can transmit and the other device will receive.

Example: Keyboards, Traditional monitors.

DATA FLOW — HALF DUPLEX

- Communication is in both directions but not at the same time.
- If one device is sending, the other can only receive, and vice versa.

Example: Walkie-Talkies.

DATA FLOW — DUPLEX OR FULL DUPLEX

- Communication is in both directions simultaneously.
- Device can send and receive at the same time.

Example: Telephone line.

PROTOCOLS

All communication schemes will have the following things in common:

- Source or sender
- Destination or receiver
- Channel or media

Rules or protocols govern all methods of communication.

Protocols used in network communications also define:

- Message encoding
- Message formatting and encapsulation
- Message timing
- Message size
- Message delivery options

PEER—TO—PEER NETWORK

- No Centralized administration.
- All peers are equal.
- Simple sharing applications.
- Not scalable.

CLIENT SERVER NETWORK

- Centralized administration.
- Request-Response model.
- Scalable.
- Server may be overloaded.

CLASSIFICATION OF COMPUTER NETWORKS

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

1. LOCAL AREA NETWORK (LAN)

A Local Area Network (LAN) is a computer network that interconnects computers within a mite are such as a residence, school, laboratory, university campus or office building.

LAN - DEVICES

- Wired LAN (Example: Ethernet - Hub, Switch)
- Wireless LAN (Example: Wi-Fi)

2. METROPOLITAN AREA NETWORK (MAN)

A metropolitan area network (MAN) is a computer network that interconnects users with computer resources in a geographic region of the size of a metropolitan area.

MAN- DEVICES

- Switches/Hub
- Routers/Bridges

3. WIDE AREA NETWORK (WAN)

A wide area network (WAN) is a telecommunications network that extends over a large geographical area or the primary purpose of computer networking.

E.g.: End devices and intermediary devices

Basics of Computer Networks

What is a Client?

- A **client** is a computer hardware device or software that accesses a *service* made available by a **server**. The server is often (but not always) located on a separate physical computer.

What is a Server?

- A **server** is a physical computer dedicated to run services to serve the needs of other computers. Depending on the service that is running, it could be a file server, database server, home media server, print server, or web server.

What is a Host?

- A **host** is a computer, connected to other computers for which it provides data or services over a network. In theory, every computer connected to a network acts as a host to other peers on the network. In essence, a host reflects the logical relationship of two or more computers on a network.
- To simplify this, suppose **you want to download an image** from another computer on your network. That computer is “hosting” the image and therefore, it is the host computer. On the other hand, if that same computer downloads an image from your computer, your computer becomes the host computer.
- Your computer can be a **host to other computers**. Likewise, your router can be a host to other routers. But a host must have an assigned IP address. Therefore, modems, hubs, and switches are not considered hosts because they do not have assigned IP addresses.

What is network bandwidth?

- **Network bandwidth** is a measurement indicating the maximum capacity of a wired or wireless communications link to transmit data over a network connection in a given amount of time. Typically, bandwidth is represented in the number of bits, kilobits, megabits or gigabits that can be transmitted in 1 second.

What is jitter?

- Information is transported from your computer in data packets across the internet. They are usually sent at regular intervals and take a set amount of time. **Jitter** is when there is a time delay in the sending of these data packets over your network connection. This is often caused by network congestion, and sometimes route changes

What is a packet?

- In networking, a **packet** is a small segment of a larger message. Data sent over computer networks, such as the Internet, is divided into packets. These packets are then recombined by the computer or device that receives them.
- Suppose **Alice is writing a letter to Bob**, but Bob's mail slot is only wide enough to accept envelopes the size of a small index card. Instead of writing her letter on normal paper and then trying to stuff it through the mail slot, Alice divides her letter into much shorter sections, each a few words long, and writes these sections out on index cards. She delivers the group of cards to Bob, who puts them in order to read the whole message.
- This is similar to how packets work on the Internet. Suppose a user needs to **load an image**. The image file does not go from a web server to the user's computer in one piece. Instead, it is broken down into packets of data, sent over the wires, cables, and radio waves of the Internet, and then reassembled by the user's computer into the original photo

What Does Frame Mean?

- In networking, a **frame** is a unit of data. A frame works to help identify data packets used in networking and telecommunications structures. Frames also help to determine how data receivers interpret a stream of data from a source

What is Local Host?

- When you call an IP address on your computer, you try to contact another computer on the internet but when you call the IP address 127.0.0.1 then you are communicating with the localhost. Localhost is always your own computer. Your computer is talking to itself when you call the localhost.
- **Localhost** can be seen as a server that is used on your own computer.
- Localhost is not just the name for the virtual server but it is also **its domain name**. Just like .example, .test, or .invalid, ., .localhost is a top-level domain reserved for documentation and testing purposes. While accessing the domain, a loopback is triggered. If you access “http://localhost” in the browser, the request will not be forwarded to the internet through the router. It will instead remain in your own system. Localhost has the IP address **127.0.0.1**. This refers back to your own server.

What is Bit Rate?

- We measure that speed using the **bit rate**, the number of bits of data that are sent each second.
- A 10 Mbps connection transfers data at 10 million bits per second.

What is Attenuation?

- **Attenuation** is the loss of signal strength in networking cables or connections.

- This typically is measured in decibels (dB) or voltage and can occur due to a variety of factors.
- It may cause signals to become distorted or indiscernible.
- An example of this is Wi-Fi signal and strength getting noticeably weaker the further that your device is from the router.

What is Distortion?

- **Distortion** is a term used to describe an interruption of transmitting signals that cause an unclear reception.
- Distortion is commonly found in sound generated or received by a computer, video or display signals and data cables such as network cables.

What's difference between The Internet and The Web ?

- The **Internet** is a global network of networks while the Web, also referred formally as World Wide Web (www) is collection of information which is accessed via the Internet.
- Another way to look at this difference is; the **Internet is infrastructure** while the Web is **service** on top of that infrastructure.
- Alternatively, the Internet can be viewed as a big book-store while the Web can be viewed as collection of books on that store.
- At a high level, we can even think of the Internet as hardware and the Web as software!

Here are essential computer network components:

Switches

Switches work as a controller which connects computers, printers, and other hardware devices to a network in a campus or a building.

It allows devices on your network to communicate with each other, as well as with other networks. It helps you to share resources and reduce the costing of any organization.

Routers

Routers help you to connect with multiple networks. It enables you to share a single internet connection with multiple devices and saves money. This networking component acts as a dispatcher, which allows you to analyze data sent across a network. It automatically selects the best route for data to travel and send it on its way.

Access points

Access points allow devices to connect to the wireless network without cables. A wireless network allows you to bring new devices and provides flexible support to mobile users.

Shared Data:

Shared data are data which is shared between the clients such as data files, printer access programs, and email.

Network Interface Card:

Network Interface card sends, receives data, and controls data flow between the computer and the network.

Local Operating System:

A local OS which helps personal computers to access files, print to a local printer and uses one or more disk and CD drives which are located on the computer.

Network Operating System:

The network operating system is a program which runs on computers and servers. It allows the computers to communicate via network.

Protocol:

A protocol is the set of defined rules that allows two entities to communicate across the network. Some standard protocols used for this purpose are IP, TCP, UDP, FTP, etc.

Hub:

Hub is a device that splits network connection into multiple computers. It acts a distribution center so whenever a computer requests any information from a computer or from the network it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network.

LAN Cable:

Local Area Network (LAN) cable is also called as Ethernet or data cable. It is used for connecting a device to the internet.

Unique Identifiers of Network

Below given are some unique network identifiers:

Hostname: Every device of the network is associated with a unique device, which is called hostname.

IP Address:

IP (Internet Protocol) address is as a unique identifier for each device on the Internet. Length of the IP address is 32-bits. IPv6 address is 64 bits.

DNS Server:

DNS stands for Domain Name System. It is a server which translates URL or web addresses into their corresponding IP addresses.

MAC Address:

MAC (Media Access Control Address) is known as a physical address is a unique identifier of each host and is associated with the NIC (Network Interface Card). General length of MAC address is : 12-digit/ 6 bytes/ 48 bits

Port:

Port is a logical channel which allows network users to send or receive data to an application. Every host can have multiple applications running. Each of these applications are identified using the port number on which they are running.

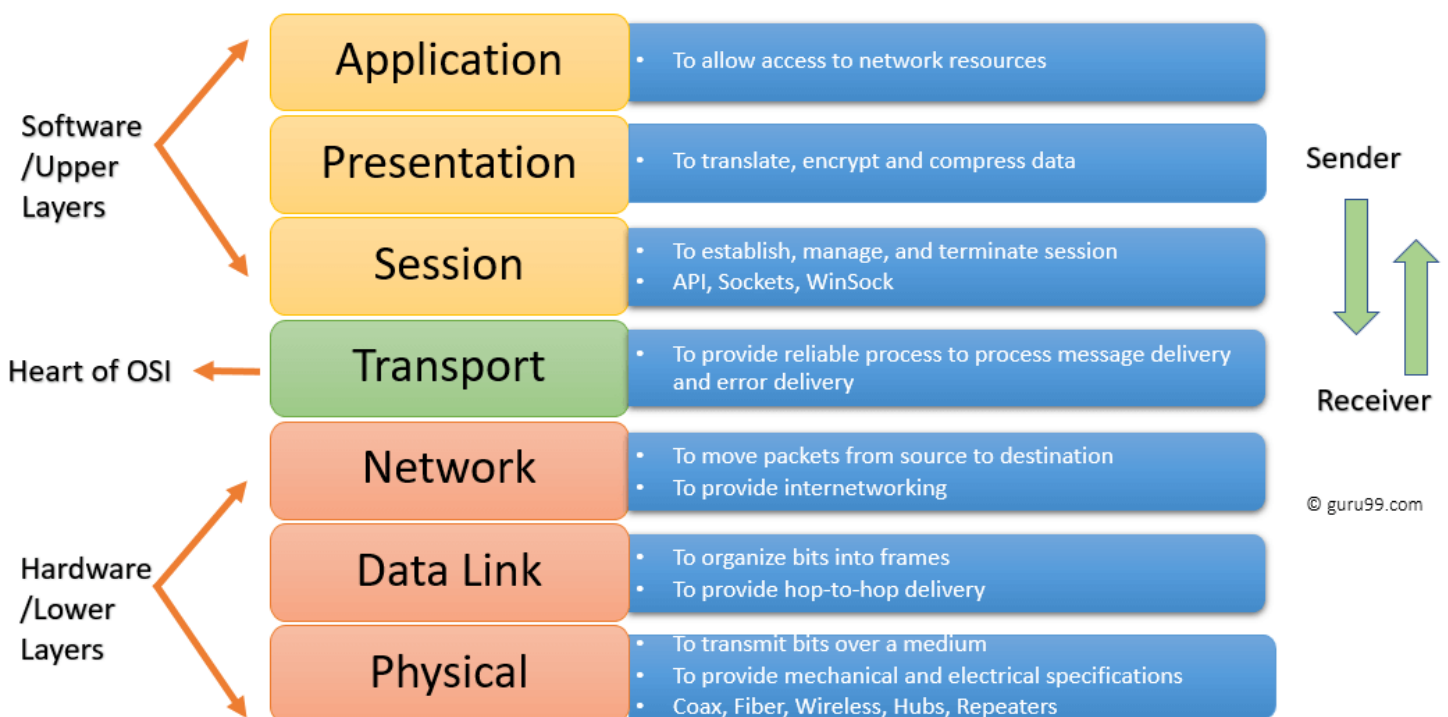
2.) OSI Layers

The OSI Model is a **logical and conceptual model** that defines network communication used by systems open to interconnection and communication with other systems. The Open System Interconnection (OSI Model) also defines a logical network and effectively describes computer packet transfer by using various layers of protocols.

7 Layers of the OSI Model

OSI model is a **layered server architecture** system in which each layer is defined according to a specific function to perform. All these seven layers work collaboratively to transmit the data from one layer to another.

- **The Upper Layers:** It deals with application issues and mostly implemented only in software. The highest is closest to the end system user. In this layer, communication from one end-user to another begins by using the interaction between the application layer. It will process all the way to end-user.
- **The Lower Layers:** These layers handle activities related to data transport. The physical layer and datalink layers also implemented in software and hardware.



Network Layers Diagram

Physical Layer

The **physical layer** helps you to define the electrical and physical specifications of the data connection. This level establishes the relationship between a device and a physical transmission medium. The physical layer is not concerned with protocols or other such higher-layer items.

Examples of hardware in the physical layer are network adapters, Ethernet, repeaters, networking hubs, etc.

Data Link Layer:

Data link layer corrects errors which can occur at the physical layer. The layer allows you to define the protocol to establish and terminates a connection between two connected network devices.

It is IP address understandable layer, which helps you to define logical addressing so that any endpoint should be identified.

The layer also helps you implement routing of packets through a network. It helps you to define the best path, which allows you to take data from the source to the destination.

The data link layer is subdivided into two types of sublayers:

1. Media Access Control (MAC) layer- It is responsible for controlling how device in a network gain access to medium and permits to transmit data.
2. Logical link control layer- This layer is responsible for identity and encapsulating network-layer protocols and allows you to find the error.

Important Functions of Datalink Layer:

- Framing which divides the data from Network layer into frames.
- Allows you to add header to the frame to define the physical address of the source and the destination machine
- Adds Logical addresses of the sender and receivers
- It is also responsible for the sourcing process to the destination process delivery of the entire message.
- It also offers a system for error control in which it detects retransmits damage or lost frames.
- Datalink layer also provides a mechanism to transmit data over independent networks which are linked together.

Transport Layer:

The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine. It is hosted using single or multiple networks, and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

Important functions of Transport Layers:

- It divides the message received from the session layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

Network Layer:

The network layer provides the functional and procedural means of transferring variable length data sequences from one node to another connected in "different networks".

Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Layer-management protocols that belong to the network layer are:

1. routing protocols
2. multicast group management
3. Network-layer address assignment.

Session Layer

Session Layer controls the dialogues between computers. It helps you to establish starting and terminating the connections between the local and remote application.

This layer request for a logical connection which should be established on end user's requirement. This layer handles all the important log-on or password validation.

Session layer offers services like dialog discipline, which can be duplex or half-duplex. It is mostly implemented in application environments that use remote procedure calls.

Important function of Session Layer:

- It establishes, maintains, and ends a session.
- Session layer enables two systems to enter into a dialog
- It also allows a process to add a checkpoint to stream of data.

Presentation Layer

Presentation layer allows you to define the form in which the data is to exchange between the two communicating entities. It also helps you to handles data compression and data encryption.

This layer transforms data into the form which is accepted by the application. It also formats and encrypts data which should be sent across all the networks. This layer is also known as a **syntax layer**.

The function of Presentation Layers:

- Character code translation from ASCII to EBCDIC.
- Data compression: Allows to reduce the number of bits that needs to be transmitted on the network.
- Data encryption: Helps you to encrypt data for security purposes — for example, password encryption.
- It provides a user interface and support for services like email and file transfer.

Application Layer

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means OSI application layer allows users to interact with other software application.

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.

Example of the application layer is an application such as file transfer, email, remote login, etc.

The function of the Application Layers are:

- Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- It allows users to log on to a remote host
- This layer provides various e-mail services
- This application offers distributed database sources and access for global information about various objects and services.

3.) Different Topologies

What is Topology?

Network topologies describe the methods in which all the elements of a network are mapped. The topology term refers to both the physical and logical layout of a network.

Types of Networking Topologies

Two main types of network topologies in computer networks are 1) Physical topology 2) Logical topology

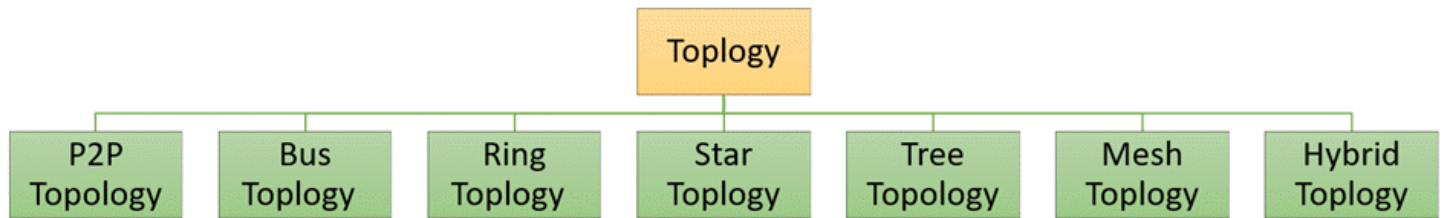
Physical topology:

This type of network is an actual layout of the computer cables and other network devices

Logical topology:

Different types of Physical Topologies are:

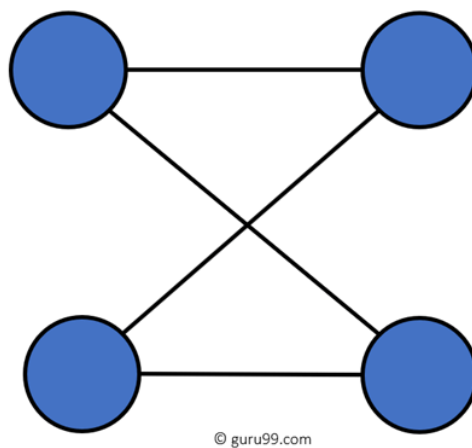
- P2P Topology
- Bus Topology
- Ring Topology
- Star Topology
- Tree Topology
- Mesh Topology
- Hybrid Topology



Network Topology Diagram

Point to Point

Point-to-point topology is the easiest of all the network topologies. In this method, the network consists of a direct link between two computers.



P2P Topology Diagram

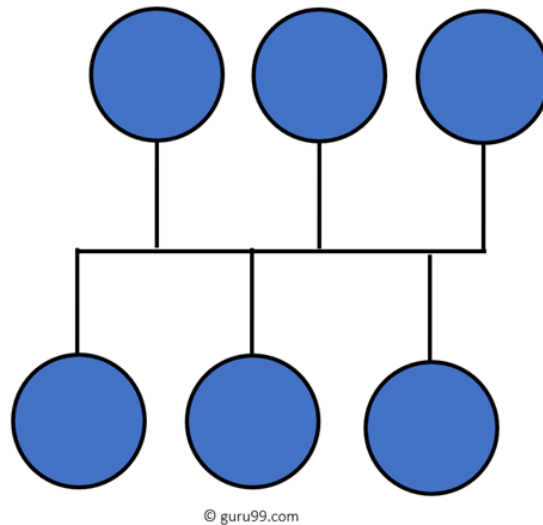
Advantages:

- This is faster and highly reliable than other types of connections since there is a direct connection.
- No need for a network operating system
- Does not need an expensive server as individual workstations are used to access the files
- No need for any dedicated network technicians because each user sets their permissions

Disadvantages:

- The biggest drawback is that it only be used for small areas where computers are in close proximity.
- You can't back up files and folders centrally
- There is no security besides the permissions. Users often do not require to log onto their workstations.

Bus Topology



Bus Topology Diagram

Bus topology uses a single cable which connects all the included nodes. The main cable acts as a spine for the entire network. One of the computers in the network acts as the computer server. When it has two endpoints, it is known as a linear bus topology.

Advantages:

Here are pros/benefits of using a bus topology:

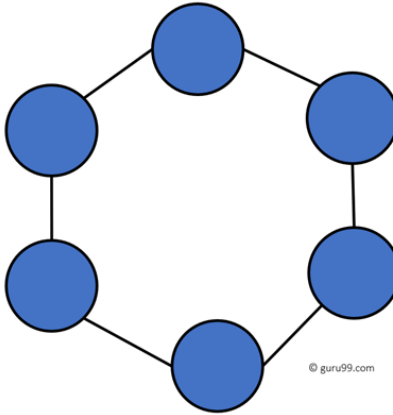
- Cost of the cable is very less as compared to other topology, so it is widely used to build small networks.
- Famous for LAN network because they are inexpensive and easy to install.
- It is widely used when a network installation is small, simple, or temporary.
- It is one of the passive topologies. So computers on the bus only listen for data being sent, that are not responsible for moving the data from one computer to others.

Disadvantages:

Here are the cons/drawbacks of bus topology:

- In case if the common cable fails, then the entire system will crash down.
- When network traffic is heavy, it develops collisions in the network.
- Whenever network traffic is heavy, or nodes are too many, the performance time of the network significantly decreases.
- Cables are always of a limited length.

Ring Topology



Ring Topology Diagram

In a ring network, every device has exactly two neighboring devices for communication purpose. It is called a ring topology as its formation is like a ring. In this topology, every computer is connected to another computer. Here, the last node is combined with a first one.

This topology uses token to pass the information from one computer to another. In this topology, all the messages travel through a ring in the same direction.

Advantages:

Here are pros/benefits of ring topology:

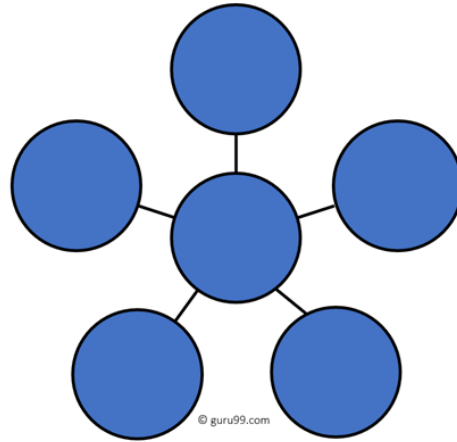
- Easy to install and reconfigure.
- Adding or deleting a device in-ring topology needs you to move only two connections.
- The troubleshooting process is difficult in a ring topology.
- Failure of one computer can disturb the whole network.
- Offers equal access to all the computers of the networks
- Faster error checking and acknowledgment.

Disadvantages:

Here are drawbacks/cons of ring topology:

- Unidirectional traffic.
- Break in a single ring can risk the breaking of the entire network
- Modern days high-speed LANs made this topology less popular.
- In the ring, topology signals are circulating at all times, which develops unwanted power consumption.
- It is very difficult to troubleshoot the ring network.
- Adding or removing the computers can disturb the network activity.

Star Topology



Star Topology Diagram

In the star topology, all the computers connect with the help of a hub. This cable is called a central node, and all other nodes are connected using this central node. It is most popular on LAN networks as they are inexpensive and easy to install.

Advantages:

Here are pros/benefits of star topology:

- Easy to troubleshoot, set up, and modify.
- Only those nodes are affected, that has failed. Other nodes still work.
- Fast performance with few nodes and very low network traffic.
- In Star topology, addition, deletion, and moving of the devices are easy.

Disadvantages:

Here are cons/drawbacks of using Star:

- If the hub or concentrator fails, attached nodes are disabled.
- Cost of installation of star topology is costly.
- Heavy network traffic can sometimes slow the bus considerably.
- Performance depends on the hub's capacity
- A damaged cable or lack of proper termination may bring the network down.

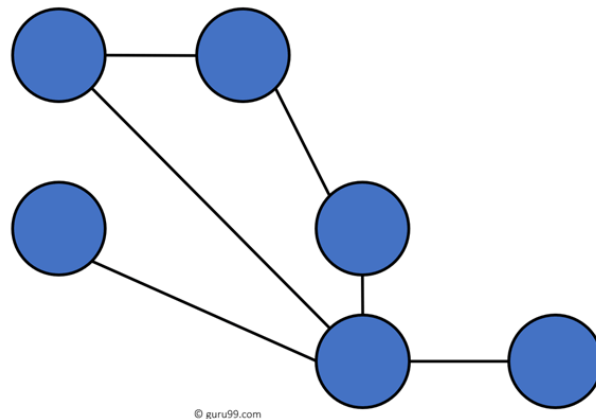
Mesh Topology

The mesh topology has a unique network design in which each computer on the network connects to every other. It develops a P2P (point-to-point) connection between all the devices

of the network. It offers a high level of redundancy, so even if one network cable fails, still data has an alternative path to reach its destination.

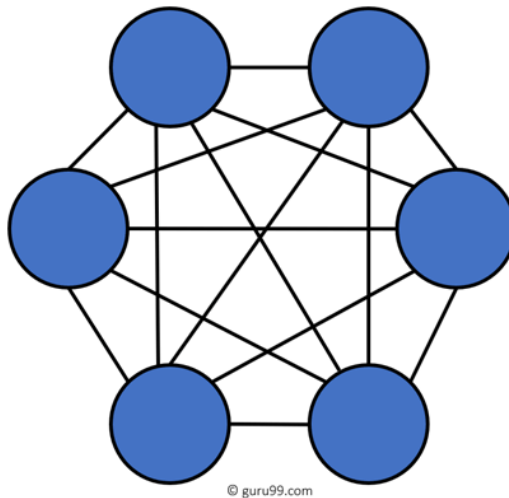
Types of Mesh Topology:

- **Partial Mesh Topology:** In this type of topology, most of the devices are connected almost similarly as full topology. The only difference is that few devices are connected with just two or three devices.



Partially Connected Mesh Topology

- **Full Mesh Topology:** In this Topology every nodes or device are directly connected with each other.



Fully Connected Mesh Topology

Advantages:

Here, are pros/benefits of Mesh topology

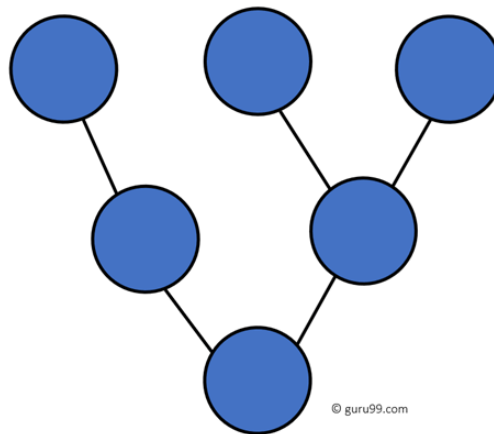
- The network can be expanded without disrupting current users.
- Need extra capable compared with other LAN topologies.

- Complicated implementation.
- No traffic problem as nodes has dedicated links.
- It has multiple links, so if any single route is blocked, then other routes should be used for data communication.
- P2P links make the fault identification isolation process easy.
- It helps you to avoid the chances of network failure by connecting all the systems to a central node.

Disadvantages:

- Installation is complex because every node is connected to every node.
- Dedicated links help you to eliminate the traffic problem.
- A mesh topology is robust.
- Every system has its privacy and security
- It is expensive due to the use of more cables. No proper utilization of systems.
- It requires more space for dedicated links.
- Because of the amount of cabling and the number of input-outputs, it is expensive to implement.
- It requires a large space to run the cables.

Tree Topology



Tree Topology

Tree topologies have a root node, and all other nodes are connected which form a hierarchy. So it is also known as hierarchical topology. This topology integrates various star topologies together in a single bus, so it is known as a Star Bus topology. Tree topology is a very common network which is similar to a bus and star topology.

Advantages:

Here are pros/benefits of tree topology:

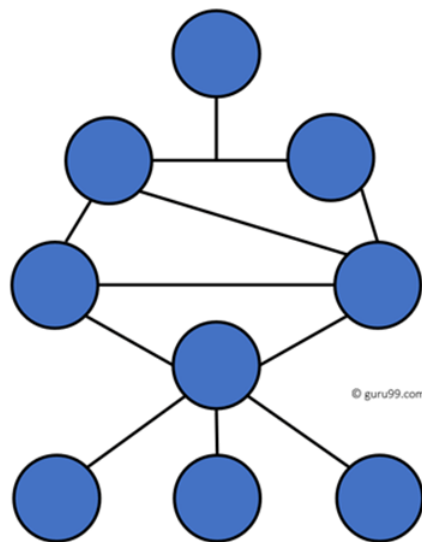
- Failure of one node never affects the rest of the network.
- Node expansion is fast and easy.
- Detection of error is an easy process
- It is easy to manage and maintain

Disadvantages:

Here are cons/drawback of tree topology:

- It is heavily cabled topology
- If more nodes are added, then its maintenance is difficult
- If the hub or concentrator fails, attached nodes are also disabled.

Hybrid Topology



Hybrid Topology

Hybrid topology combines two or more topologies. You can see in the above architecture in such a manner that the resulting network does not exhibit one of the standard topologies.

For example, as you can see in the above image that in an office in one department, Star and P2P topology is used. A hybrid topology is always produced when two different basic network topologies are connected.

Advantages:

Here, are advantages/pros using Hybrid topology:

- Offers the easiest method for error detecting and troubleshooting
- Highly effective and flexible networking topology

- It is scalable so you can increase your network size

Disadvantages:

- The design of hybrid topology is complex
- It is one of the costliest processes

4.) What is the Significance of Computer Network?

- Helps you to connect with multiple computers together to send and receive information when accessing the network.
- Helps you to share printers, scanners, and email.
- Helps you to share information at very fast speed
- Electronic communication is more efficient and less expensive than without the network.
- Helps you to share resource such as printers
- Allows you to share expensive software's and database among network participants
- Provides fast and effective communication from one computer to another computer
- Helps you to exchange data and information among users via a network.

It acts as basis of communication in Information Technology (IT).

- ✓ Provides best way of business communication.
- ✓ Streamline communication.
- ✓ Cost-effective resource sharing.
- ✓ Improving storage efficiency and volume.
- ✓ Cut costs on software & hardware.
- ✓ Utilizes Centralized Database.
- ✓ Increase in efficiency.
- ✓ Optimize convenience and flexibility.
- ✓ Allows File sharing.
- ✓ Sharing of peripherals and internet access. [Overcoming geographic separation]
- ✓ Network gaming.
- ✓ Voice over IP (VoIP).
- ✓ Media Center Server.
- ✓ Centralize network administration, meaning less IT support.
- ✓ Flexibility.
- ✓ Allowing information sharing.
- ✓ Supporting distributed processing.
- ✓ User communication.