Chapter1

Introduction to Computer Network

Definition

- 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.

- In information technology, a computer network, also called a data network, is a series of points, or nodes, interconnected by communication paths for the purpose of transmitting, receiving and exchanging data, voice and video traffic.

- Computer Networking is simply a group of computers that are connected to each other in some way (eg. wired (LAN), wireless or internet) for the purpose of communicating to each other.

Uses of the computer Network

- Exchange of information between different computers. (File sharing).
- Interconnected small computers in place of large computers.
- Communication tools (voice , video)
- Some applications and technologies are examples of Distributed system. (Railway reservation system, Distributed databases etc).

Advantages of Computer Network

- **It enhances communication and availability of information**

  Networking, especially with full access to the web, allows ways of communication that would simply be impossible before it was developed. Instant messaging can now allow users to talk in real time and send files to other people wherever they are in the world, which is a huge boon for businesses. Also, it allows access to a vast amount of useful information, including traditional reference materials and timely facts, such as news and current events.

- **It allows for more convenient resource sharing**

  This benefit is very important, particularly for larger companies that really need to produce huge numbers of resources to be shared to all the people. Since the technology involves computer-based work, it is assured that the resources they wanted to get across would be completely shared by connecting to a computer network which their audience is also using.

- **It makes file sharing easier**

  Computer networking allows easier accessibility for people to share their files, which greatly helps them with saving more time and effort, since they could do file sharing more accordingly and effectively.

- **It is highly flexible.**

  This technology is known to be very flexible, as it gives users the opportunity to explore everything about essential things, such as software without affecting their functionality. Plus, people will have the accessibility to all information they need to get and share.

- **It is an inexpensive system.**

  Installing networking software on your device would not cost too much, as you are assured that it lasts and can effectively share information to your peers. Also, there is no need to change the software regularly, as mostly it is not required to do so.

- **It increases cost efficiency.**

  With computer networking, you can use a lot of software products available on the market which can just be stored or installed in your system or server, and can then be used by various workstations.

- **It boosts storage capacity.**

  Since you are going to share information, files and resources to other people, you have to ensure all data and content are properly stored in the system. With this networking technology, you can do all of this without any hassle, while having all the space you need for storage.

Disadvantages of Computer Network

- **It lacks independence.**

  Computer networking involves a process that is operated using computers, so people will be relying more of computer work, instead of exerting an effort for their tasks at hand. Aside from this, they will be dependent on the main file server, which means that, if it breaks down, the system would become useless, making users idle.

- **It poses security difficulties.**

  Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user’s security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.

- **It lacks robustness.**

  As previously stated, if a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To deal with these problems, huge networks should have a powerful computer to serve as file server to make setting up and maintaining the network easier.

- **It allows for more presence of computer viruses and malware.**

  There would be instances that stored files are corrupt due to computer viruses. Thus, network administrators should conduct regular check-ups on the system, and the stored files at the same time.

- **Its light policing usage promotes negative acts.**

  It has been observed that providing users with internet connectivity has fostered undesirable behavior among them. Considering that the web is a minefield of distractions—online games, humor sites and even porn sites—workers could be tempted during their work hours. The huge network of machines could also encourage them to engage in illicit practices, such as instant messaging and file sharing, instead of working on work-related matters. While many organizations draw up certain policies on this, they have proven difficult to enforce and even engendered resentment from employees

- **It requires an efficient handler.**

  For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.

- **It requires an expensive set-up.**

  Though computer networks are said to be an inexpensive system when it is already running, its initial set up cost can still be high depending on the number of computers to be connected. Expensive devices, such as routers, switches, hubs, etc., can add up to the cost. Aside from these, it would also need network interface cards (NICs) for workstations in case they are not built in.

Network Models

There are several classifications for networks

- Classification based on Scale(size)
- Classification based on Topology
- Classification based on Architecture

Based on Scale

Based on the scale (size), networks are classified into following

I. PAN (Personal Area Network)
II. LAN (Local Area Network)
III. CAN (Campus Area Network)
IV. MAN (Metropolitan Area Network)
V. DAN (Desert Area Network)
VI. CAN* (Country Area Network)
VII. WAN (Wide Area Network)
VIII. GAN (Global Area Network)

Personal Area Network (PAN)

- Used for data transmission among devices such as computers, mobile phones, PDA etc.
- Within few meters like 10 meters only
- Medium : Bluetooth, Infrared
- Only very few connections will be available

Local Area Network (LAN)

The term LAN refers to a local network or a group of interconnected network that are under the same administrative control. In the early days of networking, LANS are defined as small networks that existed in a single physical location. While LANs can be a single network installed in a home or small office, the definition of LAN has evolved to include interconnected local networks consisting of many hundreds of hosts, installed in multiple buildings and locations. LANs are designed to Operate within a limited geographic area. Allow Multi-access to high bandwidth media.

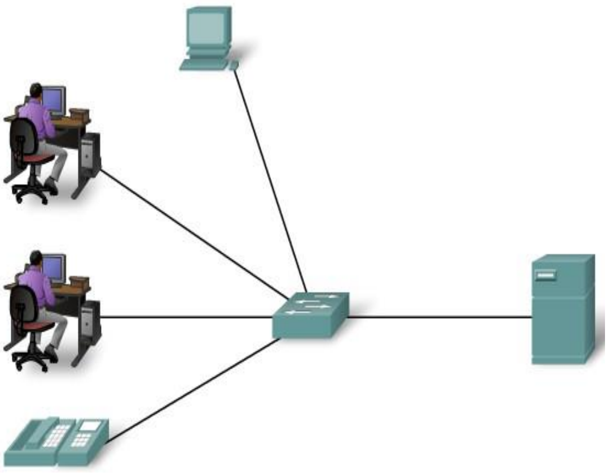
LANs consist of the following components:

- Computers
- Network interface cards
- Peripheral devices
- Networking media
- Network devices

LANs allow businesses to locally sharecompute make internal communications possible. A good example of this technology is email. LANs manage data, local communications, and computing equipment. Some common LAN technologies include the following:

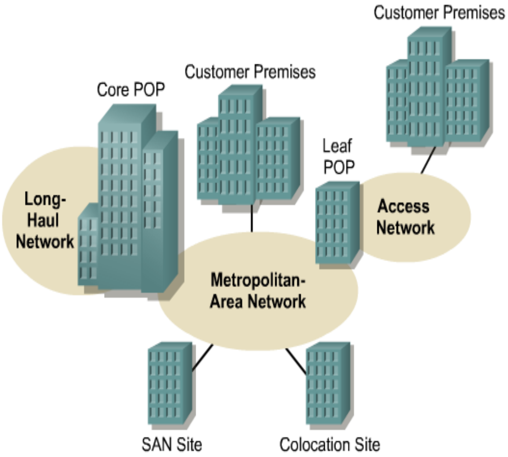
· Ethernet
· Token Ring
· FDDI

A network serving a home, building or campus is considered a Local Area Network (LAN).



Metropolitan Area Network (MAN)

- Metropolitan Area Network, are data networks designed for a town In terms of geographic breadth
- MANs are larger than local area networks (LANs), but smaller than wide-area networks s)
- MANs are usually characterized by very high-speed connections using fiber optical cable or other digital media
- Generally covers towns and cities (50 kms)
- Medium: optical fibers, cables.
- Data rates adequate for distributed computing applications.



Country Area Network (CAN*)

- It's wide area network which is limited to country
- It consist of more than one MAN
- It may be extended up to thousands kms
- It is more public network owned by some public organization or governments
- Example: In Nepal NTC have CAN*

Wide Area Network (WAN)

A network that spans broader geographical area than a local area network over public communication network. WANs interconnect LANs, which then provide access to computers or file servers in other locations. Because WANs connect user networks over a large geographical area, they make it possible for businesses to communicate across great distances. WANs allow computers, printers, and other devices on a LAN to be shared with distant locations. WANs provide instant communications across large geographic areas. Collaboration software provides access to real-time information and resources and allows meetings to be held remotely. WANs have created a new class of workers called telecommuters. These people never have to leave their homes to go to work.

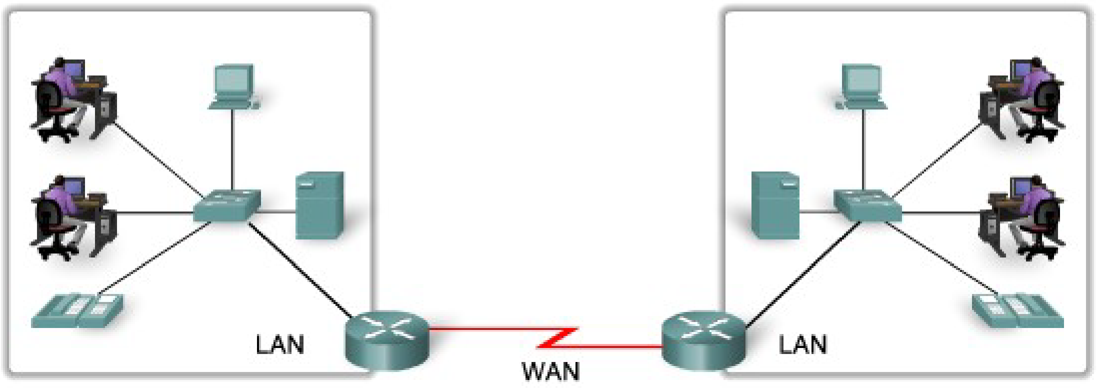
WANs are designed to do the following:

- Operate over a large and geographically separated area
- Allow users to have real-time communication capabilities with other users
- Provide full-time remote resources connected to local services
- Provide e-mail, Internet, file transfer, and e-commerce services

Some common WAN technologies include the following:

- Modems
- Integrated Services Digital Network (ISDN)
- Digital subscriber line (DSL)
- Frame Relay
- T1, E1, T3, and E3
- Synchronous Optical Network (SONET)

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



LAN	WAN
Connects host within a relatively small geographic area. • Same Building • Same room • Same Campus	Hosts may be widely dispersed. • Across Campuses • Across Cities/ Countries/ Continents
Faster	Slower
Cheaper	Expensive
Under a control of single ownership	Not under a control of a single person
Typical Speed: 10 Mbps to 10 Gbps	Typical Speed: 64 Kbps to 8 Mbps

Modes of communication:

Simplex:

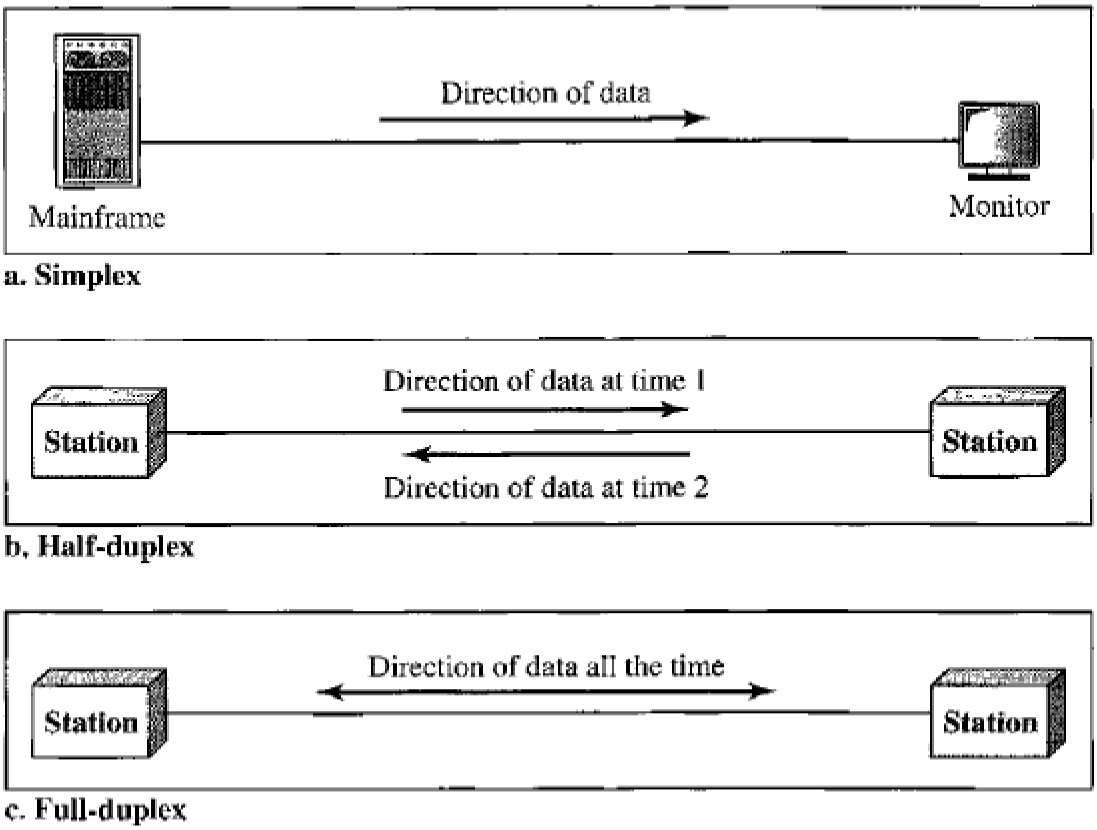
The simplest signal flow technique is the simplex configuration. In Simplex transmission, one of the communicating devices can only send data, whereas the other can only receive it. Here, communication is only in one direction (unidirectional) where one party is the transmitter and the other is the receiver. Examples of simplex communication are the simple radio, and Public broadcast television where, you can receive data from stations but can’t transmit data back. The television station sends out electromagnetic signals. The station does not expect and does not monitor for a return signal from the television set. This type of channel design is easy and inexpensive to set up.

Half-Duplex

Half duplex refers to two-way communication where, only one party can transmit data at a time. Unlike, the Simplex mode here, both devices can transmit data though, not at the same time, that is Half duplex provides Simplex communication in both directions in a single channel. When one device is sending data, the other device must only receive it and vice versa. Thus, both sides take turns at sending data. This requires a definite turnaround time during which, the device changes from the receiving mode to the transmitting mode. Due to this delay, half duplex communication is slower than simplex communication. However, it is more convenient than simplex communication as both the devices can send and receive data. For example, a walkie-talkie is a half-duplex device because only one party can talk at a time.

Full Duplex

Full duplex refers to the transmission of data in two directions simultaneously. Here, both the devices are capable of sending as well as receiving data at the same time as. Sharing the same channel and moving signals in both directions increases the channel throughput without increasing its bandwidth. For example, a telephone is a full-duplex device because both parties can talk to each other simultaneously.


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

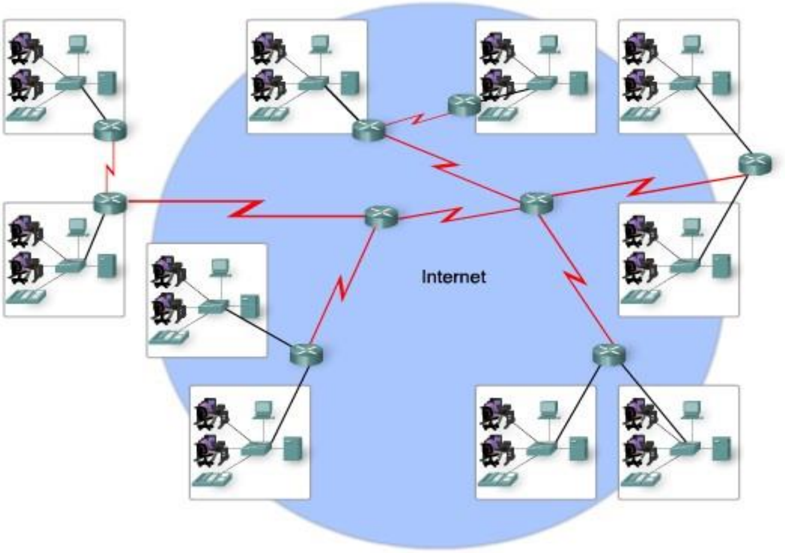
c. Full-duplex

Internet:

The network formed by the co-operative interconnection of a large number of computer networks.

- Network of Networks
- No one owns the Internet
- Every person who makes a connection owns a slice of the Internet.
- There is no central administration of the Internet.

LANs and WANs may be connected into internetworks.



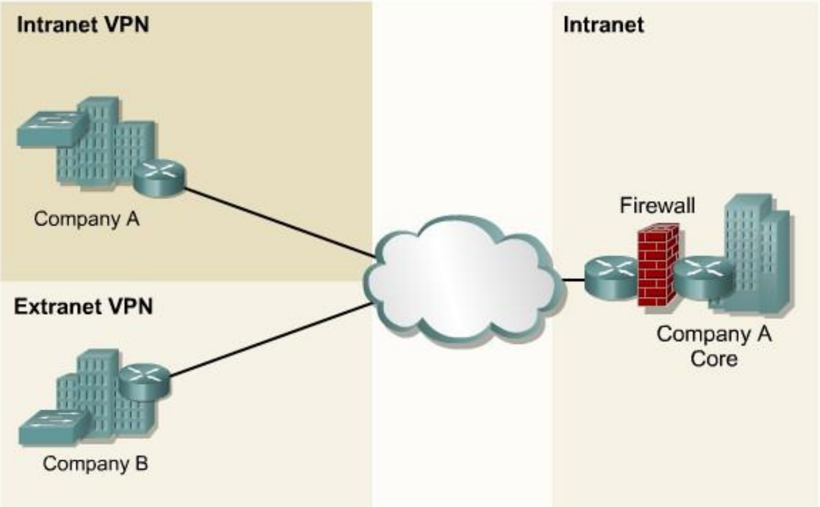
Internet is comprises of :
A community of people: who use and develop the network.
A collection of resources: that can be reached from those networks.
A setup to facilitate collaboration: Among the members of the research and educational communities worldwide.
The connected networks use the TCP/IP protocols:

Important Internet applications:
world wide web(WWW)
File Transfer Protocol(FTP)
Electronic Mail
Internet Relay Chat

Intranet:

A private TCP/IP internetwork within an organization that uses Internet technologies such as Web servers and Web browsers for sharing information and collaborating. Intranets can be used to publish company policies and newsletters, provide sales and marketing staff with product information, provide technical support and tutorials, and just about anything else you can think of that fits within the standard Web server/Web browser environment.

Intranet Web servers differ from public Web servers in that the public must have the proper permissions and passwords to access the intranet of an organization. Intranets are designed to permit users who have access privileges to the internal LAN of the organization. Within an intranet, Web servers are installed in the network. Browser technology is used as the common front end to access information on servers such as financial, graphical, or text-based data.



Extranet:

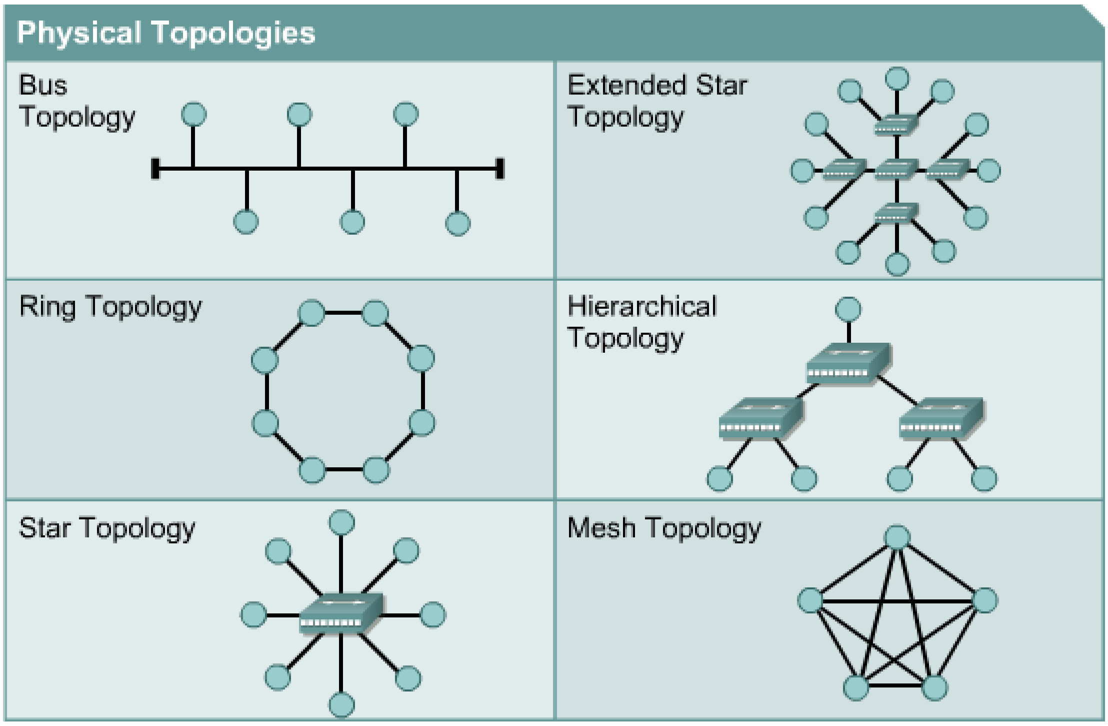
Extranets refer to applications and services that are Intranet based, and use extended, secure access to external users or enterprises. This access is usually accomplished through passwords, user IDs, and other application-level security. An extranet is the extension of two or more intranet strategies with a secure interaction between participant enterprises and their respective intranets.

Part of a Company's Intranet that is extended to users outside the company (eg Normally over the Internet). In its simplest form, a private TCP/IP network that securely shares information using Hypertext Transfer Protocol (HTTP) and other Internet protocols with business partners such as vendors, suppliers, and wholesale customers. An extranet is thus a corporate intranet that is exposed over the Internet to certain specific groups that need access to it. Extranets built in this fashion follow the client/server paradigm, with Web servers such as Apache.

Extranets are a powerful tool because they let businesses share resources on their own private networks over the Internet with suppliers, vendors, business partners, or customers. Extranets are typically used for supporting real-time supply chains, for enabling business partners to work together, or to share information such as catalogs with customers. The power of the extranet is that it leverages the existing technology of the Internet to increase the power, flexibility, and competitiveness of businesses utilizing well-known and easily used tools such as Web servers and Web browsers. Extranets also save companies money by allowing them to establish business-to-business connectivity over the Internet instead of using expensive, dedicated leased lines. Extranets can also save money by reducing phone and fax costs.

Physical Topology and Logical Topology:

Physical Topology: The term physical topology refers to the way in which a network is laid out physically. The actual layout of the wire or media. Two or more devices connect to a link; two or more links form a topology.
Logical Topology: Defines how the hosts access the media to send data. Shows the flow of data on a network.



Bus Topology:

A networking topology that connects networking components along a single cable or that uses a series of cable segments that are connected linearly. A network that uses a bus topology is referred to as a "bus network." Bus networks were the original form of Ethernet networks, using the 10Base5 cabling standard. Bus topology is used for:

- Small work-group local area networks (LANs) whose computers are connected using a thinnet cable
- Trunk cables connecting hubs or switches of departmental LANs to form a larger LAN
- Backboning, by joining switches and routers to form campus-wide networks

Advantages:

- Easy to install
- Costs are usually low
- Easy to add systems to network
- Great for small networks

Disadvantages:

- Out of date technology.
- Include difficult reconnection and fault isolation

- Can be difficult to troubleshoot.
- Unmanageable in a large network
- If cable breaks, whole network is down

Ring Topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Advantages:

- Very orderly network where every device has access to the token and the opportunity to transmit.
- Performs better than a bus topology under heavy network load
- Does not require network server to manage the connectivity between the computers

Disadvantage:

- One malfunctioning workstation or bad port in the MAU can create problems for the entire network
- Moves, adds and changes of devices can affect the network
- Network adapter cards and MAU's a Multistation Access Unit are much more expensive than Ethernet cards and hubs
- Much slower than an Ethernet network under normal load

Mesh Topology:

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To connect n nodes in Mesh topology, we require n(n-1)/2 duplex mode links.

Advantages:

- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

- Robust: If one link becomes unusable, it does not incapacitate the entire system.
- Advantage of privacy or security.
- point-to-point links make fault identification and fault isolation easy , Traffic can be routed to avoid links with suspected problems.

Disadvantage:

- Required high amount of cabling and the number of I/O ports.
- The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology:

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

Advantages:

- Less Expensive than Mesh topology.
- In a star topology, each device needs only one link and one I/O port to connect it to any number of other devices. This factor also makes it easy to install and reconfigure.
- Less Cabling, Addition and Deletion involves only one connection between the devices and the Hub or Switch.
- Easy for Fault identification and fault isolation. If one link fails, only that link is affected. All other links remain active.

Disadvantage:

- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

An extended star topology links individual stars together by connecting the hubs or switches.

A hierarchical topology is similar to an extended star. However, instead of linking the hubs or switches together, the system is linked to a computer that controls the traffic on the topology.

Logical Topology:

The logical topology of a network determines how the hosts communicate across the medium. The two most common types of logical topologies are **broadcast** and **token passing**.

The use of a **broadcast topology** indicates that each host sends its data to all other hosts on the network medium. There is no order that the stations must follow to use the network. It is first come, first serve. Ethernet works this way as will be explained later in the course.

The second logical topology is **token passing**. In this type of topology, an electronic token is passed sequentially to each host. When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself. Two examples of networks that use token passing are Token Ring and Fiber Distributed Data Interface(FDDI). A variation of Token Ring and FDDI is Arcnet. Arcnet is token passing on a bus topology.

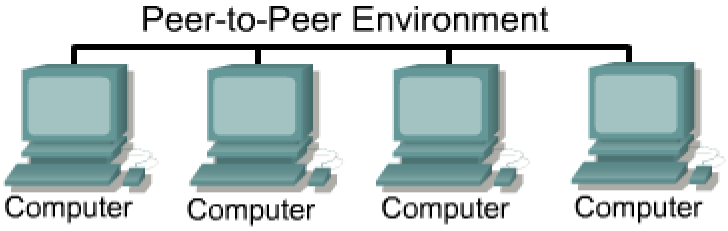
Network Architecture:

Two types of Network Architecture:

I. Peer-to-Peer Model
II. Client-server Model

Peer-to-Peer Model:

In a peer-to-peer network, networked computers act as equal partners, or peers. As peers, each computer can take on the client function or the server function. Computer A may request for a file from Computer B, which then sends the file to Computer A. Computer A acts like the client and Computer B acts like the server. At a later time, Computers A and B can reverse roles.



In a peer-to-peer network, individual users control their own resources. The users may decide to share certain files with other users. The users may also require passwords before they allow others to access their resources. Since individual users make these decisions, there is no central point of control or administration in the network. In addition, individual users must back up their own systems to be able to recover from data loss in case of failures. When a computer acts as a server, the user of that machine may experience reduced performance as the machine serves the requests made by other systems.

As networks grow, peer-to-peer relationships become increasingly difficult to coordinate. A peer-to-peer network works well with ten or fewer computers. Since peer-to-peer networks do not scale well, their efficiency decreases rapidly as the number of computers on the network increases. Also, individual users control access to the resources on their computers, which means security may be difficult to maintain. The client/server model of networking can be used to overcome the limitations of the peer-to-peer network.

Peer-to-peer networks are relatively easy to install and operate. No additional equipment is necessary beyond a suitable operating system installed on each computer. Since users control their own resources, no dedicated administrators are needed.

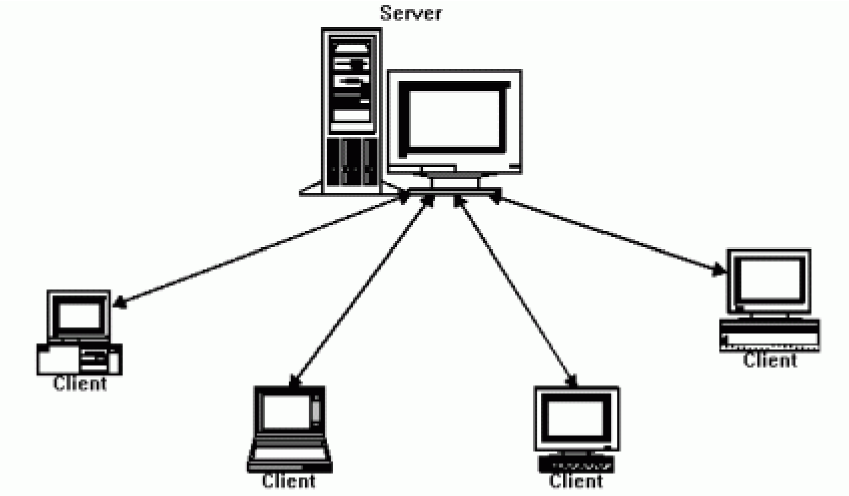
The advantages of peer-to-peer:

- No need for a network administrator.
- Network is fast/inexpensive to setup & maintain
- Each PC can make backup copies of its data to other PCs for security.
- Easiest type of network to build, peer-to-peer is perfect for both home and office use.

Client-server Model:

The term client-server refers to a popular model for computer networking that utilizes client and server devices each designed for specific purposes. The client-server model can be used on the Internet as well as local area networks (LANs). Examples of client-server systems on the Internet include Web browsers and Web servers, FTP clients and servers, and DNS.

In a client/server arrangement, network services are located on a dedicated computer called a server. The server responds to the requests of clients. The server is a central computer that is continuously available to respond to requests from clients for file, print, application, and other services. Most network operating systems adopt the form of a client/server relationship. Typically, desktop computers function as clients and one or more computers with additional processing power, memory, and specialized software function as servers.



Servers are designed to handle requests from many clients simultaneously. Before a client can access the server resources, the client must be identified and be authorized to use the resource. Each client is assigned an account name and password that is verified by an authentication service. The authentication service guards access to the network. With the centralization of user accounts, security, and access control, server-based networks simplify the administration of large networks. The concentration of network resources such as files, printers, and applications on servers also makes it easier to back-up and maintain the data. Resources can be located on specialized, dedicated servers for easier access. Most client/server systems also include ways to enhance the network with new services that extend the usefulness of the network.

The centralized functions in a client/server network has substantial advantages and some disadvantages. Although a centralized server enhances security, ease of access, and control, it introduces a single point of failure into the network. Without an operational server, the network cannot function at all. Servers require a trained, expert staff member to administer and maintain. Server systems also require additional hardware and specialized software that add to the cost.

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfill the request. Although programs within a single computer can use the client/server idea, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client/server model are very common. For example, to check your bank account from your computer, a client program in your computer forwards your request to a server program at the bank. That program might in turn forward the request to its own client program that sends a request to a database server at another bank computer to retrieve your account balance. The balance is returned back to the bank data client, which in turn serves it back to the client in your personal computer, which displays the information for you.

Advantages: Flexibility of the system, scalability, cost saving, centralized control and implementation of business rules, increase of developers productivity, portability, improved network and resource utilization.

Client-server Vs Peer-to-Peer Network:

Advantages of a Peer-to-Peer Network	Advantages of a client-server Network
Less Expensive to implementation	Provides of better security
Does not require additional specialized network administration software.	Easier to administer when the network is large because administration is centralized
Does not require a dedicated network administrator.	All date can be backed up on one central location.
Disadvantages of a Peer-to-Peer Network	Disadvantage of a Client-server Network
Does not scale well to large network and administration become unmanageable.	Requires expensive, specialized network administrative and operational software.
Less Secure	Requires a professional administrator.
All machine sharing the resources negatively impact the performance.	a single point of failure. User data is unavailable if the server is down.
Each user must be trained to perform administrative tasks.	Requires more expensive, more powerful hardware for the server machine.