Chapter -3: Network Topology

The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology.

Or

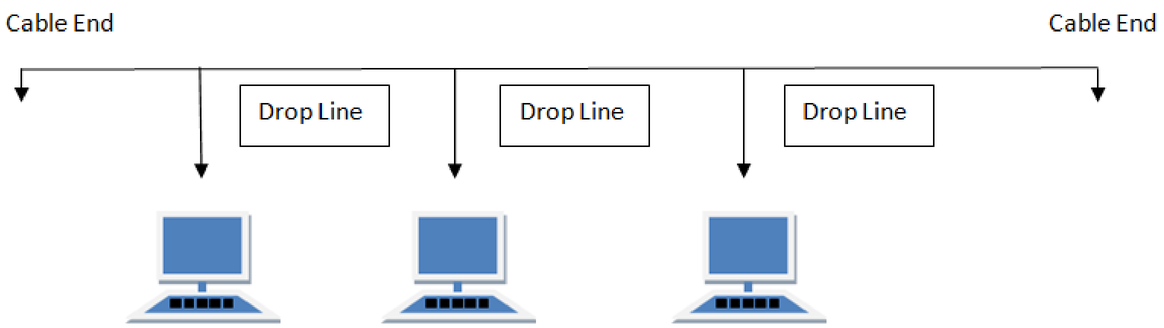
A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

➢ 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.

In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.



Features of Bus Topology

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

Advantages of Bus Topology

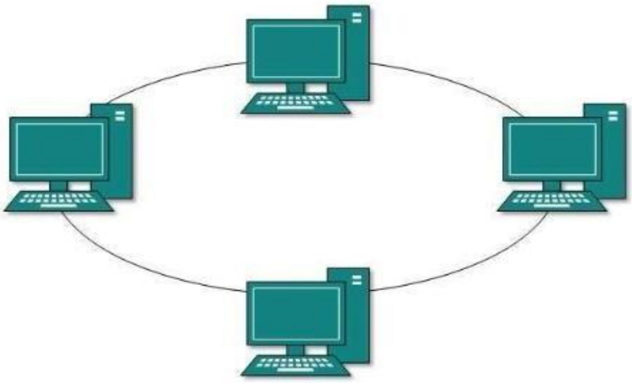
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. 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 neighbours for each device.



Features of Ring Topology

1. 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.

2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.
3. 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.
4. 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

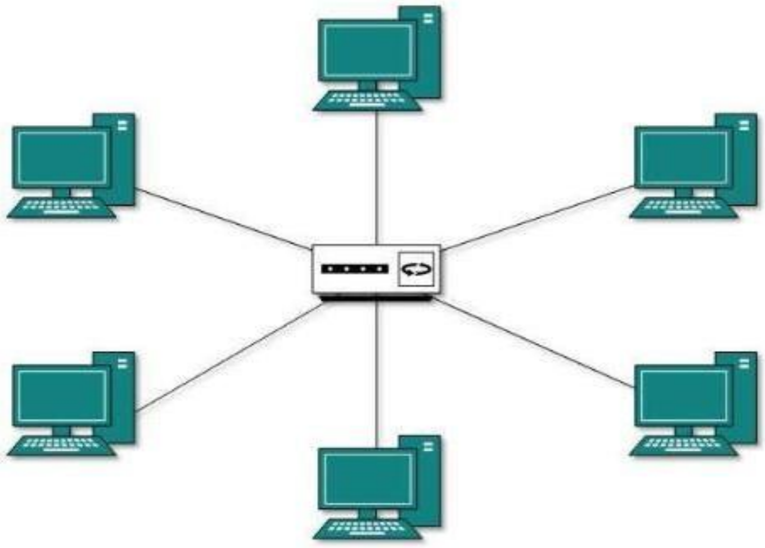
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.

➢ 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.



All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway

Features of Star Topology

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

Advantages of Star Topology

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

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. 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 :

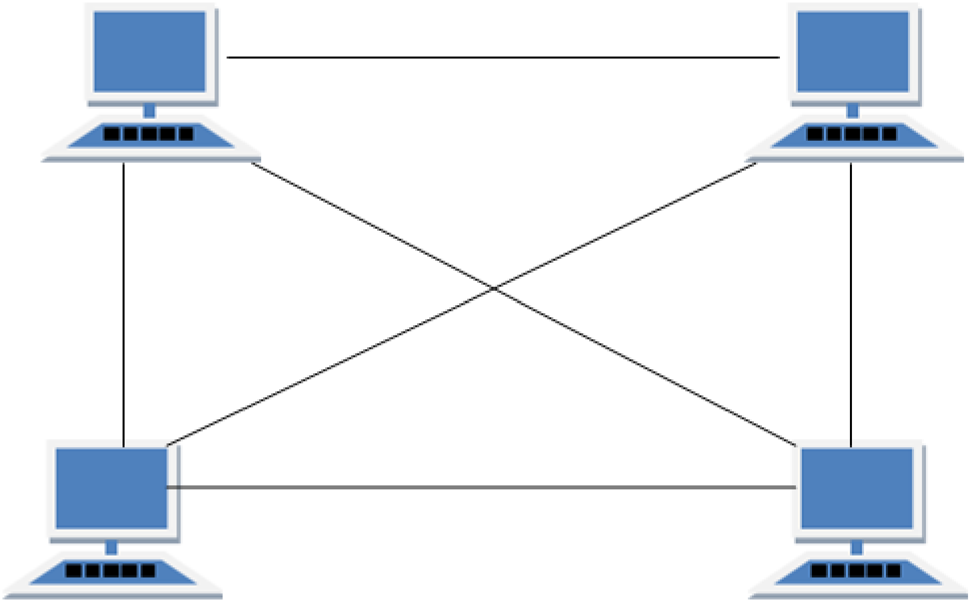
1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

1. **Partial Mesh Topology**: In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology**: Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.

3. Not flexible.

Advantages of Mesh Topology

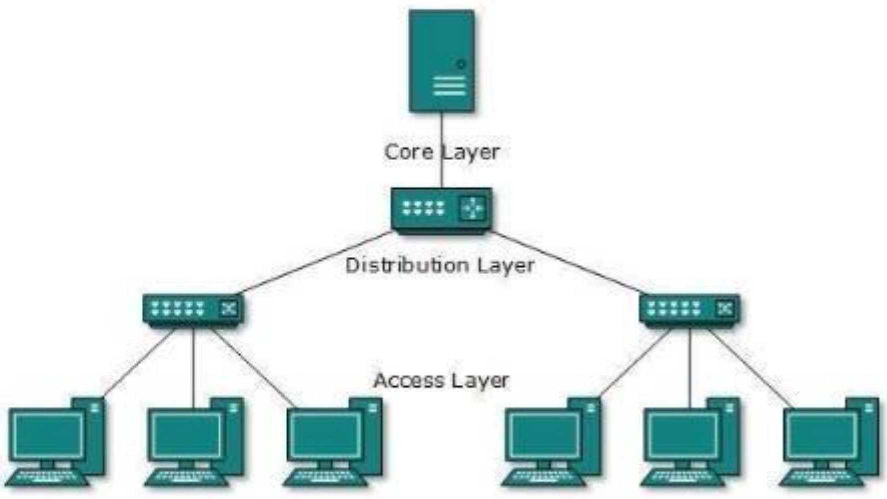
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. 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.



This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.

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

Features of Tree Topology

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

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

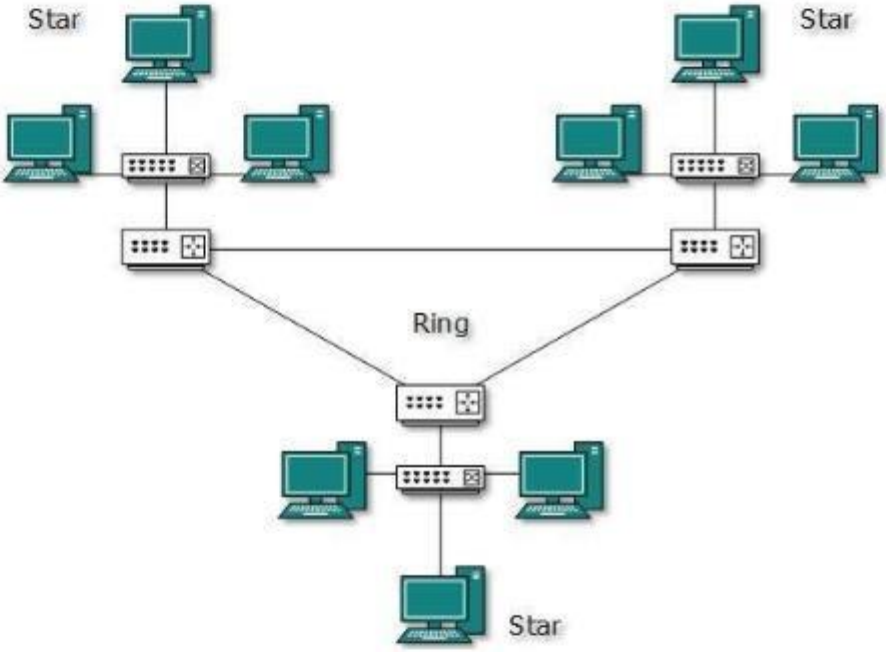
Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. 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).

The below diagram represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology



Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

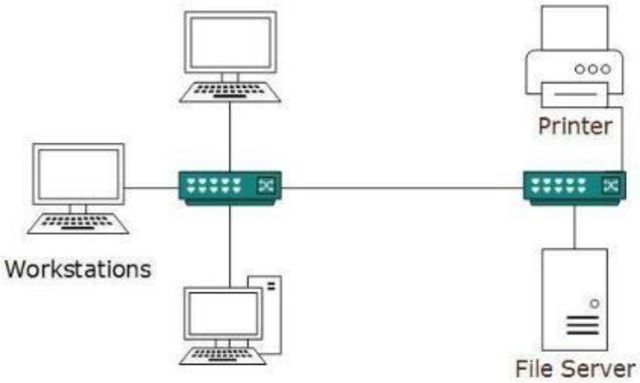
Network Types

Local Area Network(LAN)

LAN or Local Area Network links network devices in such a way that personal computer and workstations can share data, tools and programs. Data transmits at a very fast rate as the number of computers linked are limited. LAN's cover a smaller geographical area and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain.

A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized. LAN can be configured in the ring, bus and star topology. The ring topology is prevalent in the Token Ring LANs of IBM and bus is widespread in Token Bus and Ethernet LANs.

It is a broadcast network where the message is sent to all the connected hosts as all the host share the same transmission medium (wire). Broadcasting can be done in two ways statically and dynamically. In the **static technique**, the hosts are provided with a definite time slice for transmitting the information. While in the **dynamic method** the hosts can flexibly send the frame at any particular time.



Applications of LAN

- The first application of the LAN network is that it can be easily implemented as a server-client model network. For Example, In a university, suppose all the hosts are connected through LAN, then one of the PC can be converted into Server and all the other PC's will be clients which can have access to the data stored on the client computers.
- As all the workstations are connected locally, if they want to pass on some internal communication, then each node can communicate with one another without having any internet connection.
- The resources like printers, hard-disk, and FAX machine can publicly use all the nodes in LAN networks.

- Software testers can also use LAN network for sharing their testing tools within an office or within a factory using the client-server model of the networking system. The software can be put on one centralized server whose data is made accessible by all the client PCs with the help of a local administrator.

Advantages of LAN

- In an office which is connected via LAN network, we can share the hardware and software resources like printers, FAX, drivers and hard-disk as they are on one platform and thus this type of network turns out to be cost-effective.
- As being connected on the network, the offices or firms using the same type of software for job purposes need not purchase separately for each of the host clients as the software can easily be shared with everyone on an equal level.
- LAN network works as a client-server model, therefore data can be stored centrally on one PC called as a server in a network and it can be accessible to all the other client PC's via LAN. By following this method, we need not store data locally at one single node.
- Communication will be handy and economical by using LAN network.
- Internet cafe owners use the LAN network to provide internet connections to multiple nodes and users connected via a single internet connection. This makes the use of the internet a cost-effective one.

Disadvantages of LAN

- LAN networks come out to be cost-effective and time-saving, as we can share various resources on one platform. However, the initial installation cost of the network is very high.
- It is having a geographical area limitation and can only cover a small area (1-5 km).
- As it works on a single cable, if it gets faulty then the overall network will stop working. Hence, it needs a full -time maintenance officer called an administrator.
- Crucial Data of offices or factories is saved on a single server which can easily be accessible by all the nodes thus it is having all time data security issues as any unauthorized person can also access the confidential data.

Metropolitan Area Network(MAN)

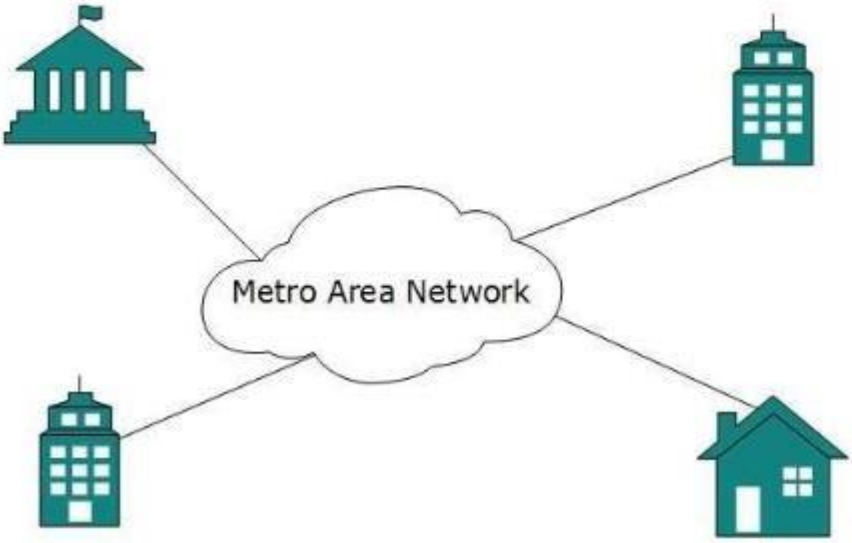
MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). It's hard to design and maintain a Metropolitan Area Network.

Types of MAN

MAN can be categorised into two types: DQDB and SMDS.

DQDB (Distributed Queue Dual Bus): It is considered as a dual bus configuration refers that each host in the network would be linked to the two backbone network lines.

SMDS (Switched Multimegabit Data Services): SMDS connects different LANs and permits packets to transfer to any other LAN on the SMDS. It is a high-speed MAN which uses packet switching as a datagram service.



Advantages of MAN

Given below are the various advantages of MAN:

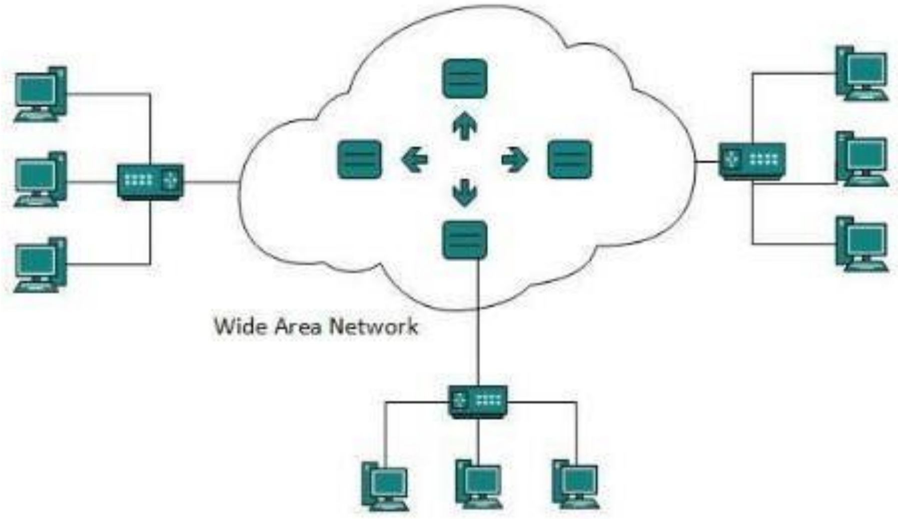
- It is very efficient and swift for communication over fiber optic cable for interconnection of networks in cities.
- It serves many villages and cities and thus provides great inter-connectivity at a low cost.
- It works on ring or bus topology with a protection link, thus data can be transmitted or received simultaneously over nodes and if one link fails the other will keep the network live.

Disadvantages of MAN

The disadvantages of MAN are:

- Depending upon the distance between two nodes, the cable length required for inter-connection differs every time. Thus greater will be the cable length, the more will be the cost of the network.
- Security is a big concern for this network as for such a big distance anyone can hack the network. We can’t put security at each level of the network, hence it becomes easier for unwanted people to access it for their own benefits.

Wide Area Network (WAN)



WAN is widely used in long-distance communication systems.

It covers bigger areas i.e right from a state to a country. Therefore the geographical area it covers is from 100 to several 1000 km. WAN networks are complex in nature, however, they are widely used in mobile communications as they cover up long distances.

Generally, fiber optic cable is used as a media for transmission in this system. WAN works on physical, data-link and network layers of the OSI Reference model.

Routers are used in WAN network for communication as they provide the shortest path for communication over long distance using routing tables. Routers also provide a secure and fast rate of transmission.

Different types of data need to be transmitted over the network like image, voice, video and data files. Therefore the routers use packet switching technique for sending and receiving data between nodes. It is not necessary that the device used should be a router only, other devices such as switches, bridges etc., are also used for connectivity.

Routers have routing tables by which they learn the host and destination address for delivery of the data packet and that in turn is the shortest path for transmission. By following this mechanism a source end router will communicate with the far end destination router and exchange the data packets.

Routers and switches have internal memories. Thus when a data packet has arrived at a switch node for delivery, it uses to store and forward the technique for data transmission.

The WAN network can be of two types:

1. **Wired WAN** – This uses OFC as the media for communication
2. **Wireless WAN** – Satellite communication is a type of WAN network.

Advantages of WAN

Given below are the various advantages of WAN:

- It connects various cities and states with one another. Hence, large scale industries can be connected to one single network.
- N number of nodes can be connected over this network for sharing software.
- As routers are used for sending and receiving the end of the network, the rate of transmission is very high even if we send large sized files of more than 10 MB.
- All users connected via WAN will remain in synchronization with each other at all the time, therefore, there will be no chances of communication gap between them.
- The users can share the hardware like printers, hard-disk etc. with each other and there is no need to buy a separate connection for internet as all type of communication can be done within as they are being on one network only.

Disadvantages of WAN

The disadvantages of WAN are:

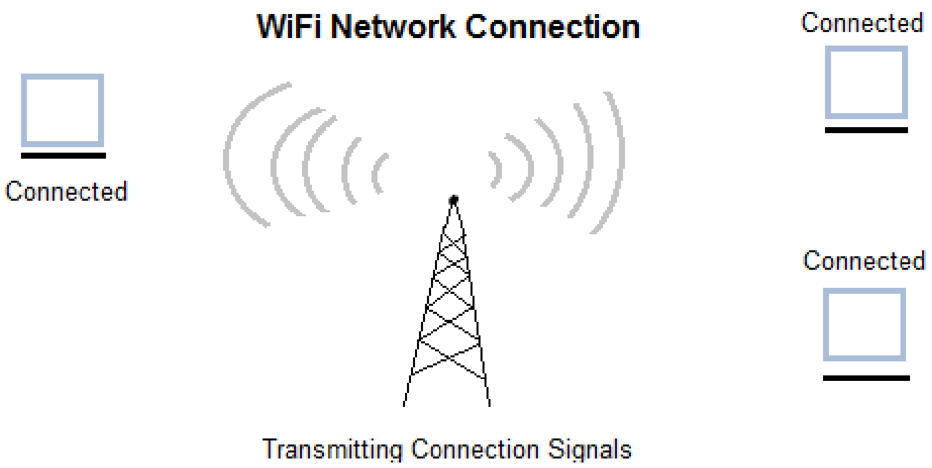
- Confidential and important data is shared over a long distance, hence there are chances for unwanted people to try to interrupt and hack the data. Therefore there is always a need to purchase a security firewall for the network to protect it from the outside threats.
- Set-up of WAN network is complex and costly.
- As WAN network is spread over a very large distance, we need to deploy a local administrator at every intermediate point to ensure its maintenance and fault control.

- Local monitoring of such wide networks is not sufficient enough to maintain it properly. Therefore, some companies, like mobile operators will set up a NOC and purchase a GUI based centralized monitoring tool for operation and maintenance purpose. This will cost them a lot of manpower and money for running it smoothly.

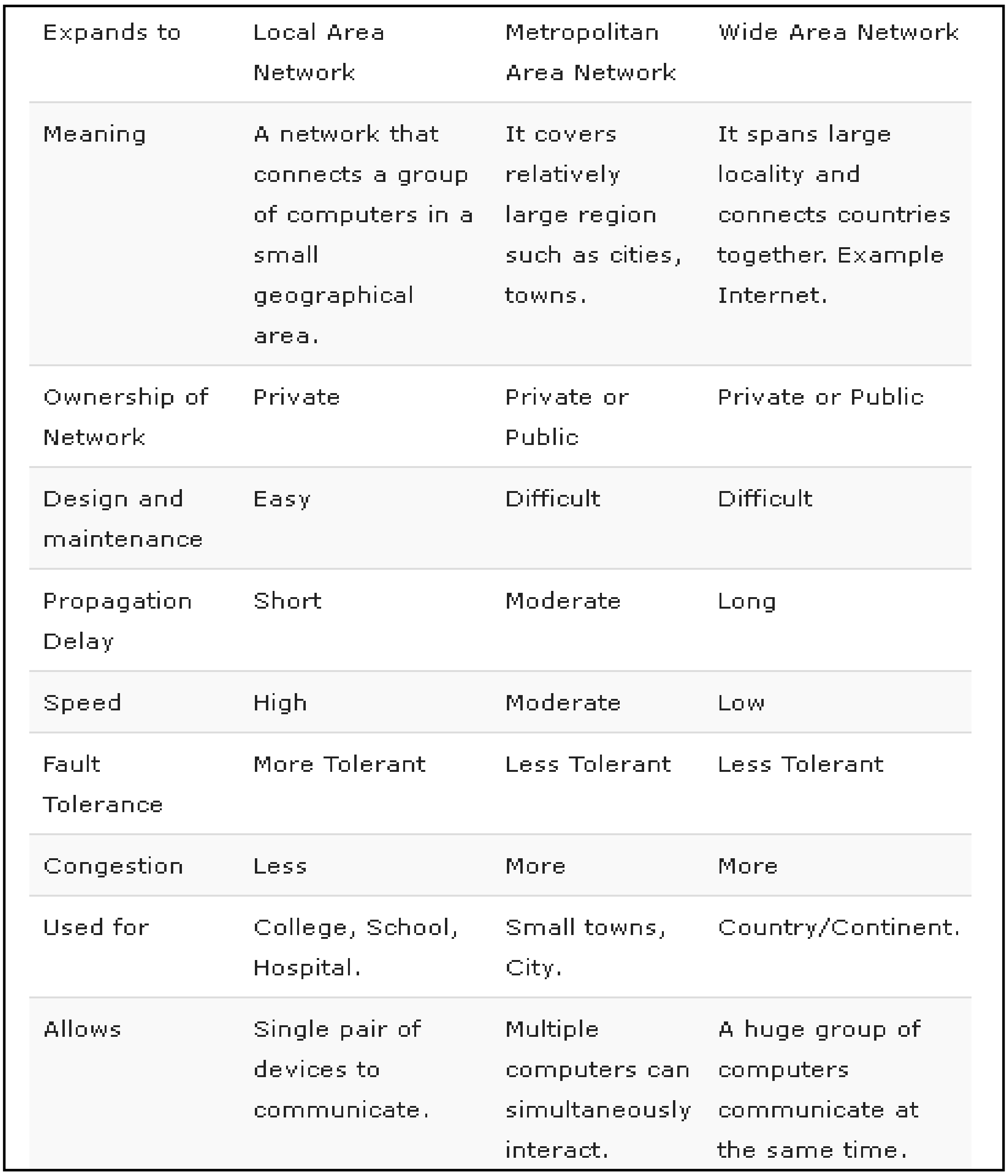
Wireless WANs

The radio network used for cellular telephones is an example of a low-bandwidth wireless WAN. This system has already gone through three generations.

- The first generation was analog and for voice only.
- The second generation was digital and for voice only.
- The third generation is digital and is for both voice and data.



Difference Between LAN, MAN and WAN



Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.
Allows	Single pair of devices to communicate.	Multiple computers can simultaneously interact.	A huge group of computers communicate at the same time.

Key Differences Between LAN, MAN and WAN

1. The geographical area covered by LAN is small, whereas, MAN covers relatively large and WAN covers the greatest of all.
2. LAN is confined to schools, hospitals or buildings, whereas, MAN connects small towns or Cities and on the other hand, WAN covers Country or a group of Countries.
3. Devices used for transmission of data are-
   LAN: WiFi, Ethernet Cables.
   MAN: Modem and Wire/Cable
   WAN: Optic wires, Microwaves, Satellites.

4. LAN’s transmit data at a faster rate than MAN and WAN.
5. Maintenance of LAN is easier than that of MAN and WAN.
6. The bandwidth available for transmission is higher in LAN than MAN and WAN.
7. Data transmission errors and noise are least in LAN, moderate in MAN and high in WAN.

Steps Involved in Designing a Network

Making a computer network is based upon its working environment whether it is home and small business or comparatively bigger canvas. When and how this concept of computer networking evolved? You can comprehend it as in an office environment when one need to connect with the other without leaving the place then the concept of LAN appears. To learn about how to make computer network we have to know about the types first.

➢ Planning Computer Network Types

LAN stands for local area network. It makes the work quick and easy. Now the branch of the same office started working in another area of city. They also need to communicate with each other. It is very difficult to leave the work and go to the other branch. If you left the office after finishing the work, still it is hectic to spend extra time for taking report of the other office as well. So the solution comes in the shape of MAN.

MAN stands for metropolitan area network and an authentic way to get data from the other branch at the same time while there is no need to leave your place. As per demand of the intercity connectivity WAN comes as a helping hand It helps to connect the branches of the same office situated at different cities.

WAN is for wide area network and it facilitates to receive the data on your spot. First of all this networking was supported by one server. This server connects to the other server in another country and ultimately a web developed into a world wide web (www). And now you can connect through internet anywhere and anytime to receive the required information.

➢ Selecting Computer Network Infrastructure

It is necessary to talk about the two options used to create these networks. These two choices are wired network and wireless network. Basically it is the game of accessibility and possibility hence wireless is more convenient and effective than wired networking.

➢ Selecting right Computer Network Topology

Then there are different topologies according to which you have to adopt your networking. Working in a LAN environment Liner bus topology is the easiest one. The plus point of this topology is that it won't cover larger space and negative point is that in case of main cable failure whole system stops working.

Also ring topology could be used in LAN environment working clockwise or anticlockwise but the problem is same as in bus topology.

Star topology is suggested in home and small business environment within LAN. It has an edge over bus and ring topologies because there is no threat of system failure if one computer fails to work suddenly. Still numbers of computers are limited in all these topologies.

As per WAN networking, being covered a wide region it need a specific topology like tree or mesh. Tree topology is the combination of bus and star topologies. It enables to work independently to every computer while attaching with the server. In tree topology many stars are interconnected by using the backbone model of bus topology. So there is an increase in the basic equipment but with more security and convenience. Keeping the process of photosynthesis in mind you can better understand its function. As every individual leaf is able to prepare food so is the case with every computer attach to it. In case of breaking one leaf or even a branch others remain in working condition, this tree topology works in the same way.

Mesh topology is the latest networking design basic and works like a router by detecting its range and adopt the safe and quick way to deliver message direct to the selective computer.

As topologies are the basic components of computer network its understanding is necessary before designing a computer network. Next step is the selection of networking mode whether it is better to have peer-to-peer network or server-client network. In peer-to-peer networking computers are directly connected and can be shared only if the designated computer from where data has to share is on. Client-server networking is more function and useful because every computer is directly attached to the server. This type of networking enables everyone to keep files, data, and important information on the server and any relevant person can access it through this networking.

➢ Devices & Components used in Computer Network

All types of computer network designs are based on same apparatus like server, hub, switch, router, and network adaptor. These network adaptors are now-a-days inbuilt in all the machines desired to be shared in networking. In peer-to-peer network only network cable is attached through the RJ45 port commonly known as NIC card and these two computers are making a network through cross cable. One computer works as a server. While in client-server network, a server is the main component of networking. First of all install a server operating system. After the installation of server software it is ready to access the clients. All the clients are added one by one in the server directory with the help of an IP address for making a closed network. Any computer wants to be the part of that network need an IP address for accessing the data.

- **Survivability**

Network survivability enables the network to maintain maximum network connectivity and quality of service under failure conditions. It has been one of the critical requirements in network planning and design. It involves design requirements on topology, protocol, bandwidth allocation, etc.

- **Security and Protection**

Various Protocols should be used to secure the network

There are a wide variety of tools available for network planning and design depending on the technologies being used. These include:

1. OPNET
2. NetSim

Software Design Issues

In this section we'll examine four software issues that must be addressed by network designers:

- How do sites use addresses to locate other sites?
- How are messages routed and how are they sent?
- How do processes communicate with each other?
- How are conflicting demands for resources resolved?

1. Addressing Conventions

Network sites need to determine how to uniquely identify their users, so they can communicate with each other and access each other's resources. Names, addresses, and routes are required because sites aren't directly connected to each other except over point-to-point links; therefore, addressing protocols are closely related to the network topology and geographic location of each site.

Using an Internet address as a typical example, we can see that it follows a hierarchical organization, starting from left to right in the following sequence: from logical user to host machine, from host machine to net machine, from net machine to cluster, and from cluster to network.

For example, in each Internet address— **someone@icarus.lis.pitt.edu** or **igss12@aber.ac.uk**—the periods are used to separate each component. These electronic mail addresses, which are fairly easy to remember, must be translated to corresponding hardware addresses. This conversion is done by the networking section of the computer's operating system.

The examples given above follow the Domain Name Service (DNS) protocol, a general-purpose distributed data query service whose principal function is the resolution of Internet addresses. If we dissect someone@icarus.lis.pitt.edu into its components, we have the following:

- someone is the logical user,
- icarus is the host for the user called someone,
- lis is the net machine for icarus,
- pitt is the cluster for lis, and
- edu is the network for the University of Pittsburgh.

Not all components need to be present in all Internet addresses. Nevertheless, the DNS is able to resolve them by examining each one in reverse order.

2. Routing Strategies

A router is an internetworking device, primarily software driven, which directs traffic between two different types of LANs or two network segments with different protocol addresses. It operates at the network layer.

Routing allows data to get from one point on a network to another. To do so, each destination must be uniquely identified. Once the data is at the proper network, the router makes sure that the correct node in the network receives it.

Two of the most widely used routing protocols in the Internet are routing information protocol and open shortest path first.

Routing Information Protocol: In routing information protocol (RIP), selection of a path to transfer data from one network to another is based on the number of intermediate nodes, or hops, between the source and the destination. The path with the smallest number of hops is always chosen. This distance vector algorithm is easy to implement, but it may not be the best in today’s networking environment because it does not take into consideration other important factors such as bandwidth, data priority, or type of network. That is, it can exclude faster or more reliable paths from being selected just because they have more hops.

When a process at site A wants to communicate with a process at site B, how is the message sent? If there is only one physical path from A to B, the message must be sent through that path. However, if there are multiple physical paths from A to B, then several routing options exist. Each site has a routing table indicating the alternative paths that can be used to send a message to other sites. The table may include information about the speed and cost of the various communication paths, and it may be updated as necessary, either manually or via programs that exchange routing information. The three most common routing schemes are fixed routing, virtual routing and dynamic routing.

Fixed routing: A path from A to B is specified in advance and does not change unless a hardware failure disables it. Usually, the shortest path is chosen, so that communication costs are minimized.

Virtual routing: A path from A to B is fixed for the duration of one session. Different sessions involving messages from A to B may use different paths. A session could be as short as a file transfer or as long as a remote-login period.

Dynamic routing: The path used to send a message from site A to site B is chosen only when the message is sent. Because the decision is made dynamically, separate messages may be assigned different paths. Site A will make a decision to send the message to site C. C, in turn, will decide to send it to site D, and so on. Eventually, a site will deliver the message to B. Usually, a site sends a message to another site on whatever link is the least used at that particular time.

Open Shortest Path First

In open shortest path first (OSPF), selection of a transmission path is made only after the state of a network has been determined so that if an intermediate hop is malfunctioning, it's eliminated immediately from consideration until its services have been restored. Routing update messages are sent only when changes in the routing environment occur, thereby reducing the number of messages in the internetwork and reducing the size of the messages by not sending the entire routing table. However, memory usage is increased because OSPF keeps track of more information than RIP. In addition, the savings in bandwidth consumption are offset by the higher CPU usage needed for the calculation of the shortest path, which is based on Dijkstra's algorithm, simply stated as find the shortest paths from a given source to all other destinations by proceeding in stages and developing the path in increasing path lengths.

3. Packet Strategies

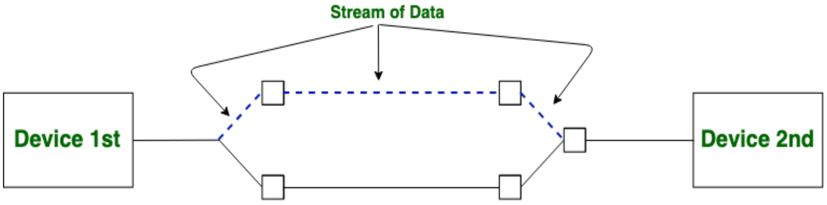
Messages generally vary in length. To simplify the system design, we commonly implement communication with fixed-length messages called **packets, frames or datagrams**. A communication implemented in one packet can be sent to its destination in a **connectionless message**. A connectionless message can be unreliable, in which case the sender has no guarantee that, and cannot tell whether, the packet reached its destination. Alternatively, the packet can be reliable. Usually, in this case, an acknowledgement packet is returned from the destination indicating that the original packet arrived.

Connection Oriented Services: There is a sequence of operation to be followed by the users of connection oriented service. These are:

1. Connection is established.
2. Information is sent.
3. 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.

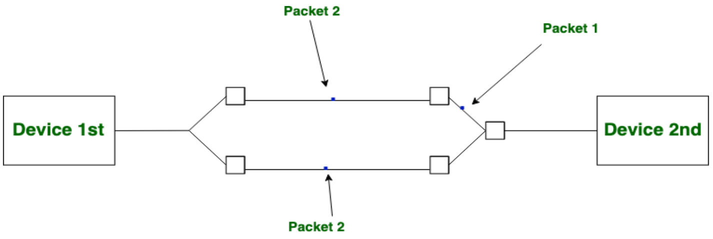


CONNECTION-ORIENTED SERVICE

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.



CONNECTIONIESS SERVICE

4. Connection Models

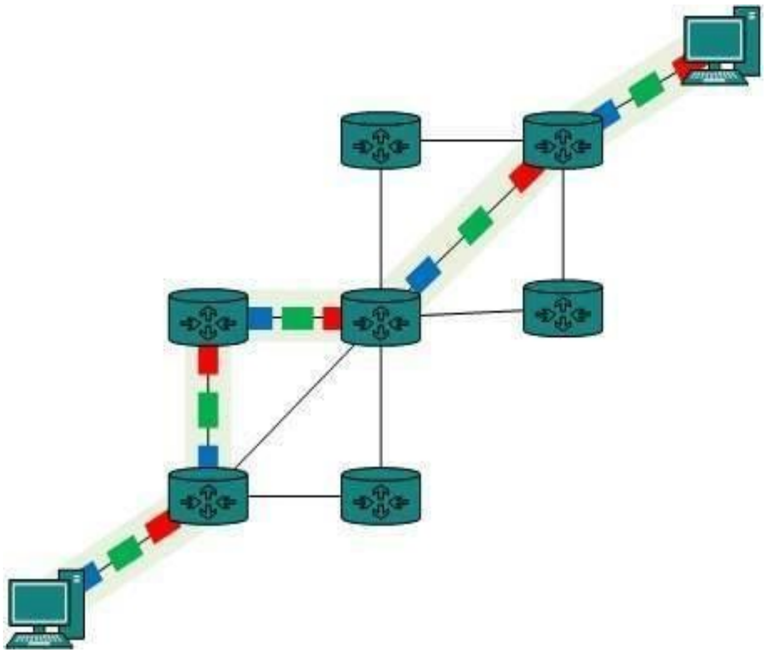
Once messages are able to reach their destinations, processes can institute communications sessions to exchange information. Pairs of processes that want to communicate over the network can be connected in a number of ways. The three most common schemes are circuit switching, message switching and packet switching.

- **Circuit Switching**

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

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

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

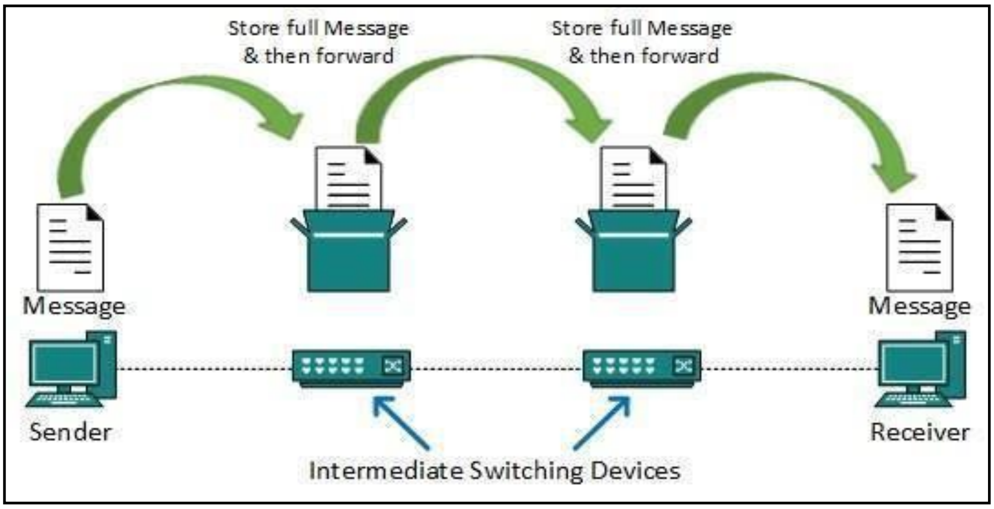


Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

➢ Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.



Characteristics of Message Switching

1. **Store and forward** – The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both available, otherwise it'll be stored indefinitely. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is accepting data. This is called the store-and-forward property.
2. **Message delivery** – This implies wrapping the entire information in a single message and transferring it from the source to the destination node. Each message must have a header that contains the message routing information, including the source and destination.

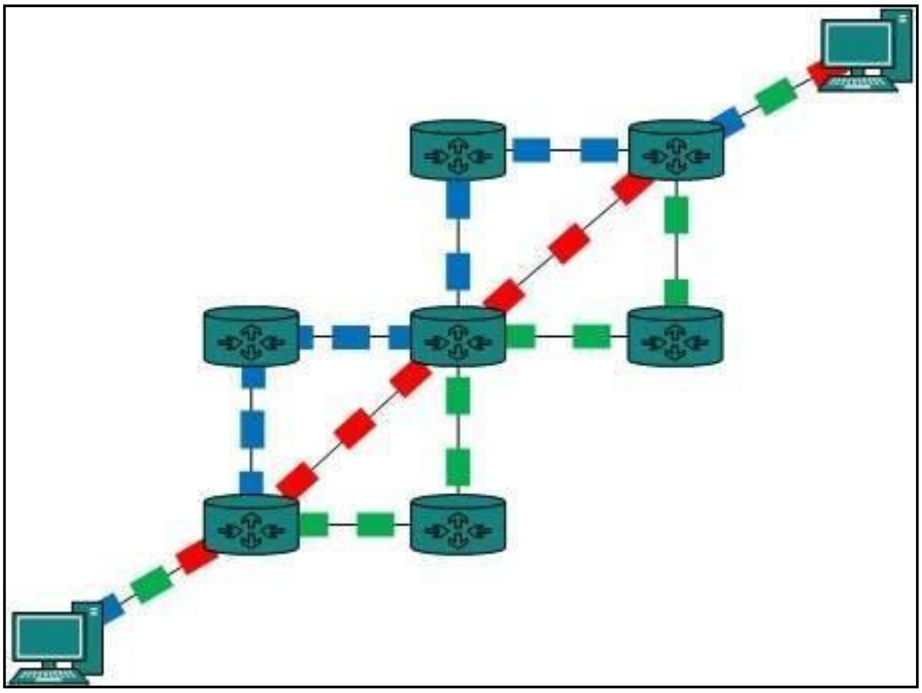
This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

➢ Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.

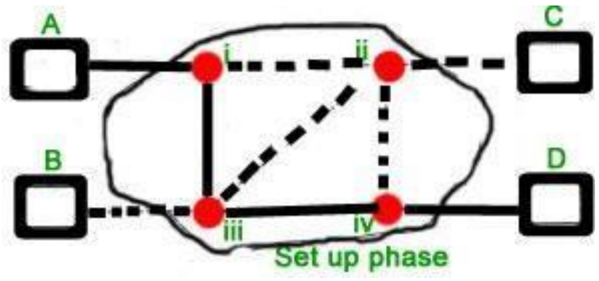


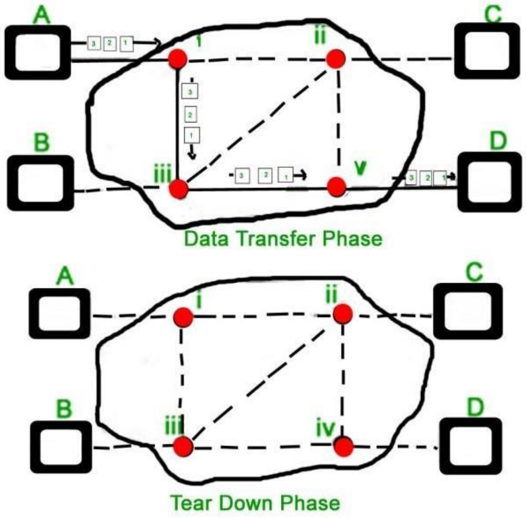
Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

Modes of Packet Switching :

Connection-oriented Packet Switching (Virtual Circuit)

Before starting the transmission, it establishes a logical path or virtual connection using signalling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence number.





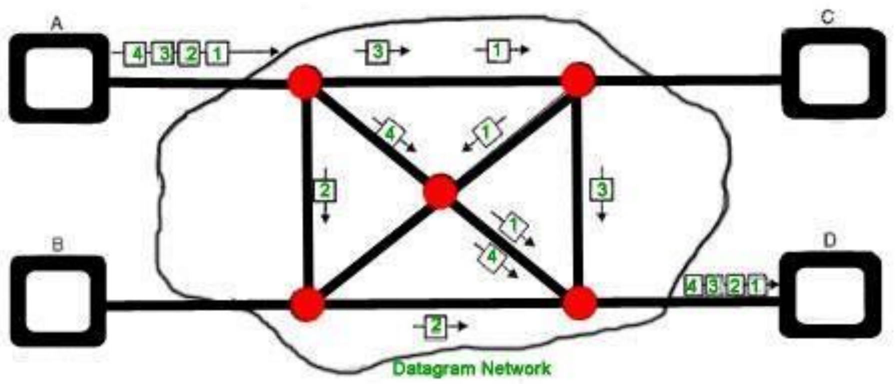
Data Transfer Phase

Tear Down Phase

Phases in virtual circuit packet switching

Overall three phases takes place here Setup, data transfer and tear down phase. All address information is only transferred during setup phase. Once the route to destination is discovered, entry is added to switching table of each intermediate node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number etc. Connection-oriented switching is very useful in switched WAN. Some popular protocols which use Virtual Circuit Switching approach are X.25, Frame-Relay, ATM and MPLS(Multi-Protocol Label Switching).

Connectionless Packet Switching (Datagram) :- Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers etc.



Datagram Packet Switching

In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.

Packet delivery is not guaranteed in connectionless packet switching, so the reliable delivery must be provided by end systems using additional protocols.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	**Virtual Circuit approach**
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

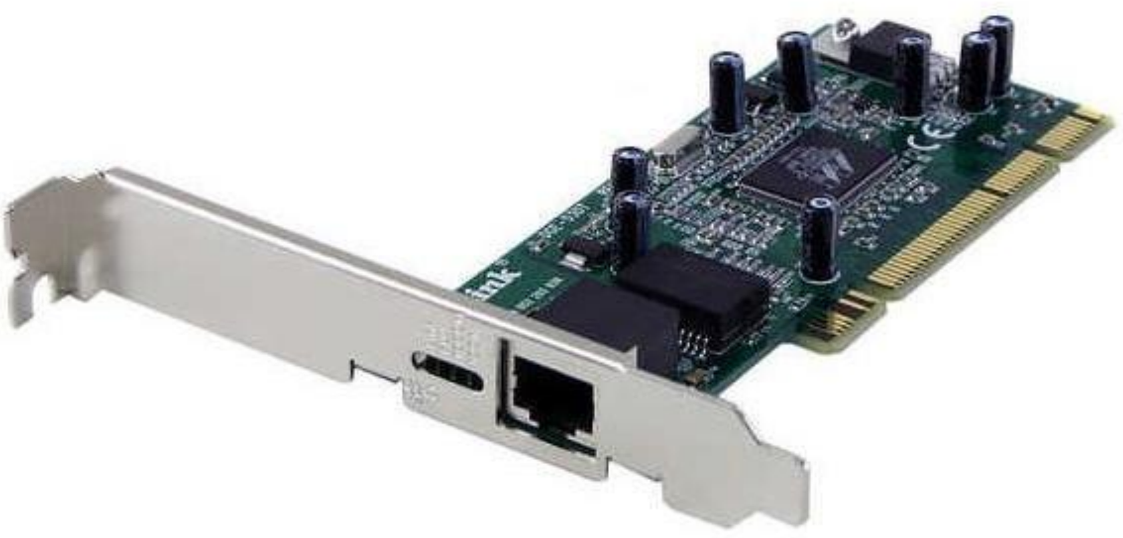
Network Interconnection Devices

Many interconnection device are required in a modern network, from the interface that allows a single computer to communicate with other computers via a LAN cable or a telephone line, to the large and complex switching devices that interconnect two or more entire networks. The main categories of interconnection device used in computer networks are listed below.

1. Network Interface Card
2. Bridge
3. Repeater
4. Switch
5. Hub4
6. Router

Network Interface Card

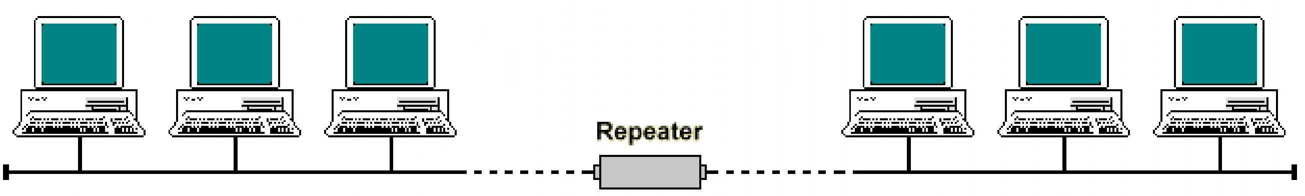
Every device on a network that needs to transmit and receive data must have a network interface card (NIC) installed. They are sometimes called network adapters, and are usually installed into one of the computer's expansion slots in the same way as a sound or graphics card. The NIC includes a transceiver, (a transmitter and receiver combined). The transceiver allows a network device to transmit and receive data via the transmission medium.



An Ethernet network interface card

Repeater

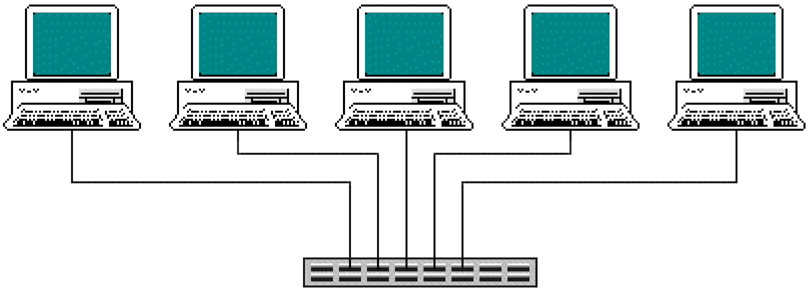
A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.



A repeater connecting network segments

Hub

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.



A hub in a star network configuration

Types of Hub

Active Hub:- These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.

Passive Hub:- These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes

Bridge

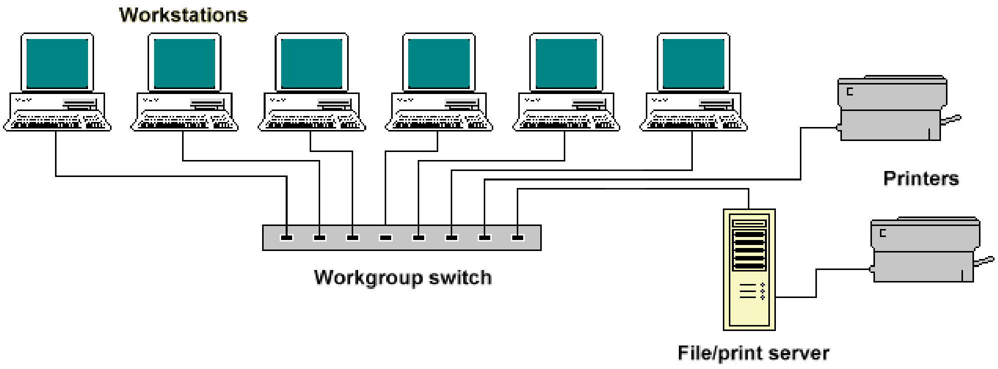
A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges**:- In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

Switch

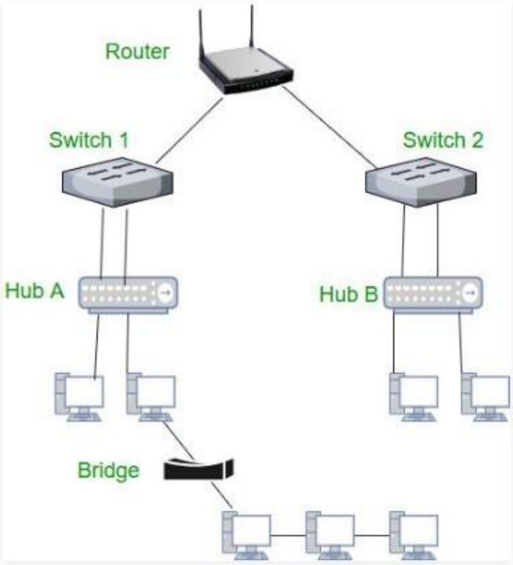
A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.



Workgroup switches connect together a number of enduser devices

Routers

A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



Client-Server Model

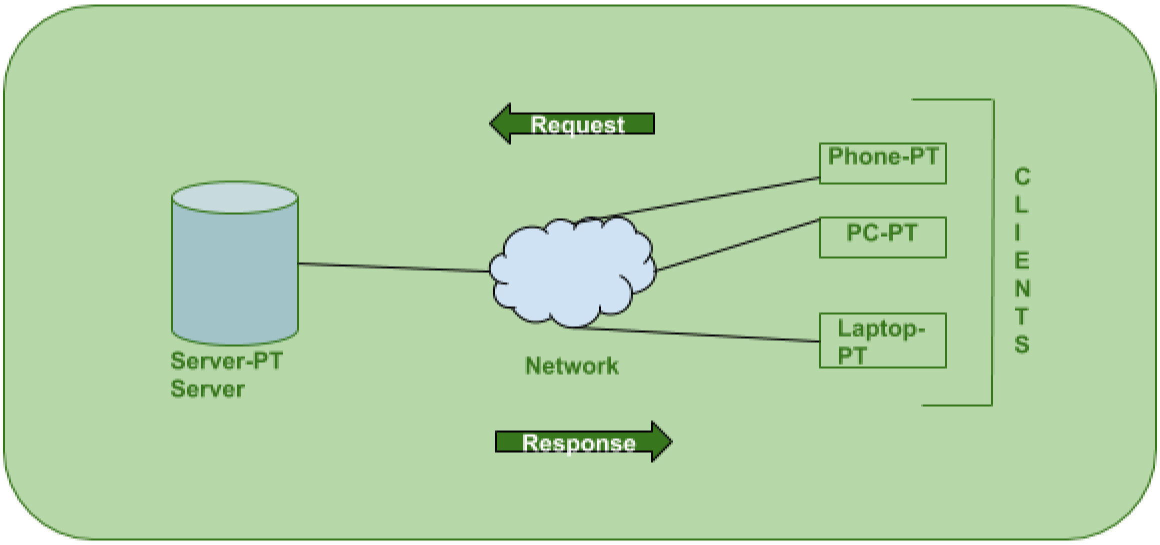
The Client-server model is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients. In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and deliver the data packets requested back to the client. Clients do not share any of their resources. Examples of Client-Server Model are Email, World Wide Web, etc.

How the Client-Server Model works ?

In this article we are going to take a dive into the **Client-Server** model and have a look at how the **Internet** works via, web browsers. This article will help us in having a solid foundation of the WEB and help in working with WEB technologies with ease.

- **Client:** When we talk the word **Client**, it mean to talk of a person or an organization using a particular service. Similarly in the digital world a **Client** is a computer (**Host**) i.e. capable of receiving information or using a particular service from the service providers (**Servers**).
- **Servers:** Similarly, when we talk the word **Servers**, It mean a person or medium that serves something. Similarly in this digital world a **Server** is a remote computer which provides information (data) or access to particular services.

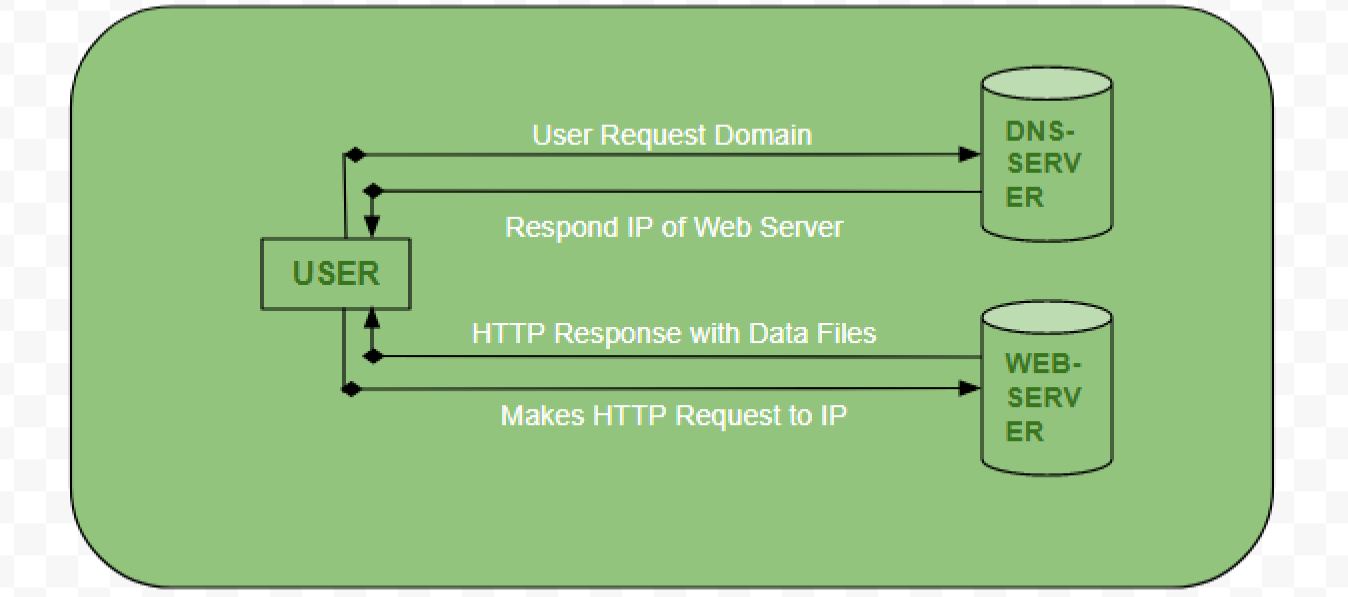
So, its basically the **Client** requesting something and the **Server** serving it as long as its present in the database.



How the browser interacts with the servers ?

There are few steps to follow to interacts with the servers a client.

- User enters the **URL**(Uniform Resource Locator) of the website or file. The Browser then requests the **DNS**(DOMAIN NAME SYSTEM) Server.
- **DNS Server** lookup for the address of the **WEB Server**.
- **DNS Server** responds with the **IP address** of the **WEB Server**.
- Browser sends over an **HTTP/HTTPS** request to **WEB Server's IP** (provided by **DNS server**).
- Server sends over the necessary files of the website.
- Browser then renders the files and the website is displayed. This rendering is done with the help of **DOM** (Document Object Model) interpreter, **CSS** interpreter and **JS Engine** collectively known as the **JIT** or (Just in Time) Compilers.



Advantages of Client-Server model:

- Centralized system with all data in a single place.
- Cost efficient requires less maintenance cost and Data recovery is possible.
- The capacity of the Client and Servers can be changed separately.

Disadvantages of Client-Server model:

- Clients are prone to viruses, Trojans and worms if present in the Server or uploaded into the Server.
- Server are prone to Denial of Service (DOS) attacks.
- Data packets may be spoofed or modified during transmission.
- Phishing or capturing login credentials or other useful information of the user are common and MITM(Man in the Middle) attacks are common.

Three-Tier Client Server Architecture in Distributed System

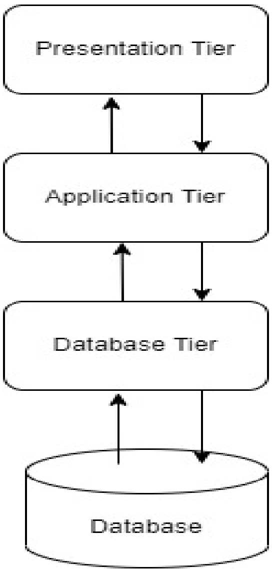
The most common type of multi-tier architecture in distributed systems is a three-tier client-server architecture. In this architecture, the entire application is organized into three computing tiers

- Presentation tier
- Application tier
- Data-tier

The major benefit of the three tiers in client-server architecture is that these tiers are developed and maintained independently and this would not impact the other tiers in case of any modification. It allows for better performance and even more scalability in architecture can be made as with the increasing demand, more servers can be added.

Three-tier client-server architecture in a distributed system:

- **Presentation Tier:** It is the user interface and topmost tier in the architecture. Its purpose is to take request from the client and displays information to the client. It communicates with other tiers using a web browser as it gives output on the browser. If we talk about Web-based tiers then these are developed using languages like- HTML, CSS, JavaScript.
- **Application Tier:** It is the middle tier of the architecture also known as the logic tier as the information/request gathered through the presentation tier is processed in detail here. It also interacts with the server that stores the data. It processes the client's request, formats, it and sends it back to the client. It is developed using languages like- Python, Java, PHP, etc.
- **Data Tier:** It is the last tier of the architecture also known as the Database Tier. It is used to store the processed information so that it can be retrieved later on when required. It consists of Database Servers like- Oracle, MySQL, DB2, etc. The communication between the Presentation Tier and Data-Tier is done using middle-tier i.e. Application Tier.



Advantages:

- Logical separation is maintained between Presentation Tier, Application Tier, and Database Tier.
- Enhancement of Performance as the task is divided on multiple machines in distributed machines and moreover, each tier is independent of other tiers.
- Increasing demand for adding more servers can also be handled in the architecture as tiers can be scaled independently.
- Developers are independent to update the technology of one tier as it would not impact the other tiers.
- Reliability is improved with the independence of the tiers as issues of one tier would not affect the other ones.
- Programmers can easily maintain the database, presentation code, and business/application logic separately. If any change is required in business/application logic then it does not impact the presentation code and codebase.
- Load is balanced as the presentation tier task is separated from the server of the data tier.
- Security is improved as the client cannot communicate directly with Database Tier. Moreover, the data is validated at Application Tier before passing to Database Tier.
- The integrity of data is maintained.
- Provision of deployment to a variety of databases rather than restraining yourself to one particular technology.

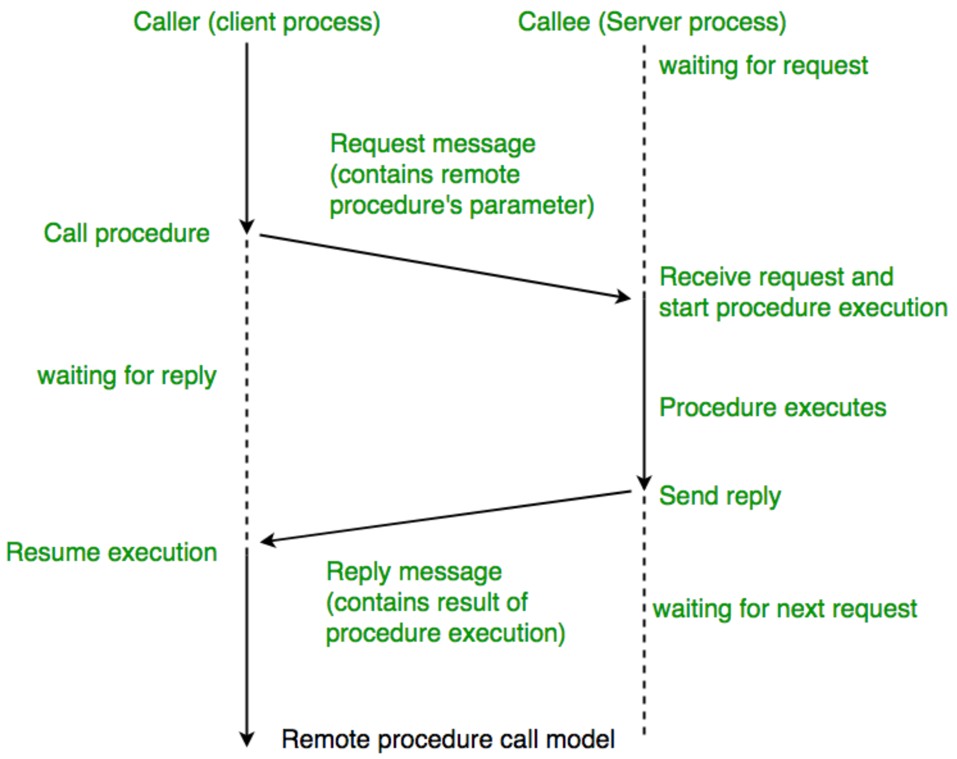
Disadvantages:

- The Presentation Tier cannot communicate directly with Database Tier.
- Complexity also increases with the increase in tiers in architecture.
- There is an increase in the number of resources as codebase, presentation code, and application code need to be maintained separately.

Remote Procedure Call (RPC) in Operating System

Remote Procedure Call (RPC) is a powerful technique for constructing **distributed, client-server based applications**. It is based on extending the conventional local procedure calling so that the **called procedure need not exist in the same address space as the calling procedure**. The two processes may be on the same system, or they may be on different systems with a network connecting them.

When making a Remote Procedure Call:



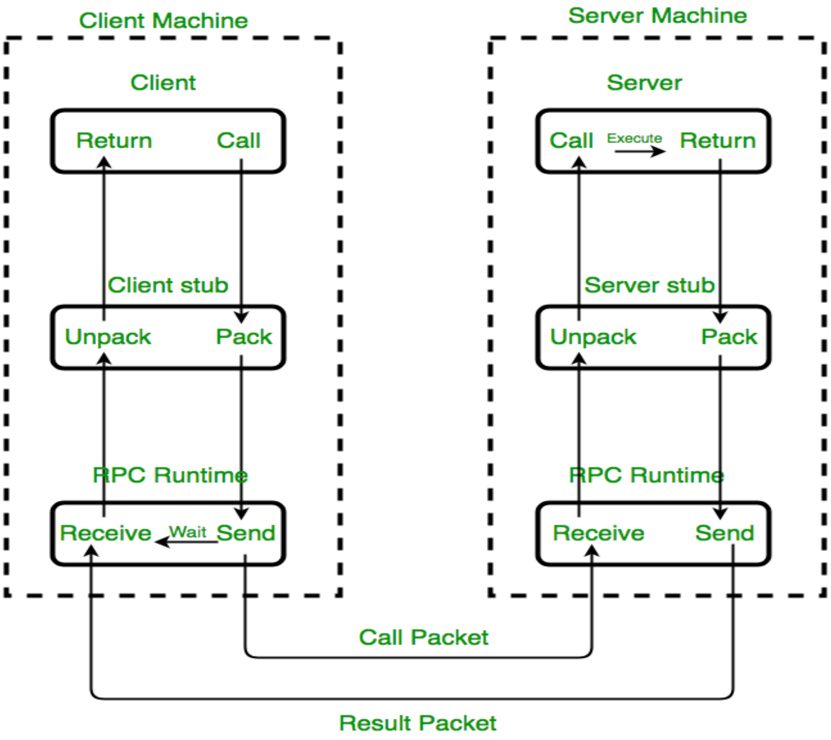
Remote procedure call model

1. The calling environment is suspended, procedure parameters are transferred across the network to the environment where the procedure is to execute, and the procedure is executed there.

2. When the procedure finishes and produces its results, its results are transferred back to the calling environment, where execution resumes as if returning from a regular procedure call.

NOTE: RPC is especially well suited for client-server **(e.g. query-response)** interaction in which the flow of control **alternates between the caller and callee**. Conceptually, the client and server do not both execute at the same time. Instead, the thread of execution jumps from the caller to the callee and then back again.

Working of RPC



Implementation of RPC mechanism

The following steps take place during a RPC :

1. A client invokes a **client stub procedure**, passing parameters in the usual way. The client stub resides within the client's own address space.
2. The client stub **marshalls(pack)** the parameters into a message. Marshalling includes converting the representation of the parameters into a standard format, and copying each parameter into the message.
3. The client stub passes the message to the transport layer, which sends it to the remote server machine.
4. On the server, the transport layer passes the message to a server stub, which **demarshalls(unpack)** the parameters and calls the desired server routine using the regular procedure call mechanism.
5. When the server procedure completes, it returns to the server stub **(e.g., via a normal procedure call return)**, which marshalls the return values into a message. The server stub then hands the message to the transport layer.
6. The transport layer sends the result message back to the client transport layer, which hands the message back to the client stub.
7. The client stub demarshalls the return parameters and execution returns to the caller.

RPC ISSUES :

Issues that must be addressed:

1. RPC Runtime: RPC run-time system is a library of routines and a set of services that handle the network communications that underlie the RPC mechanism. In the course of an RPC call, client-side and server-side run-time systems' code handle **binding, establish communications over an appropriate protocol, pass call data between the client and server, and handle communications errors.**

2. Stub: The function of the stub is to **provide transparency to the programmer-written application code**.

- **On the client side**, the stub handles the interface between the client's local procedure call and the run-time system, marshalling and unmarshalling data, invoking the RPC run-time protocol, and if requested, carrying out some of the binding steps.
- **On the server side**, the stub provides a similar interface between the run-time system and the local manager procedures that are executed by the server.

3. **Binding: How does the client know who to call, and where the service resides?** The most flexible solution is to use dynamic binding and find the server at run time when the RPC is first made. The first time the client stub is invoked, it contacts a name server to determine the transport address at which the server resides.

Binding consists of two parts:

- Naming:
- Locating:

1. **A Server** having a service to offer exports an interface for it. Exporting an interface registers it with the system so that clients can use it.
2. **A Client** must import an (exported) interface before communication can begin.

4. The call semantics associated with RPC :

It is mainly classified into following choices-

- **Retry request message –**
  Whether to retry sending a request message when a server has failed or the receiver didn't receive the message.
- **Duplicate filtering –**
  Remove the duplicate server requests.

- **Retransmission of results –**
  To resend lost messages without re-executing the operations at the server side.

ADVANTAGES :

1. RPC provides **ABSTRACTION** i.e message-passing nature of network communication is hidden from the user.
2. RPC often omits many of the protocol layers to improve performance. Even a small performance improvement is important because a program may invoke RPCs often.
3. RPC enables the usage of the applications in the distributed environment, not only in the local environment.
4. With RPC code re-writing / re-developing effort is minimized.
5. Process-oriented and thread oriented models supported by RPC.