Unit -1

Background Study and Revision

1.1 Introduction and necessity of computer networking

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

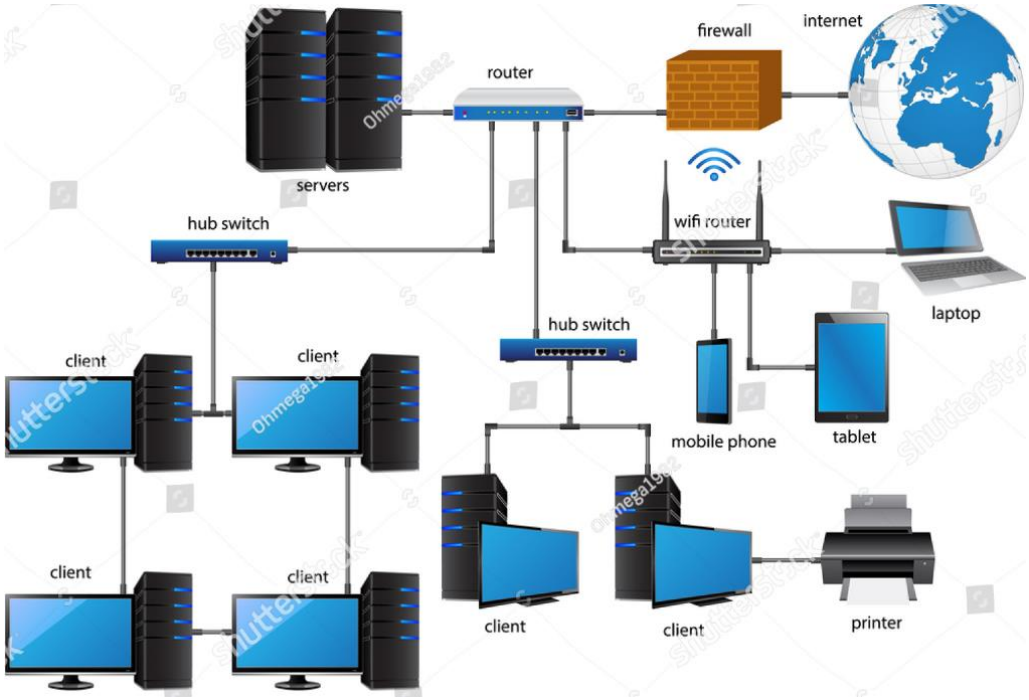

Fig: computer network

Communication is the process of reaching mutual understanding, in which participants not only exchange information, news, ideas and feelings but also create and share meaning. The communication involves – sender information, receiver information, language used for communication and medium used to establish the communication.

Uses of Computer Network

In the sense how organizations use computer networks are described below:

1. **Resource Sharing** : Many organizations have large number of substantial computers in operation often located far apart. Let us consider an example, a company having many factories situated at different locations. A computer at each location (that is in each factory) keeps the track of inventories, monitor productivity and do the local pay roll. Initially each of these computers may have worked in isolation from each other, but at some point, the management may have decided to connect these computers to be able to extract and correlate the information

of the entire company. The issue here is resource sharing. Its goal is to make all the programs, equipments, especially data available to anyone on the network irrespective of the location of the resource and the user.

2. **High Reliability**: The second goal or use of networking in companies is to high reliability by having alternative sources of supply. For example all the files can be replicated on two or more machines, so that in case one of them is not available (due to hardware failure), other copies can be used. This feature is used in financial institutions.
3. **Saving Money:** The third goal is to save money. Small computers often have better price/performance ratio than the larger ones. Mainframe (room-size) computers are roughly ten faster than the personal computers, but are a thousand times costly. This imbalance caused the system designers to design a system consisting of personal computers, one per user, with data kept on one or more shared file server machines. In this model the user are called the clients and this whole arrangement is known as the client-server model. In client-server model, the communication generally takes the form of a request message from a client to the receiver asking for some work to be done. Server does the work and sends back the reply.
4. **Scalability:** Another goal is scalability. Scalability is the ability to increase the system performance gradually as the workload grows, by just adding more processors.

In the sense how People Uses the Networks are given below :

5. **Access to Remote Information:** Access to remote information occurs in many forms. One of the areas where it is happening is access to the financial institutions. Many people pay their bills, manage bank accounts and handle investments electronically. Home shopping is also becoming popular these days. Another application that falls under this category is the access to information systems like World Wide Web which contains information about art, business, history, government, geography, economics and several other topics. All the above applications involve the interaction between the user and a remote database.
6. **Person to Person Communication:** Electronic Mail popularly known as email is widely used by millions of people to send text messages, photographs audio as well as video to other people or group of people. This application belongs to person to person communication category. Videoconferencing is also becoming popular these days. This technology makes it possible to have virtual meetings among far flung people. It is also a type of person to person communication.
7. **Interactive Entertainment:** These days we can see many live programs and shows. The best thing is that we can interact with them by participating in the quizzes and the contests organized by them.

Advantages and Disadvantages of Computer Network

The advantages of Computer Network are :

- Sharing devices such as printers saves money.
- Site (software) licenses are likely to be cheaper than buying several standalone licenses.

- Files can easily be shared between users.
- Network users can communicate by email and instant messenger.
- Security is good - users cannot see other users' files unlike on stand-alone machines.
- Data is easy to backup as all the data is stored on the file server.

The disadvantages of Computer Network are :

- Purchasing the network cabling and file servers can be expensive.
- Managing a large network is complicated, requires training and a network manager usually needs to be employed.
- If the file server breaks down the files on the file server become inaccessible. Email might still work if it is on a separate server. The computers can still be used but are isolated.
- Viruses can spread to other computers throughout a computer network.
- There is a danger of hacking, particularly with wide area networks. Security procedures are needed to prevent such abuse, e.g. a firewall.

1.2 Networks goals/motivation

Before designing a computer network we should see that the designed network fulfils the basic goals. We have seen that a computer network should satisfy a broad range of purposes and should meet various requirements. One of the main goals of a computer network is to enable its users to share resources, to provide low cost facilities and easy addition of new processing services. The computer network thus, creates a global environment for its users and computers.

Some of the basic goals that a Computer network should satisfy are:

- Cost reduction by sharing hardware and software resources.
- Provide high reliability by having multiple sources of supply.
- Provide an efficient means of transport for large volumes of data among various locations (High throughput).
- Provide inter-process communication among users and processors.
- Reduction in delay driving data transport.
- Increase productivity by making it easier to share data amongst users.
- Repairs, upgrades, expansions, and changes to the network should be performed with minimal impact on the majority of network users.
- Standards and protocols should be supported to allow many types of equipment from different vendors to share the network (Interoperatability).
- Provide centralised/distributed management and allocation of network resources like host processors, transmission facilities etc.

Classification of networks

Depending on the transmission technology i.e., whether the network contains switching elements or not, we have two types of networks:

- Broadcast networks.
- Point-to-point or Switched networks.

Broadcast networks

Broadcast networks have a single communication channel that is shared by all the machines on the network. In this type of network, short messages sent by any machine are received by all the machines on the network. The packet contains an address field, which specifies for whom the packet is intended. All the machines, upon receiving a packet check for the address field, if the packet is intended for itself, it processes it and if not the packet is just ignored.

Using Broadcast networks, we can generally address a packet to all destinations (machines) by using a special code in the address field. Such packets are received and processed by all machines on the network. This mode of operation is known as "Broadcasting". Some Broadcast networks also support transmission to a subset of machines and this is known as "Multicasting". One possible way to achieve Multicasting is to reserve one bit to indicate multicasting and the remaining (n-1) address bits contain group number. Each machine can subscribe to any or all of the groups.

Broadcast networks are easily configured for geographically localised networks. Broadcast networks may be Static or dynamic, depending on how the channel is allocated.

In Static allocation, time is divided into discrete intervals and using round robin method, each machine is allowed to broadcast only when its time slot comes up. This method is inefficient because the channel capacity is wasted when a machine has nothing to broadcast during its allocated slot.

Dynamic allocation may be centralised or decentralised. In centralised allocation method, there is a single entity, for example, a bus arbitration unit which determine who goes next and this is achieved by using some internal algorithm. In Decentralised channel allocation method, there is no central entity, here, each machine decides for itself whether or not to transmit.

The different types of Broadcast networks are:

1. Packet Radio Networks.
2. Satellite Networks.
3. Local Area Networks.

LAN (Local Area Network)

Local Area Network is a computer network that spans over a relatively small area. Most LANs are confined to a single building or group of buildings within a campus. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it is also able to access data and devices anywhere on the LAN. This means that many users can share data as well as expensive devices, such as laser printers, fax machines etc. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. There are many different types of LANs, Ethernets being the most common for PCs.

The following characteristics differentiate one LAN from another:

- **Topology:** The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line.
- **Protocols:** The rules and encoding specifications for sending data. The protocols also determine whether the network uses peer-to-peer or client/server architecture.
- **Media:** Devices can be connected by twisted-pair wire, coaxial cables, or fiber optic cables. Some networks communicate via radio waves hence, do not use any connecting media.

LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited, and there is also a limit on the number of computers that can be attached to a single LAN.

The typical characteristics of a LAN are:

- Confined to small areas i.e., it connects several devices over a distance of 5 to 10 km.
- High speed.
- Most inexpensive equipment.
- Low error rates.
- Data and hardware sharing between users owned by the user.
- Operates at speeds ranging from 10Mbps to 100Mbps. Now a days 1000 Mbps are available.

Point to Point or Switched Networks

Point–to-point or switched, networks are those in which there are many connections between individual pairs of machines. In these networks, when a packet travels from source to destination it may have to first visit one or more intermediate machines. Routing algorithms play an important role in Point-to-point or Switched networks because often multiple routes of different lengths are available.

An example of switched network is the international dial-up telephone system.

The different types of Point- to-point or Switched networks are:

- Circuit Switched Networks.
- Packet Switched Networks.

In Switched network, the temporary connection is established from one point to another for either the duration of the session (circuit switching) or for the transmission of one or more packets of data (packet switching).

Circuit Switched Networks

Circuit Switched networks use a networking technology that provides a temporary, but dedicated connection between two stations no matter how many switching devices are used in the data

transfer route. Circuit switching was originally developed for the analog based telephone system in order to guarantee steady and consistent service for two people engaged in a phone conversation. Analog circuit switching has given way to digital circuit switching, and the digital counterpart still maintains the connection until broken (one side hangs up). This means bandwidth is continuously reserved and "silence is transmitted" just the same as digital audio in voice conversation.

Packet Switched Networks

Packet switched Networks use a networking technology that breaks up a message into smaller packets for transmission and switches them to their required destination. Unlike circuit switching, which requires a constant point-to-point circuit to be established, each packet in a packet- switched network contains a destination address. Thus, all packets in a single message do not have to travel the same path. They can be dynamically routed over the network as lines become available or unavailable. The destination computer reassembles the packets back into their proper sequence.

Packet switching efficiently handles messages of different lengths and priorities. By accounting for packets sent, a public network can charge customers for only the data they transmit. Packet switching has been widely used for data, but not for real-time voice and video. However, this is beginning to change. IP and ATM technologies are expected to enable packet switching to be used for everything.

The first international standard for wide area packet switching networks was X.25, which was defined when all circuits were digited and susceptible to noise. Subsequent technologies, such as frame relay and SMDS were designed for today's almost-error free digital lines.

ATM uses a cell-switching technology that provides the bandwidth sharing efficiency of packet switching with the guaranteed bandwidth of circuit switching.

Higher-level protocols, such as TCP/IP, IPX/SPX and NetBIOS, are also packet based and are designed to ride over packet-switched topologies.

Public packet switching networks may provide value added services, such as protocol conversion and electronic mail.

Network Topology

Topology refers to the shape of a network, or the network's layout. How different nodes in a network are connected to each other and how they communicate with each other is determined by the network's topology. Topologies are either *physical* or *logical*.

Some of the most common network topologies are:

- Bus topology
- Star topology
- Ring topology
- Tree topology
- Mesh topology
- Cellular topology.

The parameters that are to be considered while selecting a physical topology are:

- Ease of installation.
- Ease of reconfiguration.
- Ease of troubleshooting.

1. Bus Topology

In Bus topology, all devices are connected to a central cable, called the bus or backbone. The bus topology connects workstations using a single cable. Each workstation is connected to the next workstation in a point-to-point fashion. All workstations connect to the same cable. *Figure* shows computers connected using Bus Topology.

In this type of topology, if one workstation goes faulty all workstations may be affected as all workstations share the same cable for the sending and receiving of information. The cabling cost of bus systems is the least of all the different topologies. Each end of the cable is terminated using a special terminator.

The common implementation of this topology is Ethernet. Here, message transmitted by one workstation is heard by all the other workstations.

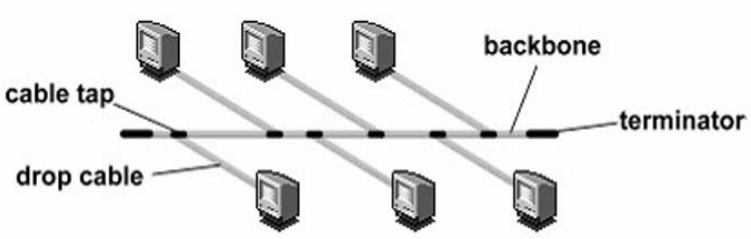

Fig: Bus Topology

Advantages of Bus Topology

- Installation is easy and cheap when compared to other topologies.
- Connections are simple and this topology is easy to use.
- Less cabling is required.

Disadvantages of Bus Topology

- Used only in comparatively small networks.
- As all computers share the same bus, the performance of the network deteriorates when we increase the number of computers beyond a certain limit.
- Fault identification is difficult.
- A single fault in the cable stops all transmission.

2. Star Topology

Star topology uses a central hub through which, all components are connected. In a Star topology, the central hub is the host computer, and at the end of each connection is a terminal as shown in Nodes communicate across the network by passing data through the hub. A star network uses a significant amount of cable as each terminal is wired back to the central hub, even if two terminals are side by side but several hundred meters away from the host. The central hub makes all routing decisions, and all other workstations can be simple.

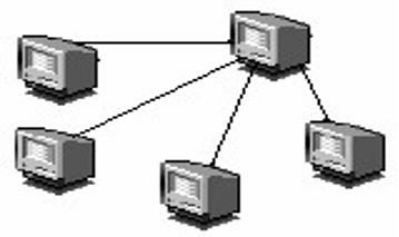

Figure: Star Topology

An advantage of the star topology is, that failure, in one of the terminals does not affect any other terminal; however, failure of the central hub affects all terminals. This type of topology is frequently used to connect terminals to a large time-sharing host computer.

Advantages of star topology

- Installation and configuration of network is easy.
- Less expensive when compared to mesh topology.
- Faults in the network can be easily traced.
- Expansion and modification of star network is easy.
- Single computer failure does not affect the network.
- Supports multiple cable types like shielded twisted pair cable, unshielded twisted pair cable, ordinary telephone cable etc.

Disadvantages of Bus Topology

- Failure in the central hub brings the entire network to a halt.
- More cabling is required in comparison to tree or bus topology because each node is connected to the central hub.

3. Ring Topology

In Ring Topology all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it, i.e., the ring topology connects workstations in a closed loop, which is depicted in *Figure*. Each terminal is connected to two other terminals (the next and the previous), with the last terminal being connected to the first. Data is transmitted around the ring in one direction only; each station passing on the data to the next station till it reaches its destination.

Information travels around the ring from one workstation to the next. Each packet of data sent on the ring is prefixed by the address of the station to which it is being sent. When a packet of data arrives, the workstation checks to see if the packet address is the same as its own, if it is, it grabs the data in the packet. If the packet does not belong to it, it sends the packet to the next workstation in the ring.

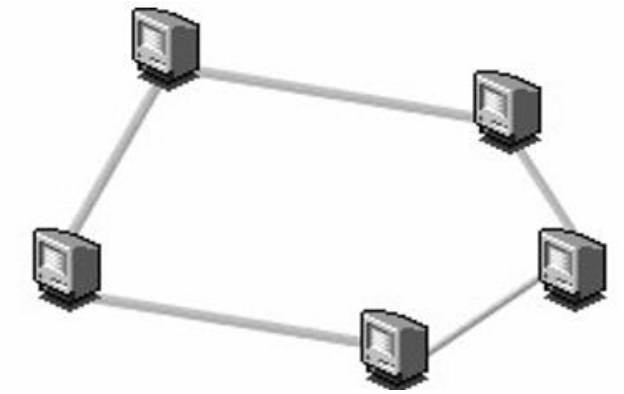

Figure: Ring Topology

Faulty workstations can be isolated from the ring. When the workstation is powered on, it connects itself to the ring. When power is off, it disconnects itself from the ring and allows the information to bypass the workstation.

The common implementation of this topology is token ring. A break in the ring causes the entire network to fail. Individual workstations can be isolated from the ring.

Advantages of ring topology

- Easy to install and modify the network.
- Fault isolation is simplified.
- Unlike Bus topology, there is no signal loss in Ring topology because the tokens are data packets that are re-generated at each node.

Disadvantages of ring topology

- Adding or removing computers disrupts the entire network.
- A break in the ring can stop the transmission in the entire network.
- Finding fault is difficult.
- Expensive when compared to other topologies.

4. Tree Topology

Tree topology is a LAN topology in which only one route exists between any two nodes on the network. The pattern of connection resembles a tree in which all branches spring from one root. *Figure* shows computers connected using Tree Topology.

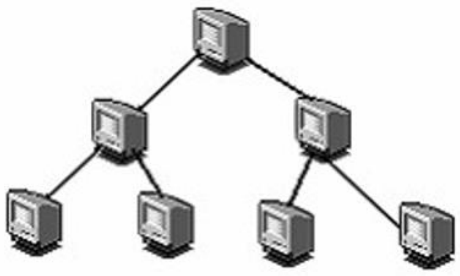

Figure: Tree topology

Tree topology is a hybrid topology, it is similar to the star topology but the nodes are connected to the secondary hub, which in turn is connected to the central hub. In this t opology groups of star-configured networks are connected to a linear bus backbone.

Advantages of Tree Topology

- Installation and configuration of network is easy.
- Less expensive when compared to mesh topology.
- Faults in the network can be detected traced.
- The addition of the secondary hub allows more devices to be attached to the central hub.
- Supports multiple cable types like shielded twisted pair cable, unshielded twisted pair cable, ordinary telephone cable etc.

Disadvantages of Tree Topology

- Failure in the central hub brings the entire network to a halt.
- More cabling is required when compared to bus topology because each node is connected to the central hub.

5. Mesh Topology

Devices are connected with many redundant interconnections between network nodes. In a well-connected topology, every node has a connection to every other node in the network. The cable requirements are high, but there are redundant paths built in. Failure in one of the computers does not cause the network to break down, as they have alternative paths to other computers.

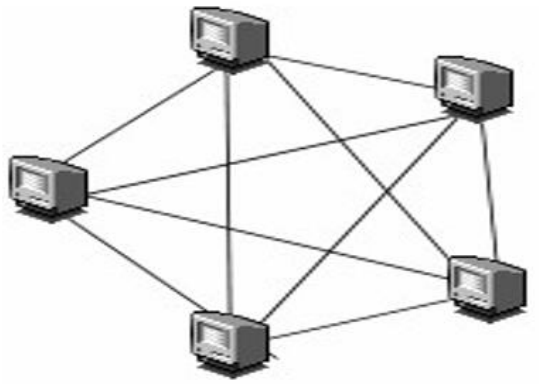

Figure: Mesh Topology

Mesh topologies are used in critical connection of host computers (typically telephone exchanges). Alternate paths allow each computer to balance the load to other computer systems in the network by using more than one of the connection paths available. A fully connected mesh network therefore has n (n-1)/2 physical channels to link n devices. To accommodate these, every device on the network must have (n-1) input/output ports.

Advantages of Mesh Topology

- Use of dedicated links eliminates traffic problems.
- Failure in one of the computers does not affect the entire network.
- Point-to-point link makes fault isolation easy.
- It is robust.
- Privacy between computers is maintained as messages travel along dedicated path.

Disadvantages of Mesh Topology

- The amount of cabling required is high.
- A large number of I/O (input/output) ports are required.

6. Cellular Topology

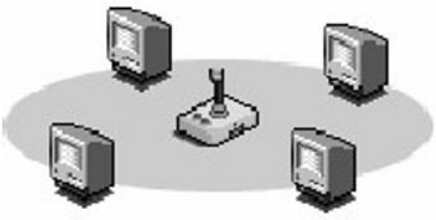

Figure: Cellular topology

Cellular topology, divides the area being serviced into cells. In wireless media each point transmits in a certain geographical area called a cell, each cell represents a portion of the total network area. *Figure*shows computers using Cellular Topology. Devices that are present within the cell, communicate through a central hub. Hubs in different cells are interconnected and hubs are responsible for routing data across the network. They provide a complete network infrastructure. Cellular topology is applicable only in case of wireless media that does not require cable connection.

Advantages of Cellular Topology

- If the hubs maintain a point-to-point link with devices, trouble shooting is easy.
- Hub-to-hub fault tracking is more complicated, but allows simple fault isolation.

Disadvantages of Cellular Topology

- When a hub fails, all devices serviced by the hub lose service (are affected).

Network Architecture

Depending on the architecture used Networks can be classified as Client/Server or Peer-to-Peer Networks.

A. Client/Server Architecture

Figure: Client/Server Architecture

Client/Server Architecture is one in which the client (personal computer or workstation) is the requesting machine and the server is the supplying machine, both of which are connected via a local area network (LAN) or wide area network (WAN). The client/server architecture significantly decreased network traffic by providing a query response rather than total file transfer. It allows multi-user updating through a GUI front end to a shared database. Remote Procedure Calls (RPCs) or standard query language (SQL) statements are typically used to communicate between the client and server.

The following are the examples of client/server architectures.

1) **Two tier architectures** A two-tier architecture is where a client talks directly to a server, with no intervening server. It is typically used in small environments(less than 50 users). In two tier client/server architectures, the user interface is placed at user's desktop environment and the database management system services are usually in a server that is a more powerful machine that provides services to the many clients. Information processing is split between the user system interface environment and the database management server environment.

2) **Three tier architectures** The three tier architecture is introduced to overcome the drawbacks of the two tier architecture. In the three tier architecture, a middleware is used between the user system interface client environment and the database management server environment.

These middleware are implemented in a variety of ways such as transaction processing monitors, message servers or application servers. The middleware perform the function of queuing, application execution and database staging. In addition the middleware adds scheduling and prioritization for work in progress.

The three tier client/server architecture is used to improve performance for large number of users and also improves flexibility when compared to the two tier approach.

The drawback of three tier architectures is that the development environment is more difficult to use than the development of two tier applications.

The widespread use of the term 3-tier architecture also denotes the following architectures:

• Application sharing between a client, middleware and enterprise server.

• Application sharing between a client, application server and enterprise database server.

i) **Three tier with message server**: In this architecture, messages are processed and prioritized asynchronously. Messages have headers that include priority information, address and identification number. The message server links to the relational DBMS and other data sources. Messaging systems are alternative for wireless infrastructures.

ii) **Three tier with an application server:** This architecture allows the main body of an application to run on a shared host rather than in the user system interface client environment. The application server shares business logic, computations and a data retrieval engine. In this architecture applications are more scalable and installation costs are less on a single server than maintaining each on a desktop client.

3-tier architecture provides

• A greater degree of flexibility

• Increased security, as security can be defined for each service, and at each level

• Increased performance, as tasks are shared between servers

The basic characteristics of client/server architectures are:

1) Combination of a client or **front-end portion** that interacts with the user, and a server or **back-end portion** that interacts with the shared resource. The client process contains **solution-specific logic** and provides the interface between the user and the rest of the application system. The server process acts as a **software engine** that manages shared resources such as databases, printers, modems, or high powered processors.

2) The front-end task and back-end task have fundamentally different requirements for computing resources such as processor speeds, memory, disk speeds and capacities, and input/output devices.

3) The environment is typically **heterogeneous** and multivendor. The hardware platform and operating system of client and server are not usually the same. Client and server processes communicate through a well-defined set of standard application program interfaces (API's) and RPC's.

4) An important characteristic of client-server systems is scalability. They can be scaled horizontally or vertically. Horizontal scaling means adding or removing client workstations with only a slight performance impact. Vertical scaling means migrating to a larger and faster server machine or multiservers.

Advantages of Client/Server Network

- Improved Data Sharing: Data is retained by usual business processes and manipulated on a server is available for designated users (clients) over an authorized access.

- Integration of Services: Every client is given the opportunity to access corporate information via desktop interface eliminating the necessity to log into a terminal mode or processor.

- Shared Resources Amongst Different Platforms: Application used for client-server model is built regardless of the hardware platform or technical background of the entitled software (operating system software) providing an open computing environment, enforcing users to obtain the services of clients and servers (database, application and communication services)

- Data Processing Capability Despite the Location: Client-server users can directly log into a system despite of the location or technology of the processors.

- Easy Maintenance: Client-server architecture is distributed model representing dispersed responsibilities among independent computers integrated across a network. Therefore, it's easy to replace, repair, upgrade and relocate a server while client remains unaffected. This unaware change is called as Encapsulation.

- Security: Servers have better control access and resources to ensure that only authorized clients can access or manipulate data and server updates are administered effectively.

Disadvantages of Client/Server Architecture

- Overloaded Servers: When there are frequent simultaneous client requests, server severely get overloaded, forming traffic congestion.

- Impact of Centralized Architecture: Since it is centralized, if a critical server failed, client requests are not accomplished. Therefore, client-server lacks the robustness of a good network.

B. Peer-to Peer Architecture

Figure: Peer-to-Peer Architecture

A type of network in which each workstation has equal capabilities and responsibilities is called peer-to-peer network. Figure shows the arrangement of computers in a peer-to-peer environment. Here each workstation acts as both a client and a server. There is no central repository for information and there is no central server to maintain. Data and resources are distributed throughout the network, and each user is responsible for sharing data and resources connected to their system. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler and less expensive, but they usually do not offer the same performance under heavy loads. A peer-to-peer network is also known as a Distributed network.

Advantages of Peer-to-Peer Architecture

1. Such networks are easy to set up and maintain as each computer manages itself.
2. It eliminates extra cost required in setting up the server.
3. Since each device is master of its own, they are not dependent on other computers for their operations.

Disadvantages of Peer-to-Peer Architecture

1. In peer-to-peer network, the absence of centralized server make it difficult to backup data as data is located on different workstations.
2. Security is weak as each system manages itself only.
3. There is no central point of data storage for file archiving.

Difference between Client/Server and Peer-to-Peer Architecture

BASIS FOR COMAPAISON	CLIENT-SERVER	PEER-TO-PEER
Basic	There is a specific server and specific clients connected to the server.	Clients and server are not distinguished; each node act as client and server.
Service	The client request for service and server respond with the service.	Each node can request for services and can also provide the services.
Focus	Sharing the information.	Connectivity.
Data	The data is stored in a centralized server.	Each peer has its own data.
Server	When several clients request for the services simultaneously, a server can get bottlenecked.	As the services are provided by several servers distributed in the peer-to-peer system, a server in not bottlenecked.
Expense	The client-server are expensive to implement.	Peer-to-peer are less expensive to implement.
Stability	Client-Server is more stable and scalable.	Peer-toPeer suffers if the number of peers increases in the system.

Types of Computer Networks

Computer Networks are mostly classified on the basis of the geographical area that the network covers, the topology used, the transmission media used and the computing model used.

Based on the geographical area covered the networks may be LAN, MAN, WAN, GAN, PAN.

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.

If more than two computers are to be connected in one LAN, additional network components such as hubs, bridges, and switches are needed, which act as coupling elements and distribution nodes. The network type LAN was developed to enable **fast transmission of large amounts of data**.

LANs enable convenient information exchange between the various devices connected to the network. In a business context, it's common to share files, network printers, and applications via LAN with several computers.

Figure: Local Area Network

If a local network is implemented via radio, it is referred to as a **Wireless Local Area Network (WLAN)**. The WLAN standard's technical basis is defined by the IEEE 802.11 family of standards. Wireless local networks offer the ability to easily integrate devices into home or corporate networks, and are compatible with wired Ethernet LANs. However, the data throughput is lower than for an Ethernet connection.

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.

LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited, and there is also a limit on the number of computers that can be attached to a single LAN.

The typical characteristics of a LAN are:

- Confined to small areas i.e., it connects several devices over a distance of 5 to 10 km.
- High speed.
- Most inexpensive equipment.
- Low error rates.
- Data and hardware sharing between users owned by the user.
- Operates at speeds ranging from 10Mbps to 100Mbps. Now a days 1000 Mbps are available.

Metropolitan Area Network (MAN)

Metropolitan Area Network is a Computer network designed for a town or city. In terms of geographic area MAN's are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MAN's are usually characterized by very high-speed connections using fiber optical cable or other digital media. The best known example of a MAN is the cable television network available in many cities. A standard for larger regional radio networks, known as **Wireless Metropolitan Area Networks (WMAN)**, was developed with IEEE 802.16. This technology

known as **WiMAX** (Worldwide Interoperability for Microwave Access) makes it possible to set up WiFi hotspots. These are several WiFi access points working together in different locations.

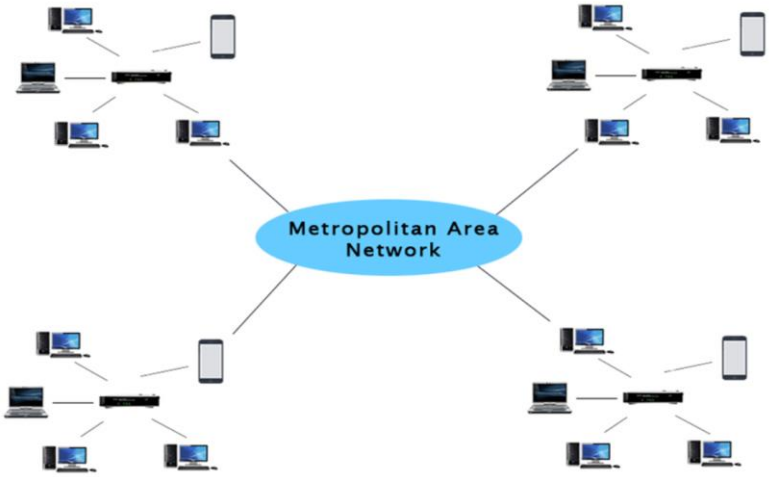

Figure: Metropolitan Area Network

The Typical Characteristics of a MAN are:

- Confined to a larger area than a LAN and can range from 10km to a few 100km in length.
- Slower than a LAN but faster than a WAN.
- Operates at a speed of 1.5 to 150 Mbps.
- Expensive equipment.
- Moderate error rates

Wide Area Network (WAN)

Wide Area Network is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs), which are depicted, in *Figure.* They can connect networks across cities, states or even countries.

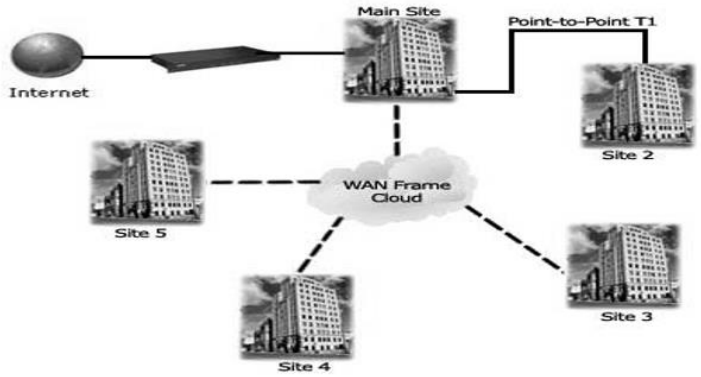

Figure: wide area network

Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.

The Typical characteristics of a WAN are:

- A WAN can range from 100km to 1000km and the speed is less than 150 Mbps.

- WAN supports large number of computers and multiple host machines.
- Various segments of network are interconnected using sophisticated support devices like routers and gateways.
- Usually the speed is much slower than LAN speed.
- Highest possible error rate compared to LAN & MAN.

Global Area Network (GAN)

A **global network**, such as the internet, is referred to as the Globe Area Network (GAN). The internet is, however, not the only computer network of its kind. Internationally operating companies also support local networks that comprise of several WANs and connect company computers across the world. GANs use the fiber optic infrastructure from wide area networks and combine these with **international undersea cables** or **satellite transmissions**.

Personal Area Network (PAN)

To enable data exchange, modern devices such as smartphones, tablets, laptops, and desktop computers can be integrated into a network. This can be wired in the form of a Personal Area Network (PAN). Common transfer techniques include **USB** or **FireWire**. The wireless variety is known as **Wireless Personal Area Network (WPAN)** and is based on technologies such as Bluetooth, Wireless USB. A wireless Personal Area Network, which can be achieved via Bluetooth, is called **Piconet**. PANs and WPANs usually only stretch over a few meters, and are therefore not suitable for connecting devices in different rooms or even buildings. Due to the limited range and a comparatively low data transfer rate, PANs are primarily used to connect peripheral devices in the hobby and entertainment sector. Typical examples include wireless headphones, game consoles, and digital cameras. Within the **Internet of Things (IoT)**'s framework, WPANs are responsible for the communication of control and monitoring applications with a low data rates. Protocols such as Insteon, Z-Wave, and ZigBee have been specifically designed for smart homes and home automation.

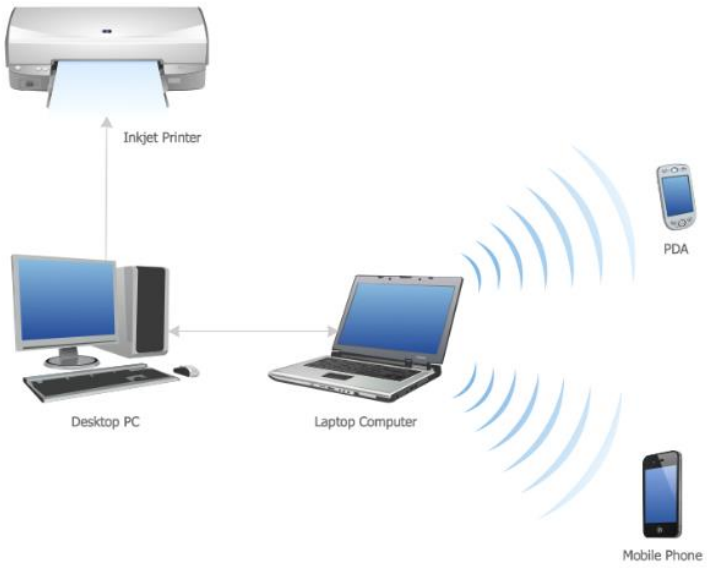

Figure: Personal Area Network

Difference between LAN, MAN and WAN

BASIS OF COMPARISON	LAN	MAN	WAN
Stands For	Local Area Network	Metropolitan Area Network	Wide Area Network
Definition	LAN (Local Area Network) is a computer network covering a small geographic area, like a home, office, school, or group of buildings.	A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city.	WAN (Wide Area Network) is a computer network that covers a broad area (e.g., any network whose communications links cross metropolitan, regional, or national boundaries over a long distance).
Covers	Local areas only (e.g., homes, offices, schools)	Covers the area inside a town or a city.	Large geographic areas (e.g., cities, states, nations)
Ownership of Network	Private	Private or Public	Private or Public
Speed	High speed (1000 Mbps)	moderate speed(44 to 150 Mbps)	Less speed (150 Mbps)
Maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Tolerance	LANs tend to have fewer problems associated with them, as there is a smaller number of systems to deal with.	Less fault tolerance	WANs tend to be less fault tolerant as they consist of a large number of systems.
Bandwidth	High bandwidth	Less bandwidth	Low bandwidth
Congestion	Less congestion	More congestion	More congestion
Example	College, School, Hospital.	The network in city building can be a MAN	The Internet is a good example of a WAN

1.3 Networks protocols

A protocol is a set of formal operating rules, procedures, or conventions that govern a given process. A communication or network protocol, therefore, describes the rules that govern the transmission of data over communication networks. These rules provide a method for orderly and efficient exchange of data between the sender and receiver, and for performing each of these functions.

1. Data sequencing. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering (or sequencing) packets to detect loss or duplication of packets and to correctly identify packets, which belong to the same message.
2. Data routing. Routing algorithms are designed to find the most efficient paths between the source and destination nodes of a message. They can handle varying degree of traffic on the present network configuration with optimal time utilization.
3. Data formatting. Data formatting rules define which group of bits or characters within a packet constitutes data, control, addressing or other information.
4. Flow control. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resources sharing and protection against traffic congestion by regulating the flow of data on the communication lines.
5. Error control. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method for correcting errors is to retransmit the erroneous message block. This method requires coordination between the sender and receiver nodes, so that the block having error is discarded by the receiver node and is retransmitted by the sender node.
6. Precedence and order of transmission. These rules ensure that all nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.
7. Connection establishment and termination. These rules defines how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.
8. Data security. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.
9. Log information. Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.