Computer Network

A **computer network**, or **data network**, is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections between nodes (data links.) These data links are established over cable media such as wires or optic cables, or wireless media such as WiFi.

Network computer devices that originate, route and terminate the data are called network node. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Evolution of Computer Network

The term *computer networks* resulted from the 'combination of two major areas, namely *computers* and *communications*.

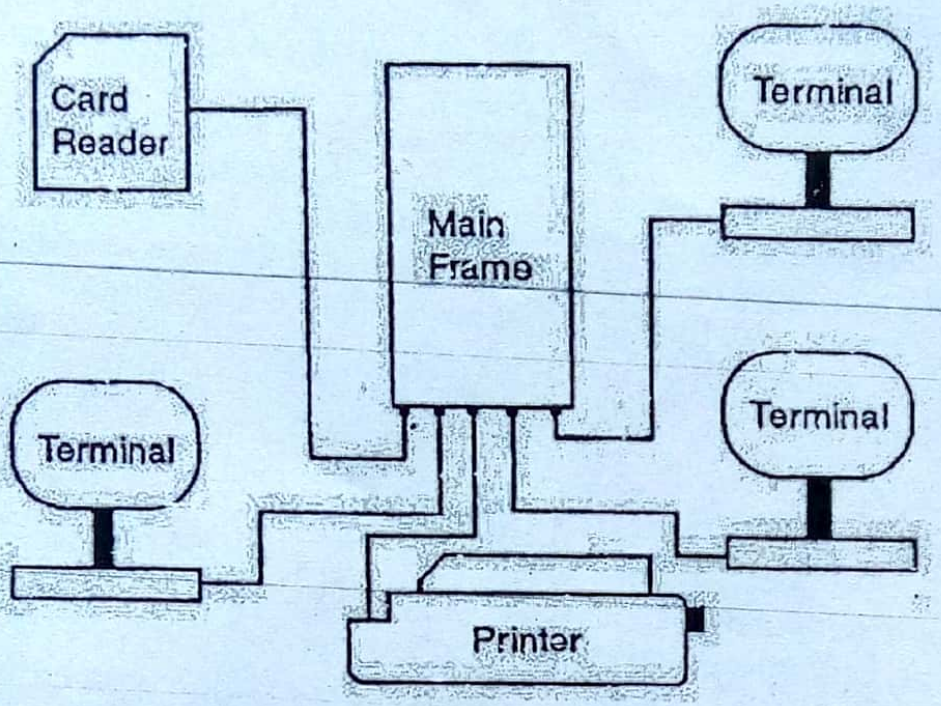
It was during the 1950's, that computers were treated as large complex machines and were operated by specially trained people. Jobs were given to computers in the form of batches. Punched cards, paper tapes, or magnetic tapes were used as input devices. There was no direct communication or interaction between the user and the computer. Users suffered with extremely long delays between the submission of jobs and the receipt of output results. The computer model resembles the one shown in Figure. Note that there are two queues, one at the input device and another at the output device.

In the 1960's, interactive terminals were developed. Remote users can be connected to a large mainframe computer via a low speed data line. The network resembles the one shown in Figure.

When more devices are' connected to a computer, it is not so economical to have a separate communication line from each device to the computer. To solve this problem, multiplexers and concentrators were developed. These devices collect the output from a set of peripheral devices and send it over a common communication link. Special communication processors called *front-ends* were developed to relieve the mainframe computers from performing all the communication functions.

Time-sharing systems were developed and that led to the development of many applications centered on a single computer. The concept of a large-scale, general-purpose network was developed. Such a network consists of a set of nodes called network switches or interface message processors (IMP) connected by means of interconnecting transmission links. Interconnecting links can be a wire, microwave radio, optical fiber, or satellite communication links. Nodes are located at geographically

separated locations. Each node forwards the message passing through it to the next node in the concerned path.



Mainframe Computer

As technology advanced, inexpensive personal computers started replacing medium and large systems in many commercial and educational institutions. Local Area Networks (LAN) were developed. A LAN is capable of sharing expensive resources like laser printers, enterprise software, etc., and provides access to a large database. LANs were initially used for the purpose of connecting people. It supports high speed switching. Special software known as *Network* OS was developed to manage and control the access of these Local Area Networks. The users demanded access to resources outside the LAN. The most common resources were printers and large databases. These resources may be components of other LAN. Remote file transfer and remote login were then developed. The concept of Wide Area Networking (WAN) evolved by interconnecting hundreds of thousands of Local Area Networks.

History

1940

George Stibitz, who is internationally recognised as one of the fathers of the first modern digital computer, uses a teletype (an electromechanical typewriter that can be used to send and receive typed messages) to send commands to the Complex Number Computer in New York over telegraph lines. It was the first computing machine ever used remotely.

1964

American Airlines calls on IBM to implement the SABRE reservation system and online transaction processing is born. Using telephone lines, SABRE links 2,000 terminals in 65 cities to a pair of IBM 7090 computers and is able to deliver data on any flight in less than three seconds. Before the introduction of SABRE, the American Airlines' system for booking flights was entirely manual. It consisted of a team of eight operators who sorted through a rotating file with cards for every flight.

1980s

Access to the ARPANET is expanded in 1981. In 1982, the internet protocol suite (TCP/IP) is introduced as the standard networking protocol on the ARPANET. In the early 1980s the NSF funds the establishment for national supercomputing centers at several universities, and provides interconnectivity in 1986 with the NSFNET project, which also created network access to the supercomputer sites in the United States from research and education organisations. Commercial Internet service providers (ISPs) begin to emerge in the late 1980s.

2000s

In the UK, on March 31st 2000, Telewest launches home ADSL – asymmetric digital subscriber line. Goldsmith Road in Gillingham, Kent, is the first street to receive the technology. In 2002, there were fewer than 200,000 broadband users, but just four years later, there were around 13 million.

2005

Box launches an online file sharing and personal cloud content management service for businesses. By 2006 Amazon Web Services introduces its cloud storage service and gains widespread recognition as the storage supplier to emerging services such as Dropbox and Pinterest.

2011

Fiber-optic broadband and new DOCSIS standards make broadband speeds easily reach 100Mbps. This in turn means end users need better routers to match the broadband speed.

2014

The new Wi-Fi standard 802.11ac launches, offering faster speed (over 2Gbps) compared to 450Mbps of the previous 802.11n standard. Along with this comes better signal coverage. 802.11ac was ratified in 2014.

2016

Beyond ....Now we know how the market has evolved, what's in store for the networking sector in the future?

Basic computer network components

Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card(NIC), local operating system(LOS), and the network operating system (NOS).

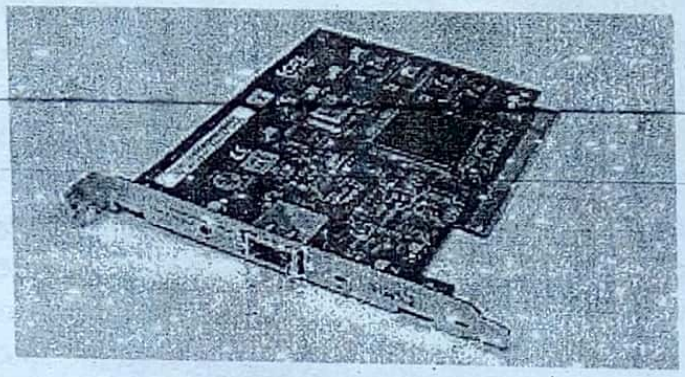
Key Components of Network – I Unit.

1. **Servers** - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, print servers, fax servers and web servers, to name a few.
2. **Clients** - Clients are computers that access and use the network and shared network resources. Client computers are basically the customers(users) of the network, as they request and receive services from the servers.
3. **Transmission Media** - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called channels, links or lines.
4. **Shared data** - Shared data are data that file servers provide to clients such as data files, printer access programs and e-mail.
5. **Shared printers and other peripherals** - Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.
6. **Network Interface Card** - Each computer in a network has a special expansion card called a network interface card (NIC). The NIC prepares(formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents.
7. **Local Operating System** - A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, Unix, Linux, Windows 2000, Windows 98, Windows XP etc.
8. **Network Operating System** - The network operating system is a program that runs on computers and servers, and allows the computers to communicate over the network.
9. **Hub** - Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.
10. **Switch** - Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming messages so that it can deliver the message to the right destination or port.

Like a hub, switch doesn't broadcast the received message to entire network; rather before sending it checks to which system or port should the message be sent. In other words, switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

11. **Network nodes- Apart from any physical transmission medium there may be, networks comprise additional basic system building blocks, such as network interface controller (NICs), repeaters, hubs, bridges, switches, routers, modems, and firewalls.**

Network interfaces



An ATM network interface in the form of an accessory card. A lot of network interfaces are built-in.

A network interface controller (NIC) is computer hardware that provides a computer with the ability to access the transmission media, and has the ability to process low-level network information. For example the NIC may have a connector for accepting a cable, or an aerial for wireless transmission and reception, and the associated circuitry.

The NIC responds to traffic addressed to a network address for either the NIC or the computer as a whole.

In Ethernet networks, each network interface controller has a unique Media Access Control (MAC) address—usually stored in the controller's permanent memory. To avoid address conflicts between network devices, the Institute of Electrical and Electronics Engineers (IEEE) maintains and administers MAC address uniqueness. The size of an Ethernet MAC address is six octets. The three most significant octets are reserved to identify NIC manufacturers. These manufacturers, using only their assigned prefixes, uniquely assign the three least-significant octets of every Ethernet interface they produce.

12. ***Repeaters and hubs***

A repeater is an electronic device that receives a network signal, cleans it of unnecessary noise, and regenerates it. The signal is retransmitted at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. With fiber optics, repeaters can be tens or even hundreds of kilometers apart.

A repeater with multiple ports is known as a hub. Repeaters work on the physical layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay that affects network performance. As a result, many network architectures limit the number of repeaters that can be used in a row, e.g., the Ethernet 5-4-3 rule.

Hubs have been mostly obsoleted by modern switches; but repeaters are used for long distance links, notably undersea cabling.

13. *Bridges*

A network bridge connects and filters traffic between two network segments at the data link layer (layer 2) of the OSI model to form a single network. This breaks the network's collision domain but maintains a unified broadcast domain. Network segmentation breaks down a large, congested network into an aggregation of smaller, more efficient networks.

Bridges come in three basic types:

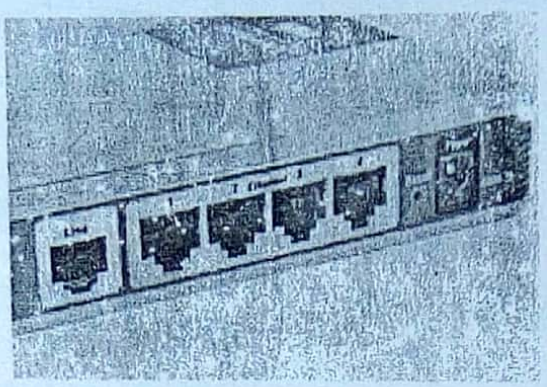
- Local bridges: Directly connect LANs
- Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.
- Wireless bridges: Can be used to join LANs or connect remote devices to LANs.

14. *Switches*

A network switch is a device that forwards and filters OSI layer 2 datagrams between ports based on the MAC addresses in the packets.[8] A switch is distinct from a hub in that it only forwards the frames to the physical ports involved in the communication rather than all ports connected. It can be thought of as a multi-port bridge.[9] It learns to associate physical ports to MAC addresses by examining the source addresses of received frames. If an unknown destination is targeted, the switch broadcasts to all ports but the source. Switches normally have numerous ports, facilitating a star topology for devices, and cascading additional switches.

Multi-layer switches are capable of routing based on layer 3 addressing or additional logical levels. The term *switch* is often used loosely to include devices such as routers and bridges, as well as devices that may distribute traffic based on load or based on application content (e.g., a Web URL identifier).

15. Routers



A typical home or small office router showing the ADSL telephone line and Ethernet network cable connections

A router is an internetworking device that forwards packets between networks by processing the routing information included in the packet or datagram (Internet protocol information from layer 3). The routing information is often processed in conjunction with the routing table (or forwarding table). A router uses its routing table to determine where to forward packets. (A destination in a routing table can include a "null" interface, also known as the "black hole" interface because data can go into it, however, no further processing is done for said data.)

16. Modems

Modems (MOdulator-DEModulator) are used to connect network nodes via wire not originally designed for digital network traffic, or for wireless. To do this one or more frequencies are modulated by the digital signal to produce an analog signal that can be tailored to give the required properties for transmission. Modems are commonly used for telephone lines, using a Digital Subscriber Line technology.

17. Firewalls

A firewall is a network device for controlling network security and access rules. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.

Network structure

Network topology is the layout or organizational hierarchy of interconnected nodes of a computer network. Different network topologies can affect throughput, but reliability is often more critical. With many technologies, such as bus networks, a single failure can cause the network to fail entirely. In general the more interconnections there are, the more robust the network is; but the more expensive it is to install.

Characteristics of Computer Networking:

A computer network is a system in which multiple computers are connected to each other to share information and resources between them or their users.

- Share Resources from one computer to another
- Create files and store them in one computer, access those files from the other computer(s) connected over the network
- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over network.
- The ability to exchange data and communicate efficiently is the main purpose of computers networking. But we have to consider beyond these points to evaluate the feasibility of networking for our own advantages.

Advantages of Computer Networking

1. Easy Communication and Speed

It is very easy to communicate through a network. People can communicate efficiently using a network with a group of people. They can enjoy the benefit of emails, instant messaging, telephony, video conferencing, chat rooms, etc.

2. Ability to Share Files, Data and Information

This is one of the major advantages of networking computers. People can find and share information and data because of networking. This is beneficial for large organizations to maintain their data in an organized manner and facilitate access for desired people.

3. Sharing Hardware

Another important advantage of networking is the ability to share hardware. For an example, a printer can be shared among the users in a network so that there's no need to have individual printers for each and every computer in the company. This will significantly reduce the cost of purchasing hardware.

4. Sharing Software

Users can share software within the network easily. Networkable versions of software are available at considerable savings compared to individually licensed version of the same software. Therefore large companies can reduce the cost of buying software by networking their computers.

5. Security

Sensitive files and programs on a network can be password protected. Then those files can only be accessed by the authorized users. This is another important advantage of networking when there are concerns about security issues. Also each and every user has their own set of privileges to prevent them accessing restricted files and programs.

6. Speed

Sharing and transferring files within networks is very rapid, depending on the type of network. This will save time while maintaining the integrity of files.

Disadvantages of Networking

1. Breakdowns and Possible Loss of Resources

One major disadvantage of networking is the breakdown of the whole network due to an issue of the server. Such breakdowns are frequent in networks causing losses of thousands of dollars each year. Therefore once established it is vital to maintain it properly to prevent such disastrous breakdowns. The worst scenario is such breakdowns may lead to loss of important data of the server.

2. Expensive to Build

Building a network is a serious business in many occasions, especially for large scale organizations. Cables and other hardware are very pricey to buy and replace.

3. Security Threats

Security threats are always problems with large networks. There are hackers who are trying to steal valuable data of large companies for their own benefit. So it is necessary to take utmost care to facilitate the required security measures.

4. Bandwidth Issues

In a network there are users who consume a lot more bandwidth than others. Because of this some other people may experience difficulties.

Although there are disadvantages to networking, it is a vital need in today's environment. People need to access the Internet, communicate and share information and they can't live without that. Therefore engineers need to find alternatives and improved technologies to overcome issues associated with networking. Therefore we can say that computer networking is always beneficial to have even if there are some drawbacks.

Following is the list of hardware's required to setup a computer network.

- Network Cables
- Distributors
- Routers
- Internal Network Cards
- External Network Cards

Network strategy

Network strategy is made to build, shape and design network infrastructure according to requirements and demands. We:

- Network is designed for data sharing and data storage, with expanded capacity and to store a large amount of data.
- Strategy for network design is planned depending upon its nature. Computer network design can be implemented in star, ring, bus or other shapes.
- The implementation of network is planned after finalizing its design and structure with hardware and software. Cabling and connectivity solutions are made which best suits your business and budget.
- Special security solutions including firewalls installation, virus defenders, employee internet management and SPAM management are installed to avoid any type of future issues.
- Our technicians plan a computer network strategy in a flexible way so that you can easily expand the network whenever needed.

- Provide computer network strategy plan and building services by experts.
- Make an effective strategic diagram to execute a best networking plan.
- Identify the requirements and necessities and plan the network strategy by using latest equipment and technology.
- Manage networking solutions after making this effective strategy.
- Select the appropriate technology with strong and reliable back up and security solutions, and constantly monitor and assess the business or home network design for the upgradation.
- Best and latest hardware devices and software applications are planned to raise the functionality standards of network.

LAN vs. WAN vs. MAN

LAN, which stands for **local area network**, and **WAN**, which stands for **wide area network**, are two types of networks that allow for interconnectivity between computers. As the naming conventions suggest, LANs are for smaller, more localized networking — in a home, business, school, etc. — while WANs cover larger areas, such as cities, and even allow computers in different nations to connect. LANs are typically faster and more secure than WANs, but WANs enable more widespread connectivity. And while LANs tend to be owned, controlled and managed in-house by the organization where they are deployed, WANs typically require two or more of their constituent LANs to be connected over the public Internet or via a private connection established by a third-party telecommunications provider.

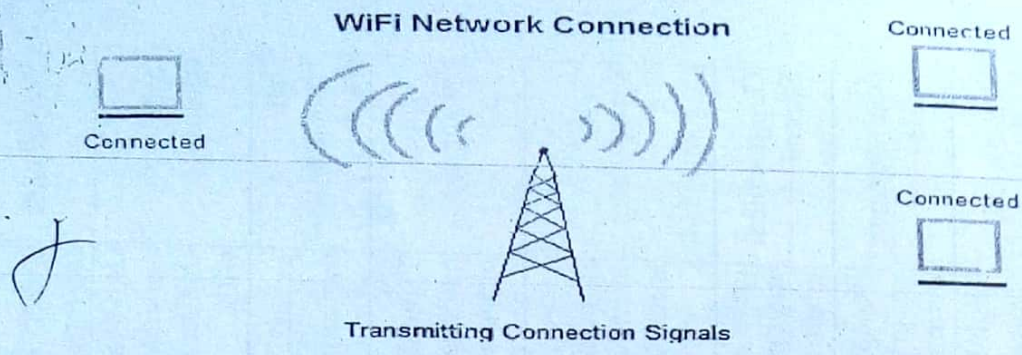
LAN vs. WAN vs. MAN — Difference b/w LAN, WAN, MAN

LAN, which stands for **local area network**, and **WAN**, which stands for **wide area network**, are two types of networks that allow for interconnectivity between computers. As the naming conventions suggest, LANs are for smaller, more localized networking — in a home, business, school, etc. — while WANs cover larger areas, such as cities, and even allow computers in different nations to connect. LANs are typically faster and more secure than WANs, but WANs enable more widespread connectivity. And while LANs tend to be owned, controlled and managed in-house by the organization where they are deployed, WANs typically require two or more of their constituent LANs to be connected over the public Internet or via a private connection established by a third-party telecommunications provider.

Comparison chart

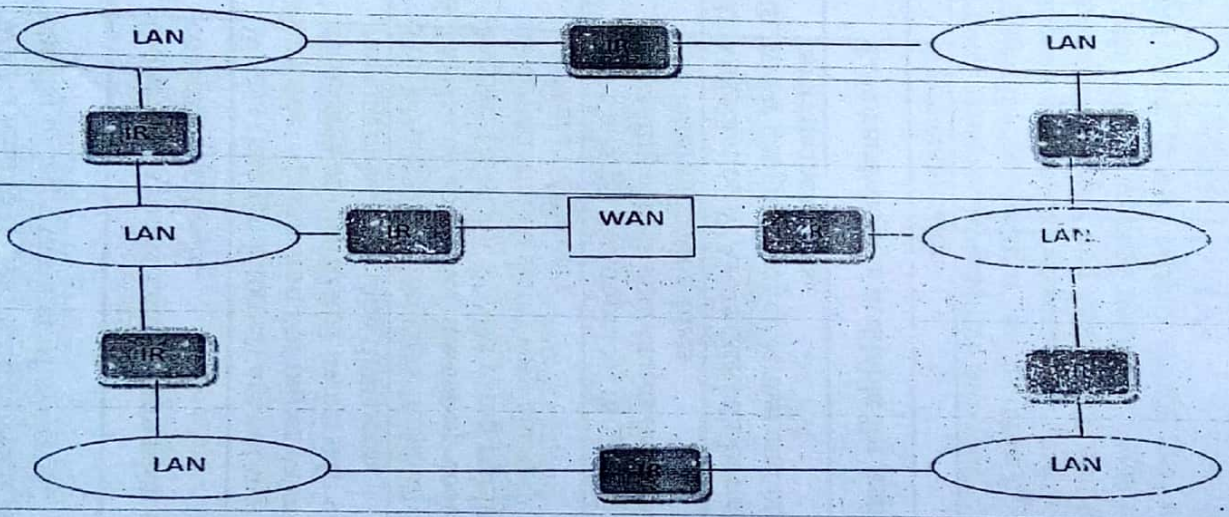
	LAN	WAN	MAN
Stands For	Local Area Network	Wide Area Network	Metropolitan Area Networks
Covers	Local areas only (e.g., homes, offices, schools)	Large geographic areas (e.g., cities, states, nations)	covers the area inside a town or a city.
Definition	LAN (Local Area Network) is a computer network covering a small geographic area, like a home, office, school, or group of buildings.	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).	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.
Speed	High speed (1000 mbps)	Less speed (150 mbps)	moderate speed(44 to 155 Mbps)
Data transfer rates	LANs have a high data transfer rate.	WANs have a lower data transfer rate compared to LANs.	high data rate but less than LAN
Example	The network in an office building can be a LAN	The Internet is a good example of a WAN	The network in city building can be a MAN
Technology	Tend to use certain connectivity technologies, primarily Ethernet and Token Ring	WANs tend to use technologies like MPLS, ATM, Frame Relay and X.25 for connectivity over longer distances	Tend to use certain connectivity technologies, primarily ATM, SMDS , FDDI
Connection	One LAN can be connected to other LANs over any distance via telephone lines and radio waves.	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.	A Metropolitan Area Networks bridges a number of 'Local Area Networks' with a fiber-optical links

	LAN	WAN	MAN
Components	Layer 2 devices like switches and bridges.Layer 1 devices like hubs and repeaters.	Layers 3 devices Routers, Multi-layer Switches and Technology specific devices like ATM or Frame-relay Switches etc.	switches, routers
Fault Tolerance	LANs tend to have fewer problems associated with them, as there are smaller number of systems to deal with.	WANs tend to be less fault tolerant as they consist of large number of systems.	less fault tolerance
Data Transmission Error	Experiences fewer data transmission errors	Experiences more data transmission errors as compared to LAN	high data transmission error/bit error rate is more
Ownership	Typically owned, controlled, and managed by a single person or organization.	WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management over long distances.	The MANs are publicly owned, while allowing all telecommunication operators open access to the networks
Set-up costs	If there is a need to set-up a couple of extra devices on the network, it is not very expensive to do that.	For WANs since networks in remote areas have to be connected the set-up costs are higher. However WANs using public networks can be setup very cheaply using just software (VPN etc).	If there is a need to set-up a couple of extra devices on the network, it is expensive to do that.
Geographical Spread	Have a small geographical range and do not need any leased telecommunication lines	Have a large geographical range generally spreading across boundaries and need leased telecommunication lines	Have a large geographical range
Maintenance costs	Because it covers a relatively small geographical area, LAN is easier to maintain at relatively low costs.	Maintaining WAN is difficult because of its wider geographical coverage and higher maintenance costs.	maintenance cost is more than that of LAN
Bandwidth	High bandwidth is available for transmission.	Low bandwidth is available for transmission.	less bandwidth
Congestion	Less congestion	More congestion	more congestion



Inter Network

When we connect two or more networks then they are called internetwork or internet. We can join two or more individual networks to form an internetwork through devices like routers gateways or bridges.



INTERNETWORK

Chapter 8
Communication and Connectivity

Introduction

Data communication is the exchange of data between two (or more) devices via some form of transmission medium. Data communication may be considered local or remote. Data communication refers to the exchange of data between a source and a receiver. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area. The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.

Note: In computer information systems, data are represented by binary information units (bits) produced and consumed in the form of 0s and 1s. The efficiency of a data communication system depends on three fundamental characteristics:

1. Delivery
2. Accuracy
3. Timeliness

Datum mean the facts information statistics or the like derived by calculation or experimentation. The facts and information so gathered are processed in accordance with defined systems of procedure. Data can exist in a variety of forms such as numbers, text, bits and bytes. The Figure is an illustration of a simple data communication system.

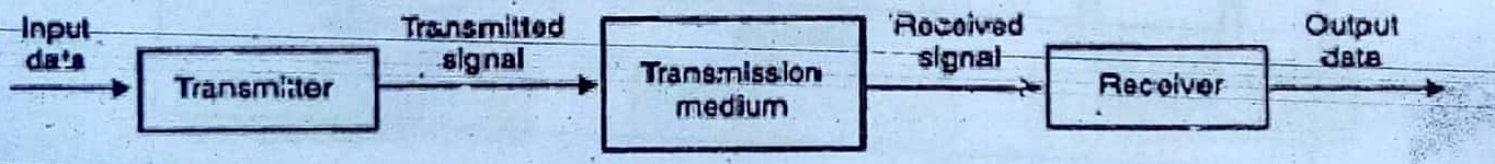


Figure 8.1 Block diagram of Data Communication System

A data communication system may collect data from remote locations through data transmission circuits, and then outputs processed results to remote locations. Figure provides a broader view of data communication networks. The different data communication techniques which are presently in widespread use evolved gradually either to improve the data communication techniques already existing or to replace the same with better options and features. Then, there are data communication jargons to contend with such as baud rate, modems, routers, LAN, WAN, TCP/IP, ISDN, during the selection of communication systems. Hence, it becomes necessary to review and understand these terms and gradual development of data communication methods.

Components of data communication system

A Communication system has following components:

1. **Message**: It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.
2. **Sender**: It is the device/computer that generates and sends that message.
3. **Receiver**: It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.
4. **Medium**: It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.
5. **Protocol**: It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.

A protocol performs the following functions:

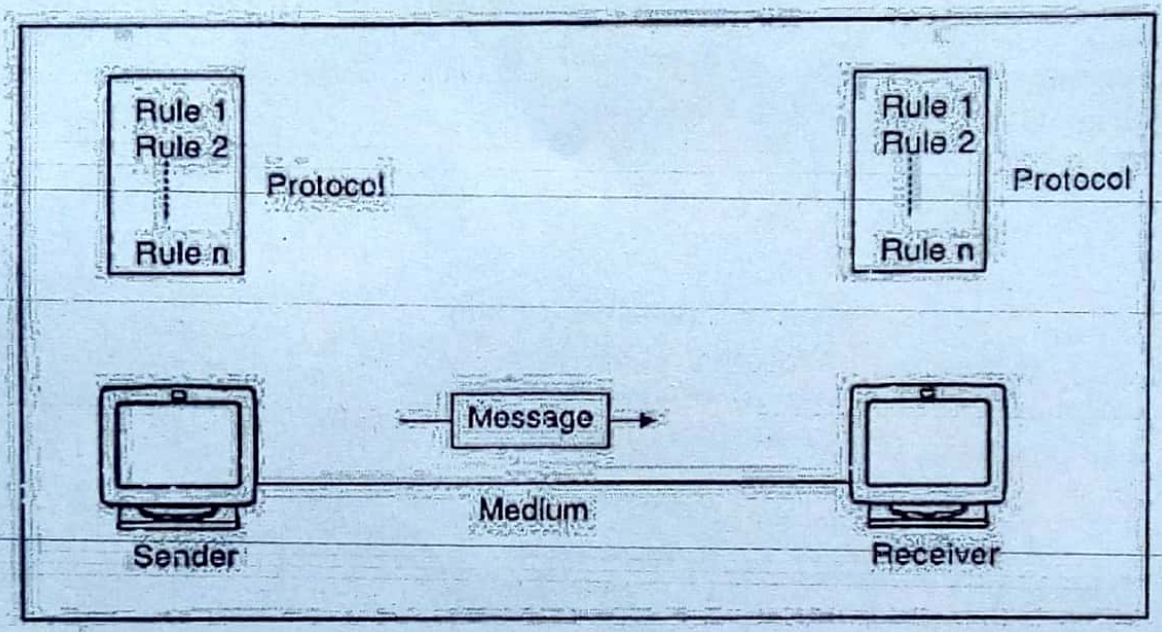


Figure 8.2 Block diagram of Data Communication System by using protocol rules

1. Data sequencing. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.
2. Data routing. Data routing defines the most efficient path between the source and destination.
3. Data formatting. Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.
4. Flow control. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on 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 is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

6. Precedence and order of transmission. These rules ensure that all the 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 define 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.

Transmission Mode

The term Transmission Mode defines the direction of the flow of information between two communication devices i.e. it tells the direction of signal flow between the two devices.

The transmission is characterized by:

- the direction of the exchanges
- the transmission mode: the number of bits sent simultaneously
- synchronization between the transmitter and receiver

There are three ways or modes of data transmission: Simplex, Half duplex (HDX), Full duplex (FDX)

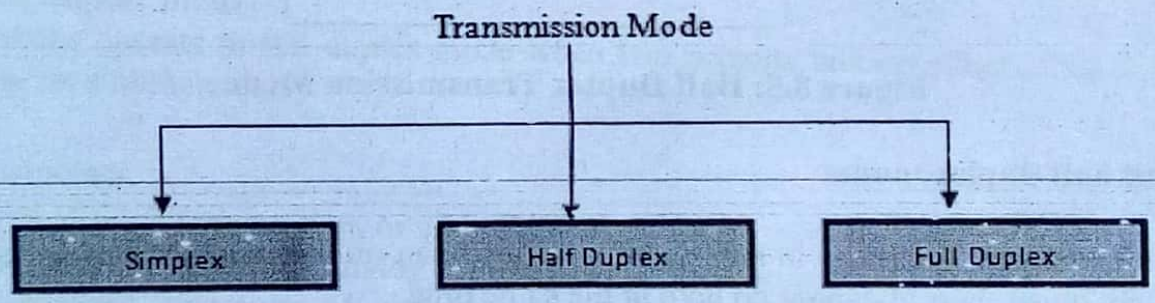


Figure 8.3: Transmission Mode

Simplex

In this type of transmission mode data can be sent only through one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems.

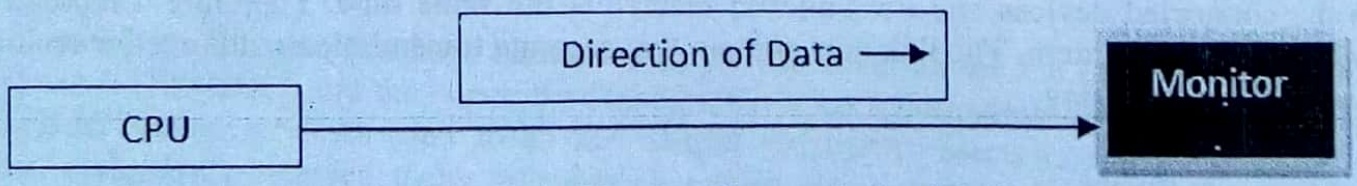


Figure 8.4: Simplex Transmission Mode

Examples of Simplex mode:

- Communication between a computer and a keyboard involves simplex duplex transmission. A television broadcast is an example of simplex duplex transmission.
- Another example of simplex transmission is loudspeaker system. An announcer speaks into a microphone and his/her voice is sent through an amplifier and then to all the speakers. .
- Many fire alarm systems work the same way.

Half Duplex

In half duplex system we can send data in both directions but it is done one at a time that is both the connected devices can transmit and receive but not simultaneously. When one device is sending the other can only receive and vice-versa. The data is sent in one direction.
This is generally used for relatively low-speed transmission

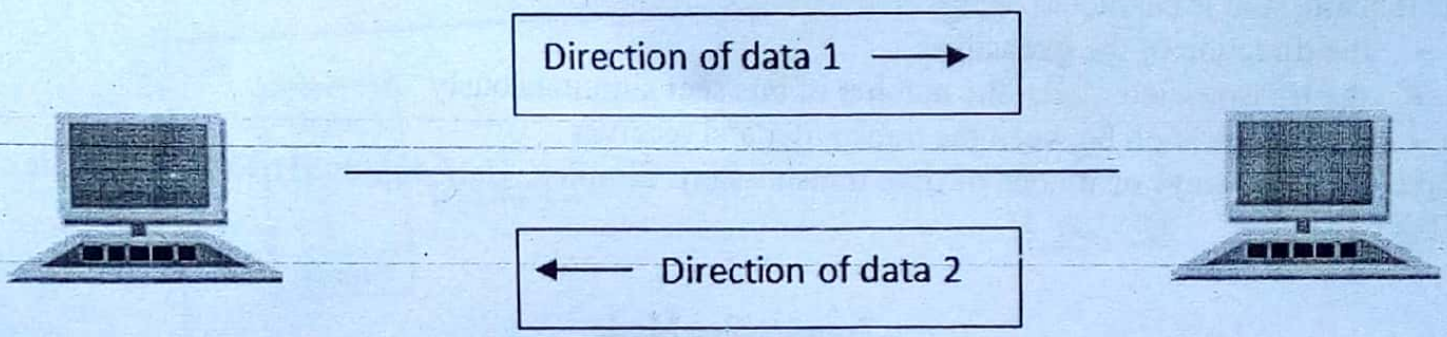


Figure 8.5: Half Duplex Transmission Mode

Example of half duplex mode:

- A walkie-talkie operates in half duplex mode. It can only send or receive a transmission at any given time. It cannot do both at the same time.
- As shown in fig. computer A sends information to computer B. At the end of transmission, computer B sends information to computer A. Computer A cannot send any information to computer B, while computer B is transmitting data.

Full Duplex

A full duplex system can transmit data simultaneously in both directions on transmission path. Full-duplex method is used to transmit the data over a serial communication link. Two wires needed to send data over a serial communication link layer. Full-duplex transmission, the channel capacity is shared by both communicating devices at all times.

Both the connected devices can transmit and receive at the same time. Therefore it represents truly bi-directional system. The link may contain two separate transmission paths one for sending and another for receiving.

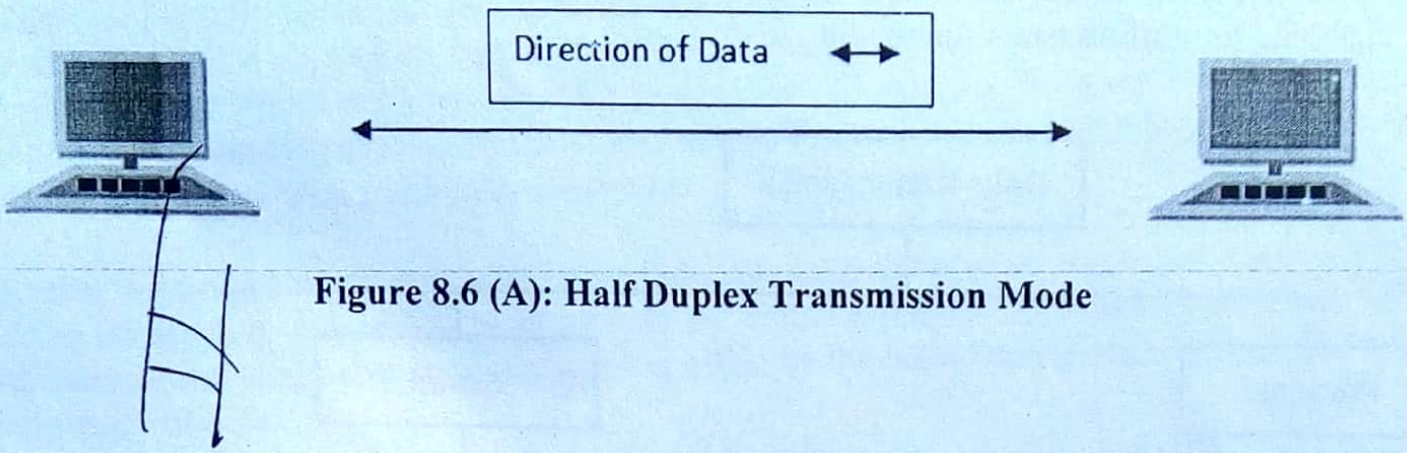


Figure 8.6 (A): Half Duplex Transmission Mode

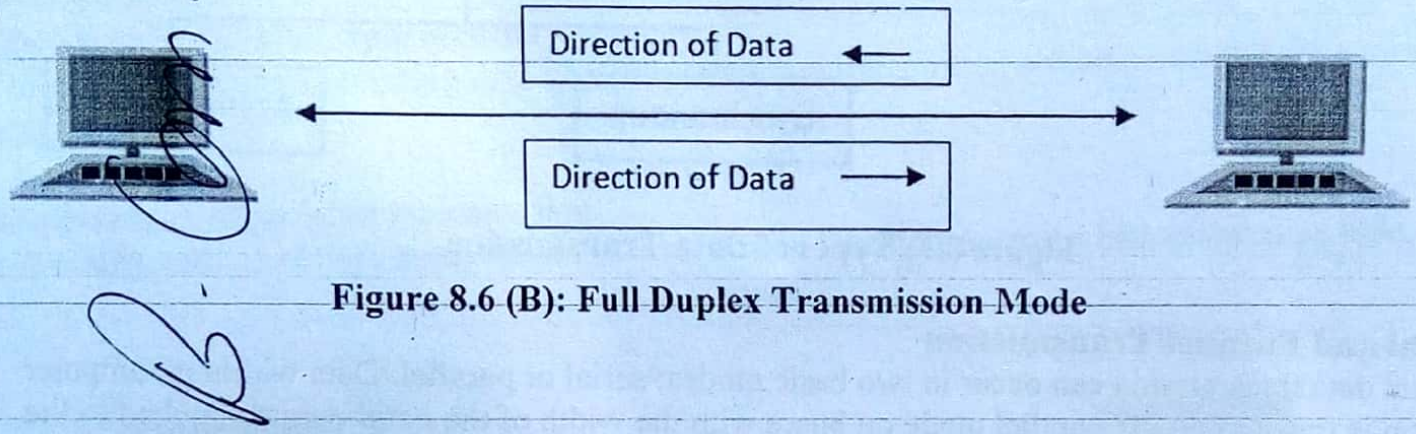


Figure 8.6 (B): Full Duplex Transmission Mode

Example of Full duplex mode:
Telephone networks operate in full duplex mode when two persons talk on telephone line, both can listen and speak simultaneously.

Data Transmission

Data transmission, digital transmission, or digital communications is the physical transfer of data (a digital bit stream or a digitized analog signal) over a point-to-point or point-to-multipoint communication channel. Examples of such channels are copper wires, optical fibers, wireless communication channels, storage media and computer buses. The data are represented as an electromagnetic signal, such as an electrical voltage, radio wave, microwave, or infrared signal.

When we enter data into the computer via keyboard, each keyed element is encoded by the electronics within the keyboard into an equivalent binary coded pattern, using one of the standard coding schemes that are used for the interchange of information. To represent all characters of the keyboard, a unique pattern of 7 or 8 bits in size is used. The use of 7 bits means that 128 different elements can be represented, while 8 bits can represent 256 elements. A similar procedure is followed at the receiver that decodes every received binary pattern into the corresponding character.

The most widely used codes that have been adopted for this function are the Extended Binary Coded Decimal (EBCDIC) and the American Standard Code for Information Interchange codes (ASCII). Both coding schemes cater to all the normal alphabetic, numeric, and punctuation characters, collectively referred to as printable characters and a range of additional control characters, known as non-printable characters.

Data transmission refers to the movement of data in form of bits between two or more digital devices via some form of transmission media

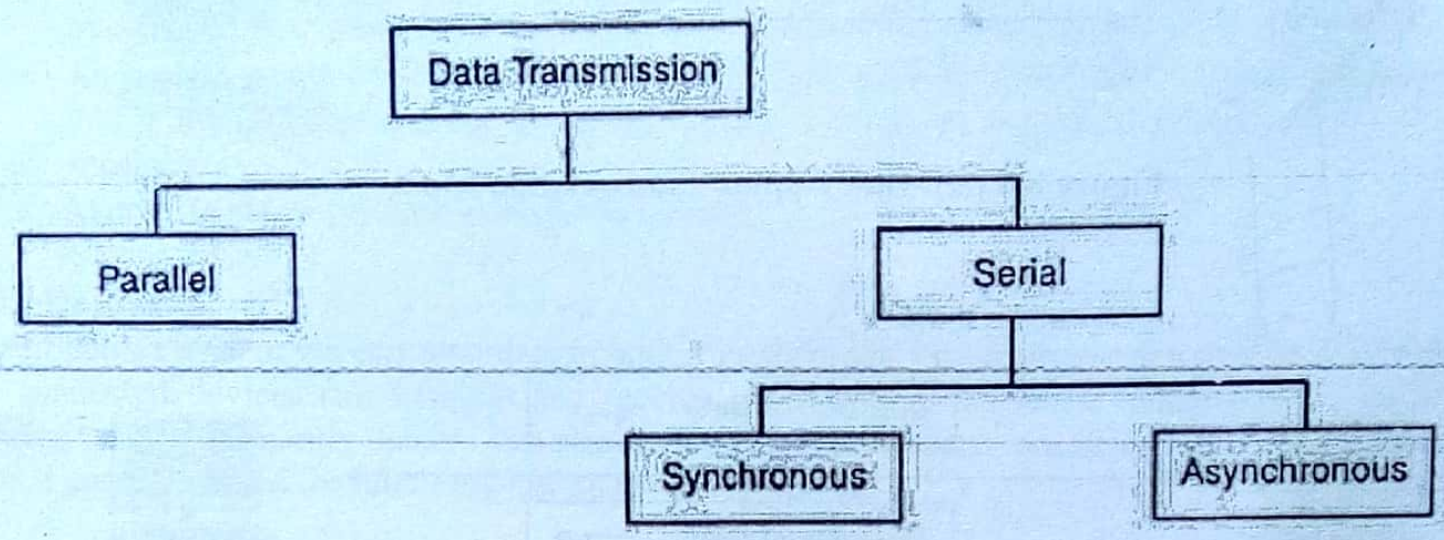


Figure 8.7: Types of Data Transmission

Serial and Parallel Transmission

Digital data transmission can occur in two basic modes: serial or parallel. Data within a computer system is transmitted via parallel mode on buses with the width of the parallel bus matched to the word size of the computer system. Data between computer systems is usually transmitted in bit serial mode. Consequently, it is necessary to make a parallel-to-serial conversion at a computer interface when sending data from a computer system into a network and a serial-to-parallel conversion at a computer interface when receiving information from a network. The type of transmission mode used may also depend upon distance and required data rate.

Parallel Transmission

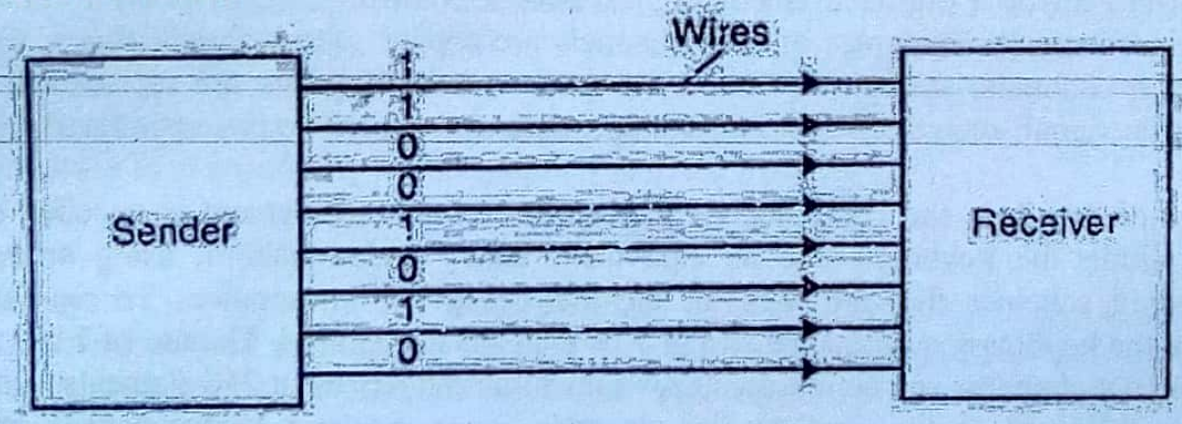


Figure 8.8: Parallel Transmission

In parallel transmission, all the bits of data are transmitted simultaneously on separate communication lines i.e. multiple **bits** (usually 8 bits or a byte/character) are sent simultaneously on different channels (wires, frequency channels) within the same cable, or radio path, and **synchronized** to a clock. Parallel transmission is used for short distance communication. Parallel devices have a wider data bus than serial devices and can therefore transfer data in words of one

or more bytes at a time. As a result, there is a speedup in parallel transmission bit rate over serial transmission bit rate. However, this speedup is a tradeoff versus cost since multiple wires cost more than a single wire, and as a parallel cable gets longer, the synchronization timing between multiple channels becomes more sensitive to distance. The timing for parallel transmission is provided by a constant clocking signal sent over a separate wire within the parallel cable; thus parallel transmission is considered **synchronous**.

Examples of parallel mode transmission include connections between a computer and a printer (parallel printer port and cable). Most printers are within 6 meters or 20 feet of the transmitting computer and the slight cost for extra wires is offset by the added speed gained through parallel transmission of data.

Advantage of parallel transmission
It is speedy way of transmitting data as multiple bits are transmitted simultaneously with a single clock pulse.

Disadvantage of parallel transmission
It is costly method of data transmission as it requires *n* lines to transmit *n* bits at the same time.

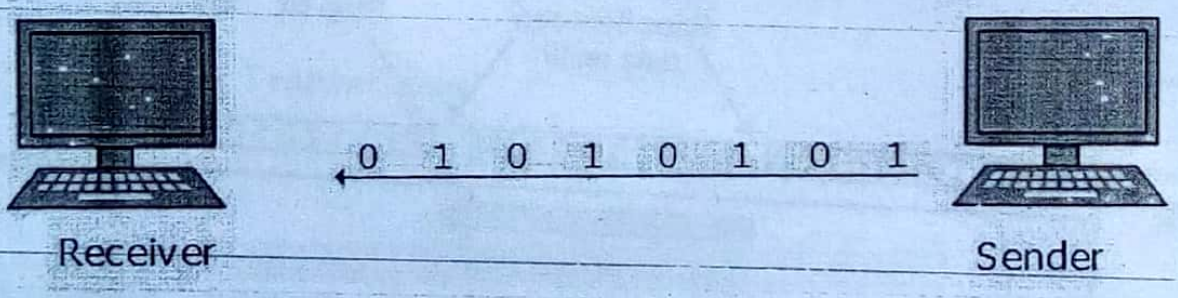


Figure 8.9: Serial Transmission

In serial transmission, the various bits of data are transmitted serially one after the other i.e. bits are sent sequentially on the same channel (wire) which reduces costs for wire but also slows the speed of transmission. It requires only one communication line rather than n lines to transmit data from sender to receiver. Also, for serial transmission, some overhead time is needed since bits must be assembled and sent as a unit and then disassembled at the receiver. Serial transmission is used for long distance communication.

Examples of serial mode transmission include connections between a computer and a modem using the RS-232 protocol. Although an RS-232 cable can theoretically accommodate 25 wires, all but two of these wires are for overhead control signaling and not data transmission; the two data wires perform simple serial transmission in either direction. In this case, a computer may not be close to a modem, making the cost of parallel transmission prohibitive—thus speed of transmission may be considered less important than the economical advantage of serial transmission.

Advantage of Serial transmission

Use of single communication line reduces the transmission line cost by the factor of n as compared to parallel transmission.

Disadvantages of Serial transmission

1. Use of conversion devices at source and destination end may lead to increase in overall transmission cost.
2. This method is slower as compared to parallel transmission as bits are transmitted serially one after the other.

Types of Serial Transmission

There are two types of serial transmission-synchronous and asynchronous both these transmissions use 'Bit synchronization'. Bit Synchronization is a function that is required to determine when the beginning and end of the data transmission occurs.

Bit synchronization helps the receiving computer to know when data begin and end during a transmission. Therefore bit synchronization provides timing control.

(A) Asynchronous Transmission

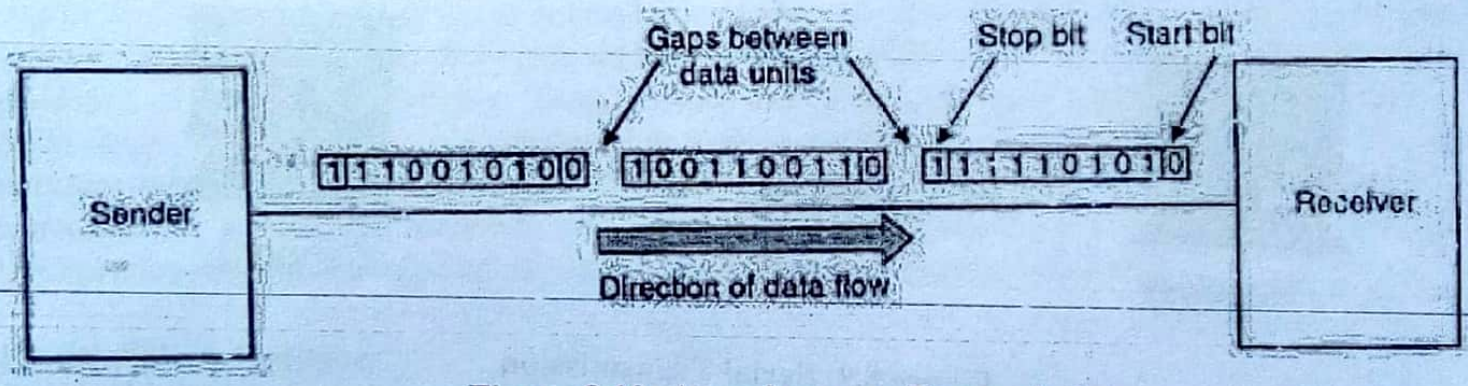


Figure 8.10: Asynchronous Transmission

synchronous transmission sends only one character at a time where a character is either a letter of the alphabet or number or control character *i.e.* it sends one byte of data at a time. In asynchronous transmission, groups of bits are sent as independent units with start/stop flags and no data link synchronization, to allow for arbitrary size gaps between frames. However, start/stop bits maintain physical bit level synchronization once detected. Bit synchronization between two devices is made possible using start bit and stop bit. Start bit indicates the beginning of data *i.e.* alerts the receiver to the arrival of new group of bits. A start bit usually 0 is added to the beginning of each byte. Stop bit indicates the end of data *i.e.* to let the receiver know that byte is finished, one or more additional bits are appended to the end of the byte. These bits, usually 1s are called stop bits. Addition of start and stop increase the number of data bits. Hence more bandwidth is consumed in asynchronous transmission. There is idle time between the transmissions of different data bytes. This idle time is also known as Gap. The gap or idle time can be of varying intervals. This mechanism is called Asynchronous, because at byte level sender and receiver need not to be synchronized. But within each byte, receiver must be synchronized with the incoming bit stream.

There are few Examples of Asynchronous transmission, is well suited for keyboard type-terminals and paper tape devices. The advantage of this method is that it does not require any local storage at the terminal or the computer as transmission takes place character by character. Asynchronous transmission is best suited to Internet traffic in which information is transmitted in short bursts. This type of transmission is used by modems.

Advantages of Asynchronous transmission

1. This method of data transmission is cheaper in cost as compared to synchronous *e.g.* If lines are short, asynchronous transmission is better, because line cost would be low and idle time will not be expensive.
2. In this approach each individual character is complete in itself, therefore if character is corrupted during transmission, its successor and predecessor character will not be affected.
3. It is possible to transmit signals from sources having different bit rates.
4. The transmission can start as soon as data byte to be transmitted becomes available.
5. Moreover, this mode of data transmission in easy to implement.

Disadvantages of Asynchronous transmission

1. This method is less efficient and slower than synchronous transmission due to the overhead of extra bits and insertion of gaps into bit stream.
2. Successful transmission inevitably depends on the recognition of the start bits. These bits can be missed or corrupted.

(B) Synchronous Transmission

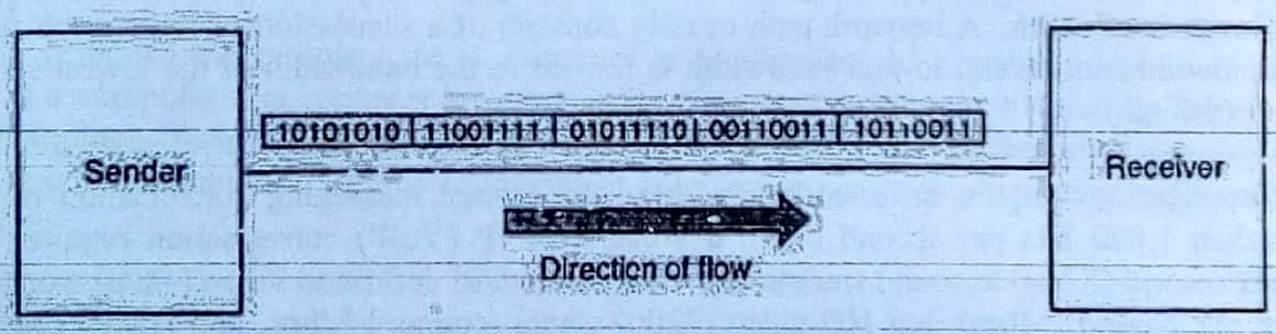


Figure 8.11: Synchronous Transmission

In synchronous transmission, groups of bits are combined into frames and frames are sent continuously with or without data to be transmitted. Synchronous transmission does not use start and stop bits. In this method bit stream is combined into longer frames that may contain multiple bytes. There is no gap between the various bytes in the data stream. In the absence of start & stop bits, bit synchronization is established between sender & receiver by 'timing' the transmission of each bit. Since the various bytes are placed on the link without any gap, it is the responsibility of receiver to separate the bit stream into bytes so as to reconstruct the original information. In order to receive the data error free, the receiver and sender operates at the same clock frequency. Synchronous transmission is used for high speed communication between computers.

Advantage of Synchronous transmission

This method is faster as compared to asynchronous as there are no extra bits (start bit & stop bit) and also there is no gap between the individual data bytes.

Disadvantages of Synchronous transmission

1. It is costly as compared to asynchronous method. It requires local buffer storage at the two ends of line to assemble blocks and it also requires accurately synchronized clocks at both ends. This lead to increase in the cost.
2. The sender and receiver have to operate at the same clock frequency. This requires proper synchronization which makes the system complicated.

Bandwidth

There are two frequently used definitions of bandwidth in the context of Information Technology-

(1) In computer networks, bandwidth is used as a synonym for data transfer rate, the amount of data that can be carried from one point to another in a given time period (usually a second). Network bandwidth is usually expressed in bits per second (bps); modern networks typically have speeds measured in the millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps).

Note that bandwidth is not the only factor that affects network performance: There is also packet loss, latency and jitter, all of which degrade network throughput and make a link perform like one with lower bandwidth. A network path usually consists of a succession of links, each with its own bandwidth, so the end-to-end bandwidth is limited to the bandwidth of the lowest speed link (the bottleneck).

Different applications require different bandwidths. An instant messaging conversation might take less than 1,000 bits per second (bps); a voice over IP (VoIP) conversation requires 56 kilobits per second (Kbps) to sound smooth and clear. Standard definition video (480p) works at 1 megabit per second (Mbps), but HD video (720p) wants around 4 Mbps, and HDX (1080p), more than 7 Mbps.

(2) Bandwidth is the range of frequencies or wavelengths -- the difference between the highest-frequency signal component and the lowest-frequency signal component -- an electronic signal uses on a given transmission medium. Like the frequency of a signal, bandwidth is measured in hertz (cycles per second). This is the original meaning of bandwidth, although it is now used primarily in discussions about cellular networks and the spectrum of frequencies that operator's license from various governments for use in mobile services.

Computer Network

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. The most common resource shared today is connection to

the Internet. Other shared resources can include a printer or a file server. The Internet itself can be considered as a computer network.

Benefits of networking

There are lots of advantages from build up a network, but the three big facts are-

(1) File Sharing

From sharing files you can view, modify, and copy files stored on a different computer on the network just as easily as if they were stored on your computer.

(2) Resource Sharing

Resources such as printers, fax machines, Storage Devices (HDD, FDD and CD Drives), Webcam, Scanners, Modem and many more devices can be shared.

(3) Program Sharing

Just as you can share files on a network, you can often also share program on a network. For example, if you have the right type of software license, you can have a shared copy of Microsoft Office, or some other program, and keep it on the network server, from where it is also run

Computer Network Terminology

Server

A computer or device on a network that manages network resources. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems, however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

Client

Usually refers to the recipient, be it computer or application, of a server's hosted service. A client is a computer that retrieves information from or uses resources provided by the server or main computer. Each of these computers connects to a central server, which allows processing to be done on the client side instead of the server side and reduces the processing requirements of the server.

Workgroup

A workgroup is a collection of computers on a local area network (LAN) that share common resources and responsibilities. Workgroups provide easy sharing of files, printers and other network resources. All computers are peers; no computer has control over another computer. Each computer has a set of user accounts. To use any computer in the workgroup, you must have an account on that computer. There are typically no more than ten to twenty computers. All computers must be on the same local network or subnet.

Domain

A domain is a group of network resources assigned to a group of users. Domains divide global areas of a corporation or a corporation's departments. A domain may need to be specified when mapping a network computer or drive. One or more computers are servers. Network administrators use servers to control the security and permissions for all computers on the domain. This makes it easy to make changes because the changes are automatically made to all computers. If you have a user account on the domain, you can log on to any computer on the

domain without needing an account on that computer. There can be hundreds or thousands of computers.

Login

To make a computer system or network recognizes you so that you can begin a computer session. In computer security, a login or logon refers to the credentials required to obtain access to a computer system or other restricted area. Logging in or on and signing in or on is the process by which individual access to a computer system is controlled by identifying and authenticating the user through the credentials presented by the user. Once a user has logged in, they can then log out or log off when access is no longer needed. To log out is to close off one's access to a computer system after having previously logged in.

Categories of Network

Network can be divided in to two main categories:

- Server – based (also called a client/server network)
- Peer-to-peer (also called a workgroup)

Server-based Network

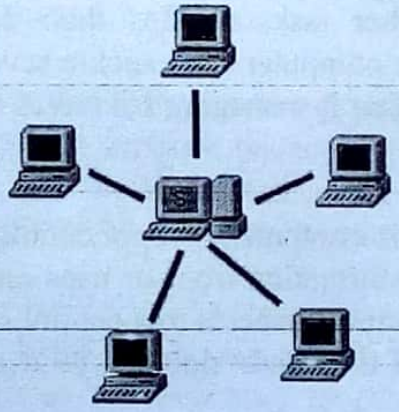


Figure 8.12: Server-based Network

In a server-based network, the server is the central location where users share and access network resources. This dedicated computer controls the level of access that users have to shared resources. Shared data is in one location, making it easy to back up critical business information. Each computer that connects to the network is called a client computer. In a server-based network, users have one user account and password to log on to the server and to access shared resources. Server operating systems are designed to handle the load when multiple client computers access server-based resources.

Windows SBS 2008 is installed and configured as the central server on a server-based network. Windows SBS 2008 provides the central point for authenticating users, accessing resources, and storing information.

Peer-to-peer Network

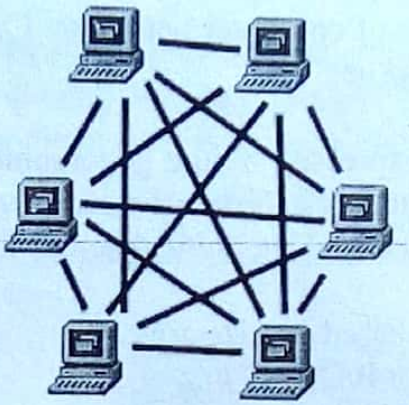


Figure 8.13: Peer-to-peer Network

In this network, a group of computers is connected together so that users can share resources and information. There is no central location for authenticating users, storing files, or accessing resources. A peer-to-peer network in which every computer acts as both a client and server This means that users must remember which computers in the workgroup have the shared resource or information that they want to access. It also means that users must log on to each computer to access the shared resources on that computer.

In most peer-to-peer networks, it is difficult for users to track where information is located because data is generally stored on multiple computers. This makes it difficult to back up critical business information, and it often results in small businesses not completing backups. Often, there are multiple versions of the same file on different computers in the workgroup.

In some peer-to-peer networks, the small business uses one computer that is running a client operating system, such as Microsoft Windows 98 or Windows XP Professional, as the designated "server" for the network. Although this helps with saving data in a central location, it does not provide a robust solution for many of the needs of a small business, such as collaborating on documents.

Point-to-point Network

There is another type of connection Point-to-point networks contains exactly two hosts (computer or switches or routers or servers) connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other end and vice-versa.

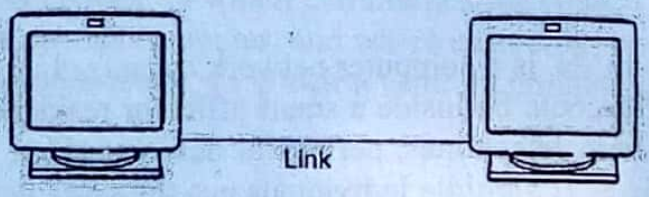


Figure 8.14: Point-to-point Network

If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

Types of Networks

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose.

The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.

Some of the different networks based on size are:

- Personal area network, or PAN
- Local area network, or LAN
- Metropolitan area network, or MAN
- Wide area network, or WAN

In terms of purpose, many networks can be considered general purpose, which means they are used for everything from sending files to a printer to accessing the Internet. Some types of networks, however, serve a very particular purpose. Some of the different networks based on their main purpose are:

- Storage area network, or SAN
- Enterprise private network, or EPN
- Virtual private network, or VPN

Personal Area Network (PAN)

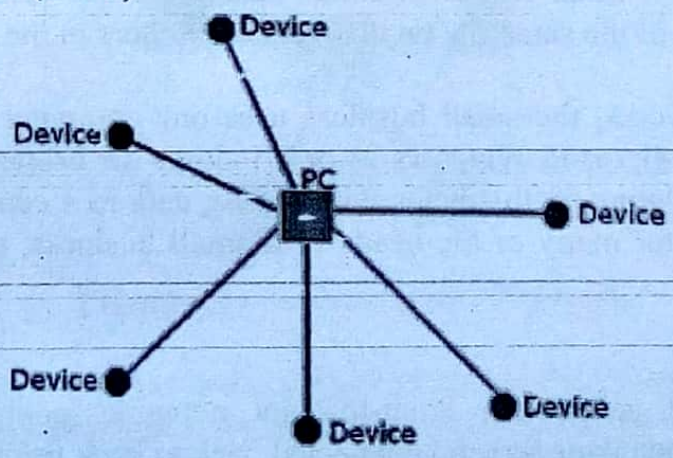


Figure 8.15: Personal Area Network (PAN)

A personal area network, or PAN, is a computer network organized around an individual person within a single building. This could be inside a small office or residence. A typical PAN would include one or more computers, telephones, peripheral devices, video game consoles and other personal entertainment devices. If multiple individuals use the same network within a residence, the network is sometimes referred to as a home area network, or HAN. In a very typical setup, a residence will have a single wired Internet connection connected to a modem. This modem then provides both wired and wireless connections for multiple devices. The network is typically managed from a single computer but can be accessed from any device. This type of network provides great flexibility. For example, it allows you to:

- Send a document to the printer in the office upstairs while you are sitting on the couch with your laptop.
- Upload the photo from your cell phone to your desktop computer.
- Watch movies from an online streaming service to your TV.

If this sounds familiar to you, you likely have a PAN in your house without having called it by its name.

Local Area Network (LAN)

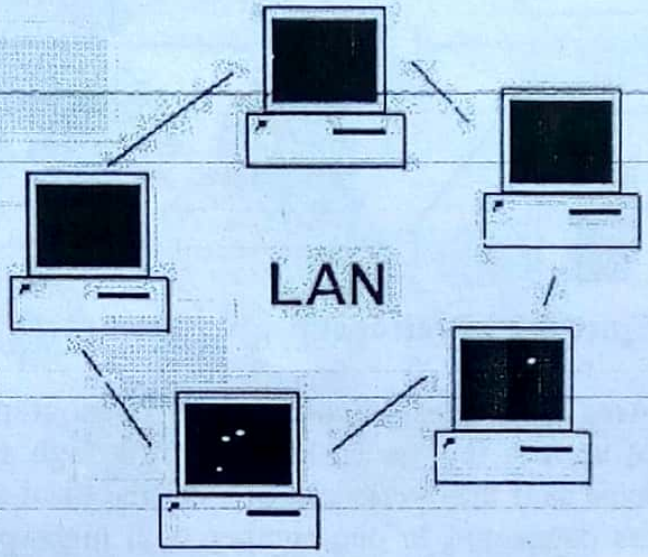


Figure 8.16: Local Area Network (LAN)

LAN stands for Local Area Network. It's a group of computers which all belong to the same organization, and which are linked within a small geographic area using a network, and often the same technology (the most widespread being Ethernet).

A local area network is a network in its simplest form. Data transfer speeds over a local area network can reach up to 10 Mbps (such as for an Ethernet network) and 1 Gbps (as with FDDI or Gigabit Ethernet). A local area network can reach as many as 100, or even 1000, users.

By expanding the definition of a LAN to the services that it provides, two different operating modes can be defined:

- In a **"peer-to-peer"** network, in which communication is carried out from one computer to another, without a central computer, and where each computer has the same role.
- In a "client/server" environment, in which a central computer provides network services to users.

Metropolitan Area Networks (MANs)

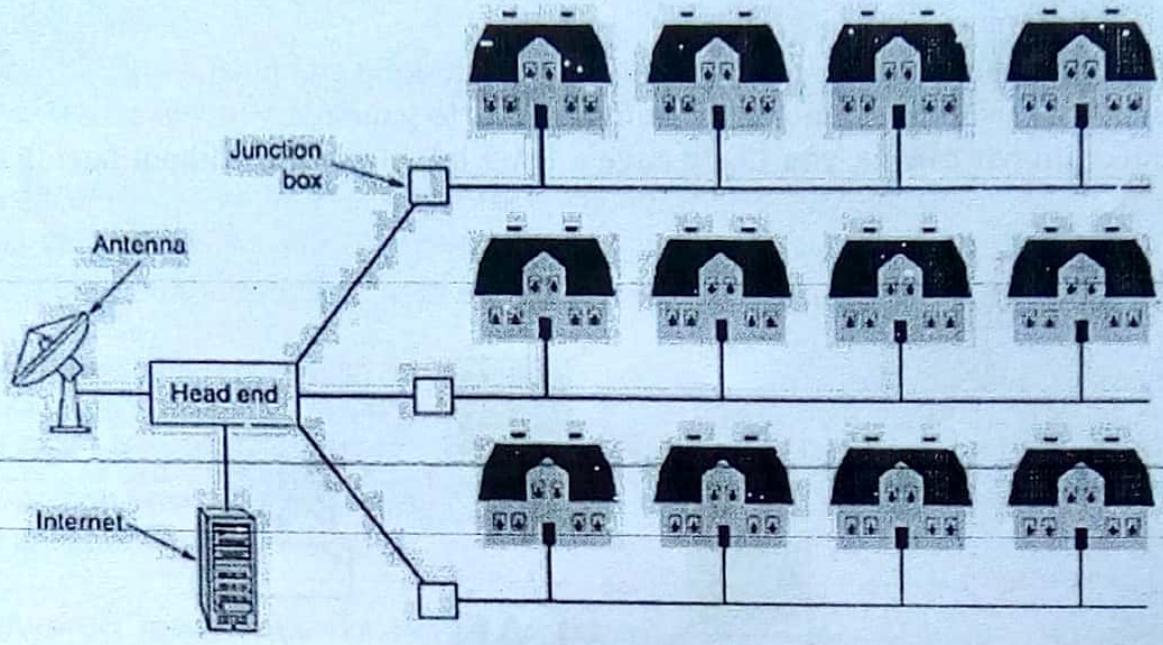


Figure 8.17: Metropolitan Area Networks (MANs)

MANs (Metropolitan Area Networks) connect multiple geographically nearby LANs to one another (over an area of up to a few dozen kilometers) at high speeds. Thus, a MAN lets two remote nodes communicate as if they were part of the same local area network. A MAN is made from switches or routers connected to one another with high-speed links (usually fiber optic cables).

MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for inter-networking of local networks. Its geographic scope falls between a WAN and LAN. MANs provide Internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the Internet.

Wireless Local Area Networks (WLAN)

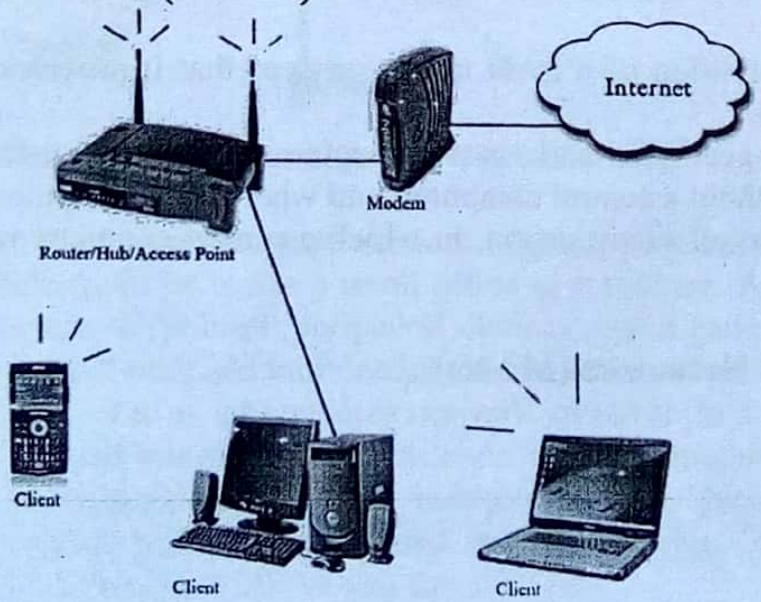


Figure 8.18: Wireless Local Area Networks (WLAN)

Wireless Local Area Networks are much like LAN networks, except they do not require network cables to connect each other. Radio and infrared signals are used to communicate between machines whilst using a wireless local area network. Wireless Local Area Networks allow for small amounts of mobility whilst being connected to the internet. Wireless Local Area Networks work according to the IEEE 802.11 standards. Wireless Area Networks are commonly seen being used by a WiFi internet connection. Wireless LAN connections offer a surprising amount of mobility for users with laptops and smart phones while being able to stay connected to the

Wide Area Network (WANs)

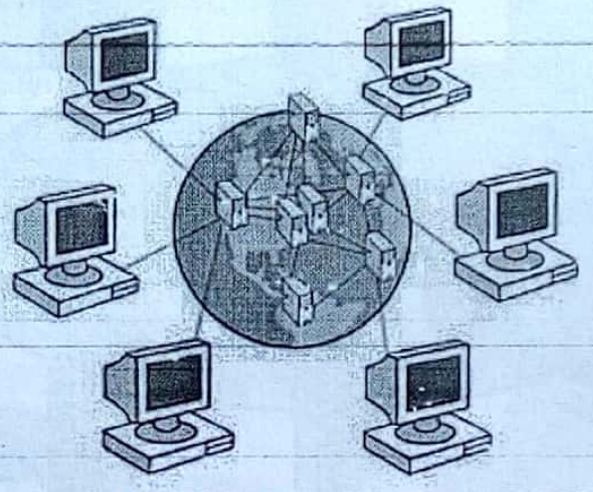


Figure 8.19: Wide Area Network (WANs)

A WAN (Wide Area Network or extended network) connects multiple LANs to one another over great geographic distances. The speed available on a WAN varies depending on the cost of the connections (which increases with distance) and may be low. WANs operate using routers, which can "choose" the most appropriate path for data to take to reach a network node. The most well-known WAN is the Internet.

Campus Area Networks (CAN)

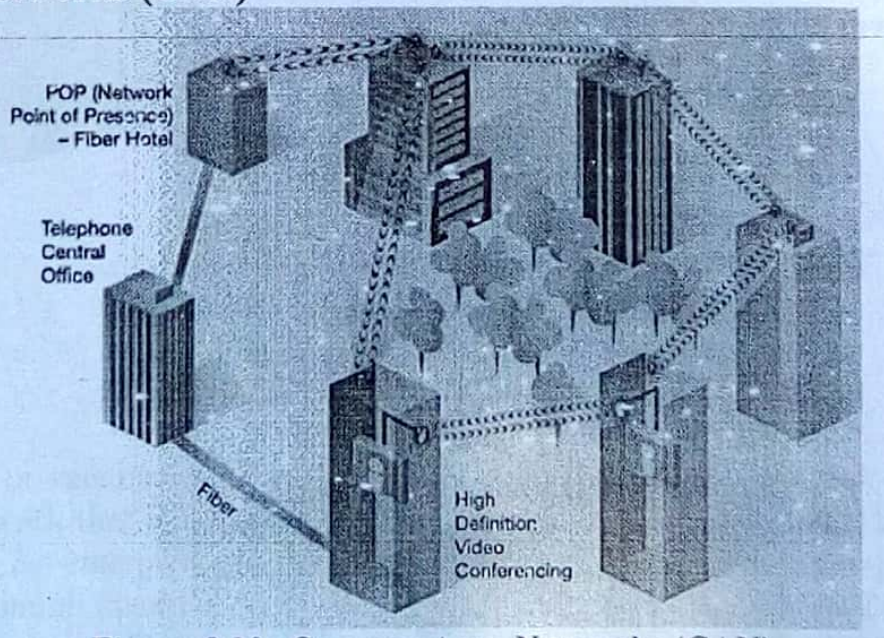


Figure 8.20: Campus Area Networks (CAN)

Campus Area Networks are usually a connection of many small LAN networks which are often used on university campuses and office buildings. Campus Area Networks allow for easy file sharing between different departments as all the files are usually shared on the server machines of each LAN network. This type of network offers a lot of simplicity in the transfer and downloading of files.

Storage Area Network (SAN)

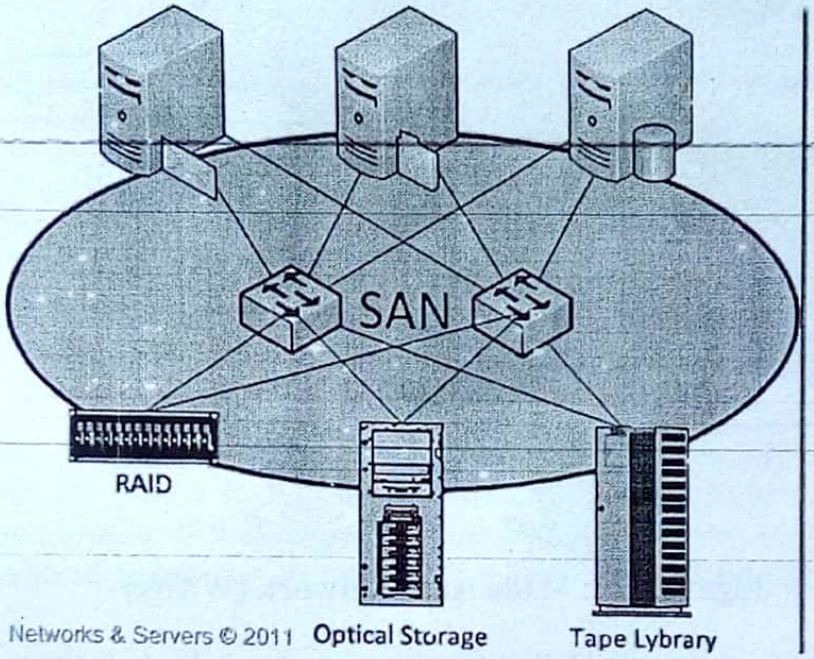


Figure 8.21: Storage Area Networks (SAN)

Storage Area Networks are primarily used as information databases. They are not usually used by large organizations or similar entities. They are specifically used for the storage of information, and easy retrieval of specific pieces of data whenever required. Storage Area Networks are usually used by websites which offer downloading services.

System Area Network (SAN)

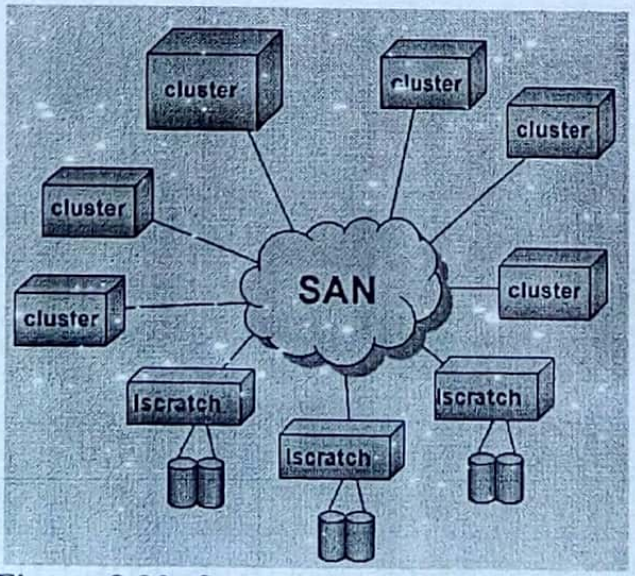


Figure 8.22: System Area Network (SAN)

System Area Networks are speed oriented networks which provide high speed internet connections to a cluster of computers. These are primarily used for server purposes, and allow other computers to connect to these System Area Networks. Permission to different access points are given according to what status a system is on the System Area Network, such as administrators or simple users.

Private Networks

One of the benefits of networks like PAN and LAN is that they can be kept entirely private by restricting some communications to the connections within the network. This means that those communications never go over the Internet.

For example, using a LAN, an employee is able to establish a fast and secure connection to a company database without encryption since none of the communications between the employee's computer and the database on the server leave the LAN. But what happens if the same employee wants to use the database from a remote location? What you need is a private network.

(I) Enterprise Private Network (EPN)

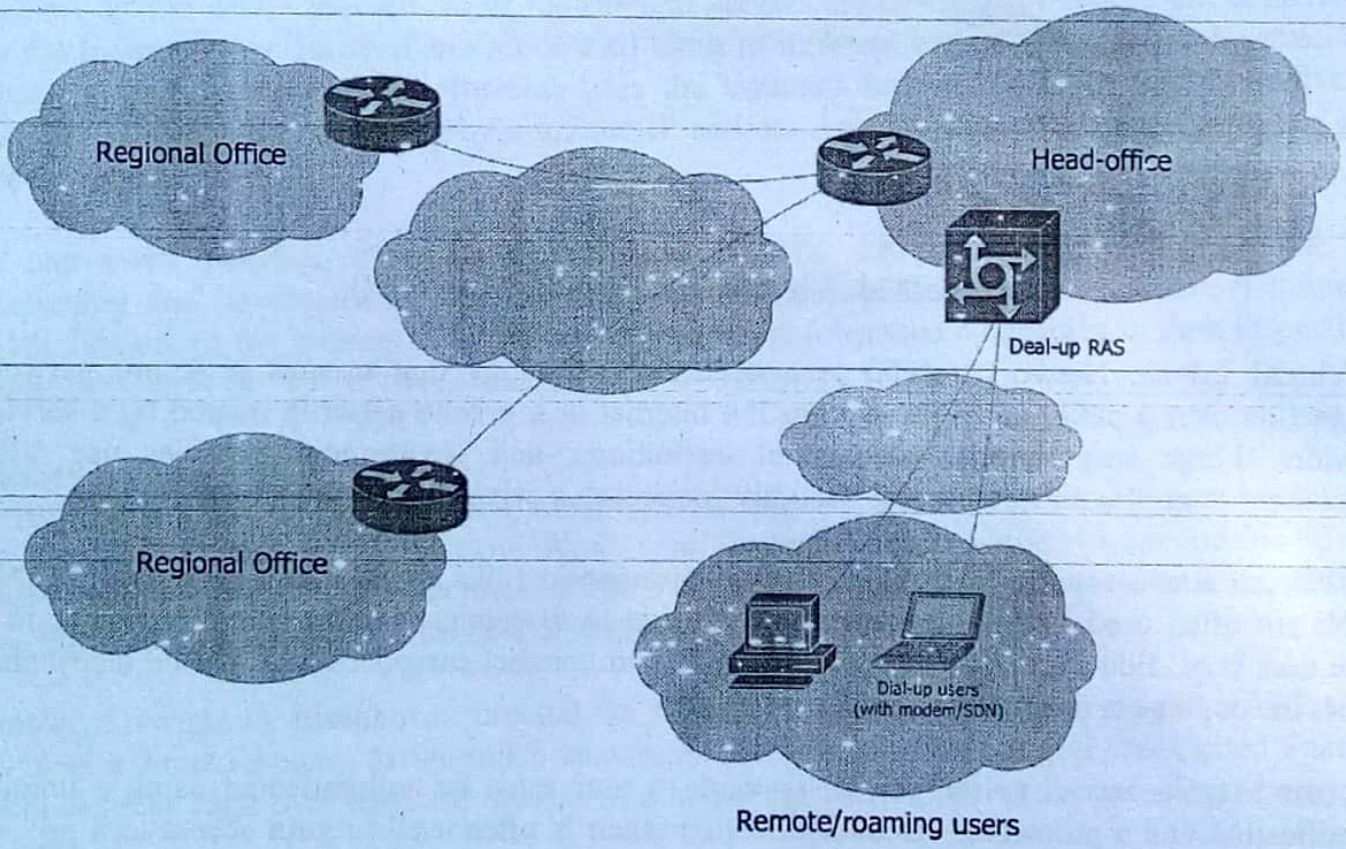


Figure 8.23: Virtual Private Network (VPN)

One approach to a private network is to build an **Enterprise Private Network**, or **EPN**. An EPN is a computer network that is entirely controlled by one organization, and it is used to connect multiple locations. An enterprise private network is mainly set up to share computer resources. Historically, telecommunications companies, like AT&T, operated their own network, separate from the public Internet. EPNs are still fairly common in certain sectors where security is of the

highest concern. For example, a number of health facilities may establish their own network between multiple sites to have full control over the confidentiality of patient records.

(II) Virtual Private Network (VPN)

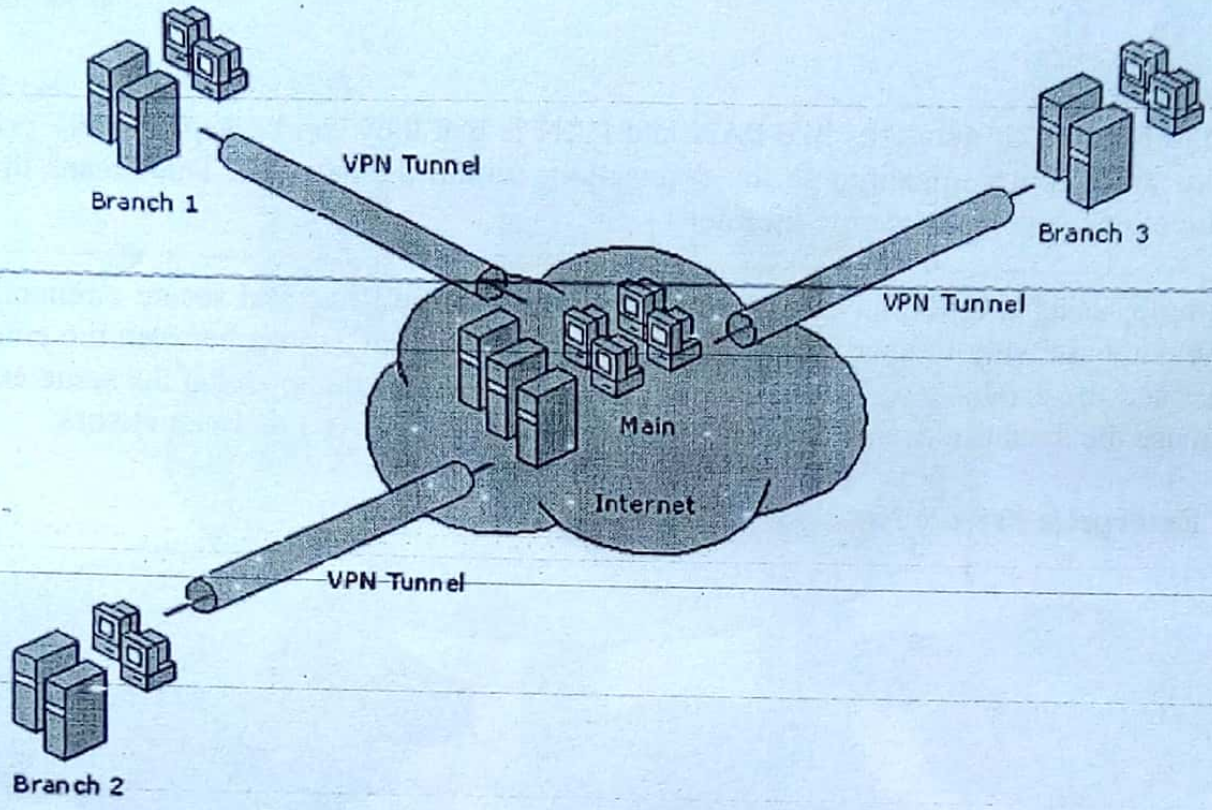


Figure 8.24: Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Large corporations, educational institutions, and government agencies use VPN technology to enable remote users to securely connect to a private network.

A VPN can connect multiple sites over a large distance just like a Wide Area Network (WAN). VPNs are often used to extend intranets worldwide to disseminate information and news to a wide user base. Educational institutions use VPNs to connect campuses that can be distributed across the country or around the world.

In order to gain access to the private network, a user must be authenticated using a unique identification and a password. An authentication token is often used to gain access to a private network through a personal identification number (PIN) that a user must enter. The PIN is a unique authentication code that changes according to a specific frequency, usually every 30 seconds or so.

Internet

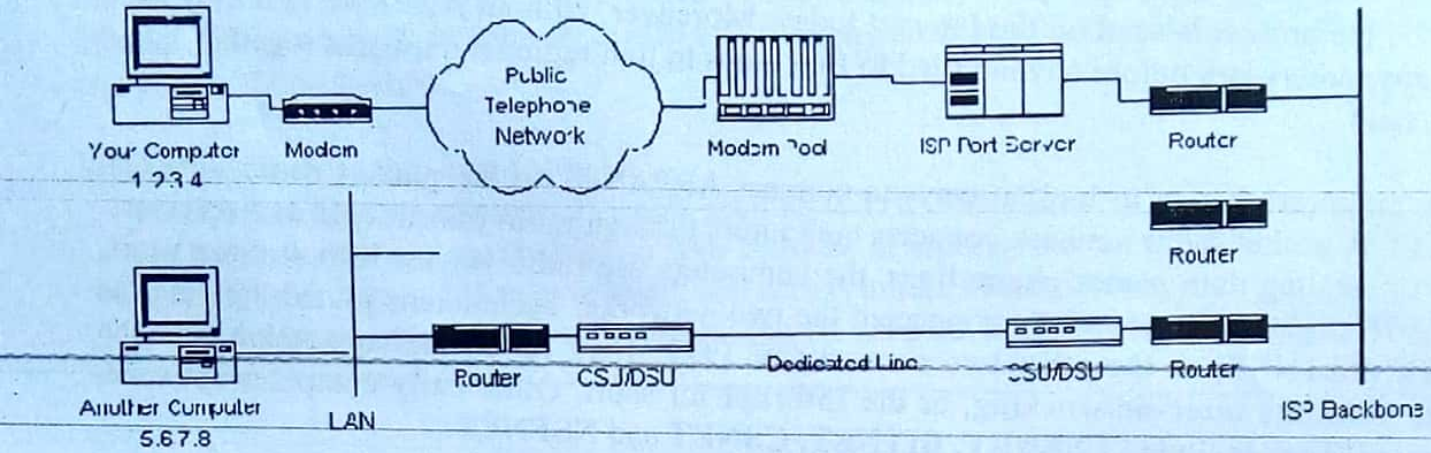


Figure 8.25: Internet

Alternatively referred to as the net or the web, it is a world-wide / global system of interconnected computer networks. A means of connecting a computer to any other computer anywhere in the world via dedicated routers and servers. When two computers are connected over the Internet, they can send and receive all kinds of information such as text, graphics, voice, video, and computer programs. Internet uses the standard Internet Protocol (TCP/IP). Every computer in internet is identified by a unique IP address. Internet is accessible to every user all over the world.

No one owns Internet, although several organizations the world over collaborate in its functioning and development. The high-speed, fiber-optic cables (called backbones) through which the bulk of the Internet data travels are owned by telephone companies in their respective countries.

History of the Internet

In 1957 when the then Soviet Union launched **Sputnik**, the first man-made satellite. Americans were shocked by the news. The Cold War was at its peak, and the United States and the Soviet Union considered each other enemies. If the Soviet Union could launch a satellite into space, it was possible it could launch a missile at North America.

President Dwight D. Eisenhower created the **Advanced Research Projects Agency** (**ARPA**) in 1958 as a direct response to Sputnik's launch. ARPA's purpose was to give the United States a technological edge over other countries. One important part of ARPA's mission was computer science.

In the 1950s, computers were enormous devices that filled entire rooms. They had a fraction of the power and processing ability you can find in a modern PC. Many computers could only read magnetic tape or punch cards, and there was no way to network computers together.

ARPA aimed to change that. It enlisted the help of the company Bolt, Beranek and Newman (BBN) to create a computer network. The network had to connect four computers running on four different operating systems. They called the network ARPANET.

Without ARPANET, the Internet wouldn't look or behave the way it does today - it might not even exist. Although other groups were working on ways to network computers, ARPANET established the protocols used on the Internet today. Moreover, without ARPANET, it may have taken many more years before anyone tried to find ways to join regional networks together into a larger system.

In 1973, engineers began to look at ways to connect ARPANET to the **packet radio network (PRNET)**. A packet radio network connects computers through radio transmitters and receivers. Instead of sending data across phone lines, the computers use radio waves. It took three years, but in 1976 engineers successfully connected the two networks. Technicians joined the Satellite **Network** (SATNET) to the other two networks in 1977. They called the connection between multiple networks **inter-networking**, or the **Internet** for short. Other early computer networks soon joined. They included **USENET, BITNET, CSNET** and **NSFNET**.

In 1990, Tim Berners-Lee developed a system designed to simplify navigation on the Internet. In time, this system became known as the **World Wide Web**. It didn't take long for some people to mistakenly identify the Internet and the Web as the same thing. The Internet is a global interconnection of computer networks; the World Wide Web is a way to navigate this massive network. In sailing terms, it's like comparing an ocean to a ship.

Most early Internet users were government and military employees, graduate students and computer scientists. Using the World Wide Web, the Internet became much more accessible. Colleges and universities began to connect to the Internet, and businesses soon followed. By 1994, Internet commerce had become a reality.

Today, the Internet is more complex than ever. It connects computers, satellites, mobile devices and other gadgets together in a massive network millions of times more intricate than the original ARPANET.

Intranet

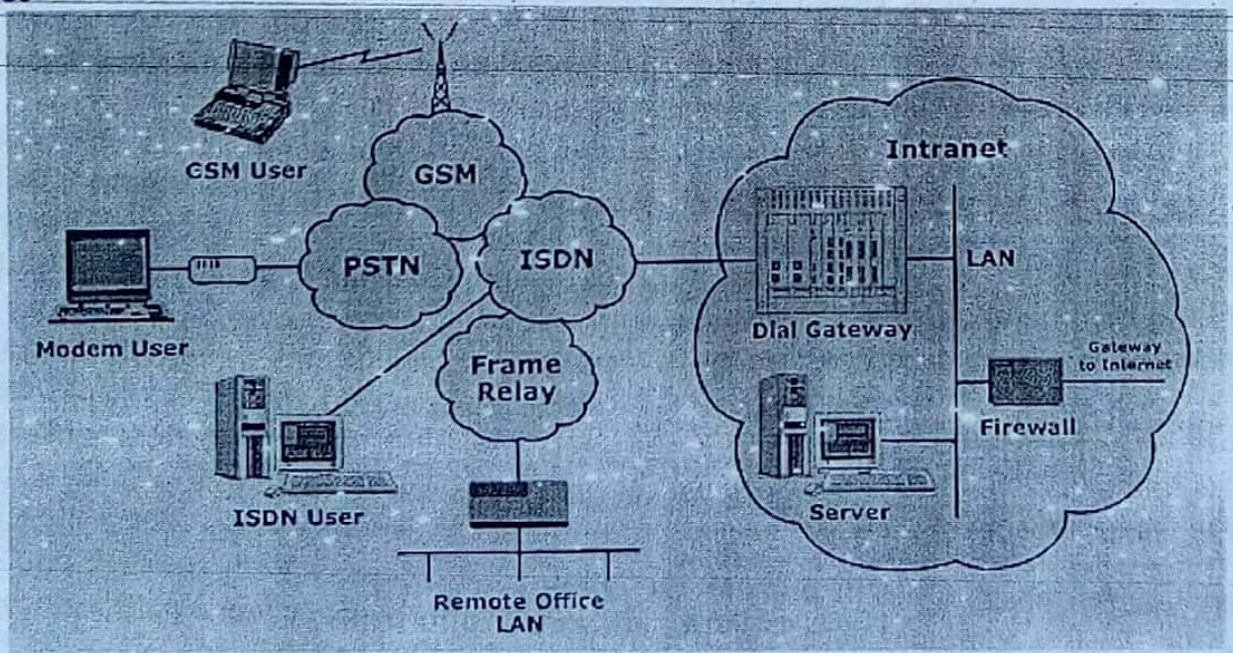


Figure 8.26: Intranet

Intranet is system in which multiple PCs are connected to each other. PCs in intranet are not available to the world outside the intranet. Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet. Each computer in Intranet is also identified by an IP Address which is unique among the computers in that Intranet.

Similarities in Internet and Intranet

- Intranet uses the internet protocols such as TCP/IP and FTP.
- Intranet sites are accessible via web browser in similar way as websites in internet. But only members of Intranet network can access intranet hosted sites.
- In Intranet, own instant messengers can be used as similar to yahoo messenger / gtalk over the internet.

Differences in Internet and Intranet

- Internet is general to PCs all over the world whereas Intranet is specific to few PCs.
- Internet has wider access and provides a better access to websites to large population whereas Intranet is restricted.
- Internet is not as safe as Intranet as Intranet can be safely privatized as per the need.

Extranet

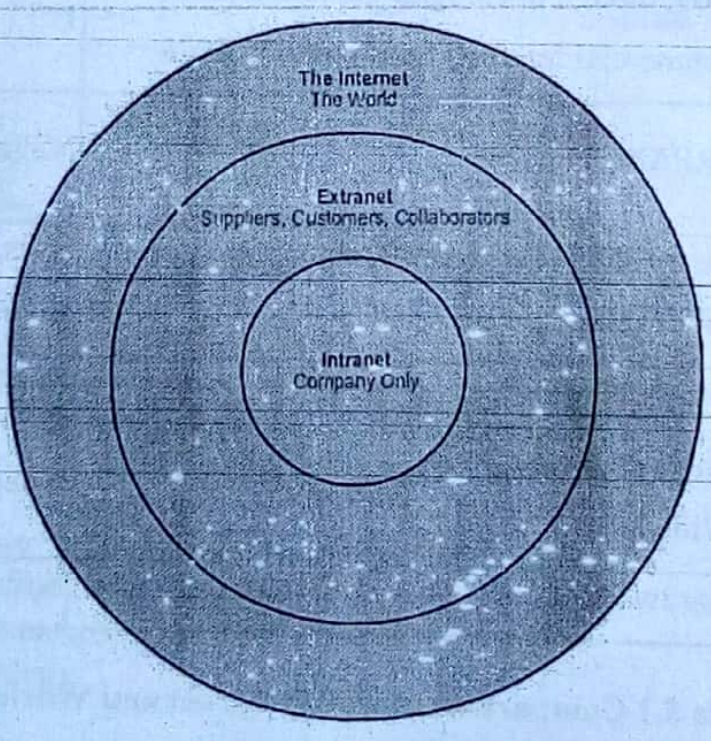


Figure 8.27: Extranet

An extranet is a private network that allows controlled access from the outside for specific business or educational purposes and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.. Extranets are extensions to, or segments of, private intranet networks that have been built in many corporations for information sharing and ecommerce.

WWW (World Wide Web)

The World Wide Web is also abbreviated as **WWW** or **W3**, commonly known as the **Web**. WWW is a system of interlinked hypertext documents that are accessed via the Internet. WWW or Web, is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet. The Web uses the HTTP protocol, only one of the languages spoken over the Internet, to transmit data. Web services, which use HTTP to allow applications to communicate in order to exchange business logic, use the the Web to share information. The Web also utilizes browsers, such as Internet Explorer or Firefox, to access Web documents called Web pages that are linked to each other via hyperlinks. Web documents also contain graphics, sounds, text and video.

The Web is just one of the ways that information can be disseminated over the Internet. The Internet, not the Web, is also used for e-mail, which relies on SMTP, Usenet news groups, instant messaging and FTP. So the Web is just a portion of the Internet, albeit a large portion, but the two terms are not synonymous and should not be confused. Following table show the difference between Internet and WWW-

Features	Internet	World Wide Web
Estimated year of Origin	1969, though opening of the network to commercial interests began only in 1988	1993
Name of the first version	ARPANET	NSFnet
Comprises	Network of Computers, copper wires, fibre-optic cables & wireless networks	Files, folders & documents stored in various computers
Governed by	Internet Protocol	Hyper Text Transfer Protocol
Dependency	This is the base, independent of the World Wide Web	It depends on Internet to work
Nature	Hardware	Software

Table 8.1 Comparison chart of Internet and World Wide Web

History of World Wide Web (WWW)

Dwight D. Eisenhower started the **Advanced Research Projects Agency** (ARPA) in 1958 to increase U.S. technological advancements in the shadow of Sputnik's launch. By October 29, 1969, the first **ARPANET** network connection between two computers was launched -- and promptly crashed. But happily, the second time around was much more successful and the Internet was born. More and more computers were added to this ever-increasing network and the megalith we know today as the Internet began to form. Further information about ARPA can be discovered by reading How ARPANET Works.

But the creation of the World Wide Web didn't come until decades later, with the help of a man named Tim Berners-Lee. In 1990, he developed the backbone of the World Wide Web -- the **hypertext transfer protocol (HTTP)**. People quickly developed **browsers** which supported the use of HTTP and with that the popularity of computers skyrocketed. In the 20 years during which ARPANET ruled the Internet, the worldwide network grew from four computers to more than 300,000. By 1992, more than a million computers were connected -- only two years after HTTP was developed. HTTP is -- it's simply the widely used set of rules for how files and other information are transferred between computers. So what Berners-Lee did, in essence, was determine how computers would communicate with one another.

Network Topology

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection 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

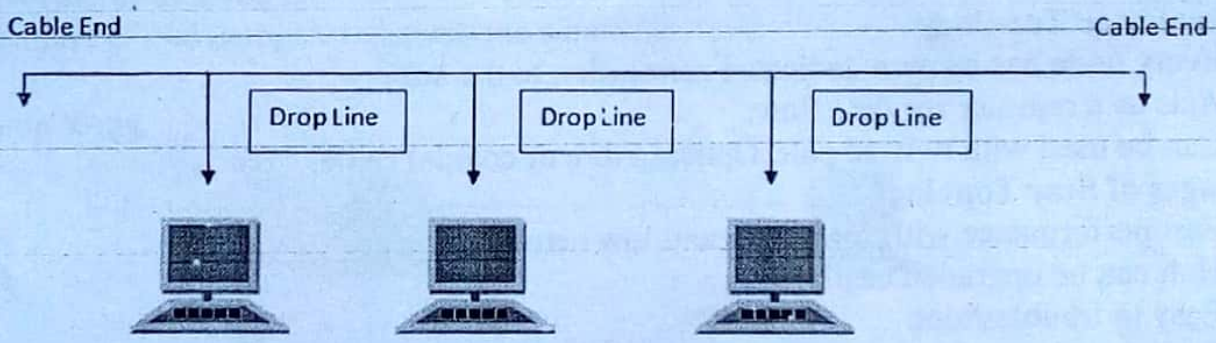


Figure 8.28: Bus Topology

Bus topology is a network type in where every computer and network device is connected to single cable. In contrast to point-to-point, in bus topology all device share single communication line or cable. 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.

Star Topology

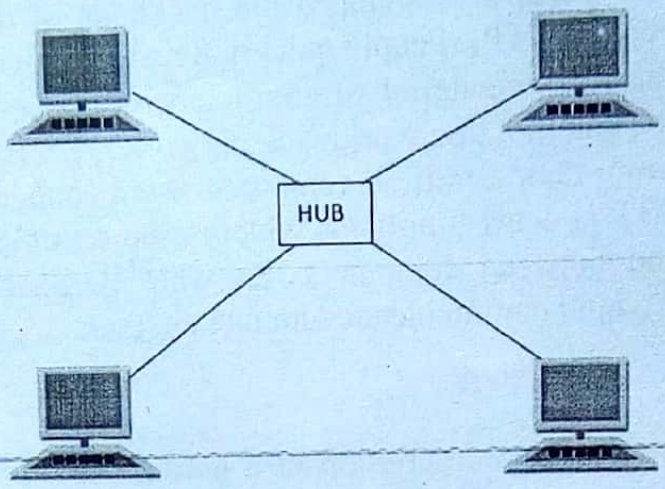


Figure 8.29: Star Topology

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.

Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. 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 is affected 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.

Ring Topology

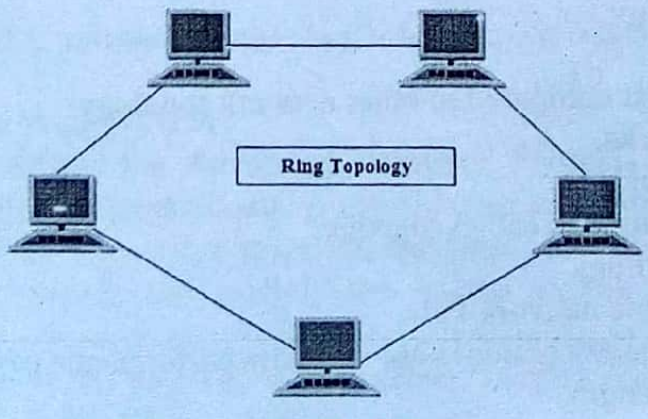


Figure 8.30: Ring Topology

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 neighbors for each device, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure administrator may need only one more extra cable. Failure of any host results in failure of the whole ring. Thus every connection in the ring is point of failure. There exist methods which employs one more backup ring.

Features of Ring Topology

1. A number of repeaters are used and the transmission is unidirectional.
2. Date is transferred in a sequential manner that is bit by bit.

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.
3. Failure of one computer disturbs the whole network.

Mesh Topology

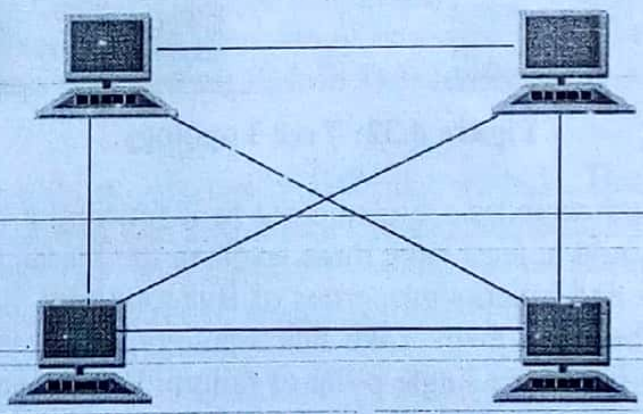


Figure 8.31: Mesh Topology

In this type of topology, a host is connected to one or two or more than two hosts. This topology may have hosts having point-to-point connection to every other host or may also have hosts which are having point to point connection to few hosts only. Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links.

Types of Mesh Topology

- **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 cables (connection) are required. It provides the most reliable network structure among all network topologies.
- **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some host whereas others are not as such necessary.

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

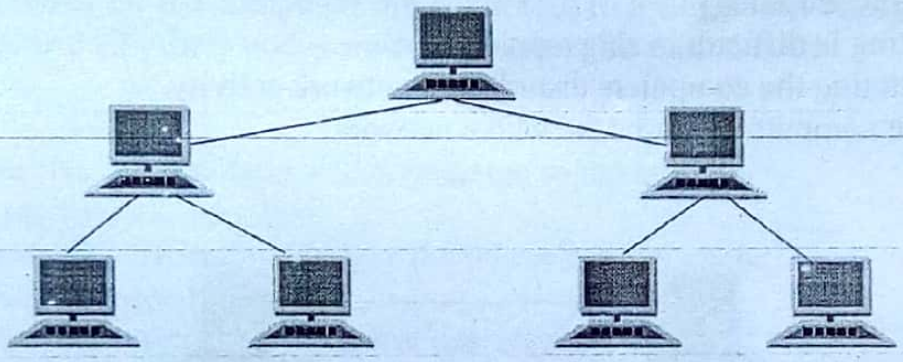


Figure 8.32: Tree Topology

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 imitates as extended Star Topology and inherits properties of Bus topology. All neighboring hosts have point-to-point connection between them. Like bus topology, if the root goes down, the entire network suffers. 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 and so on.

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

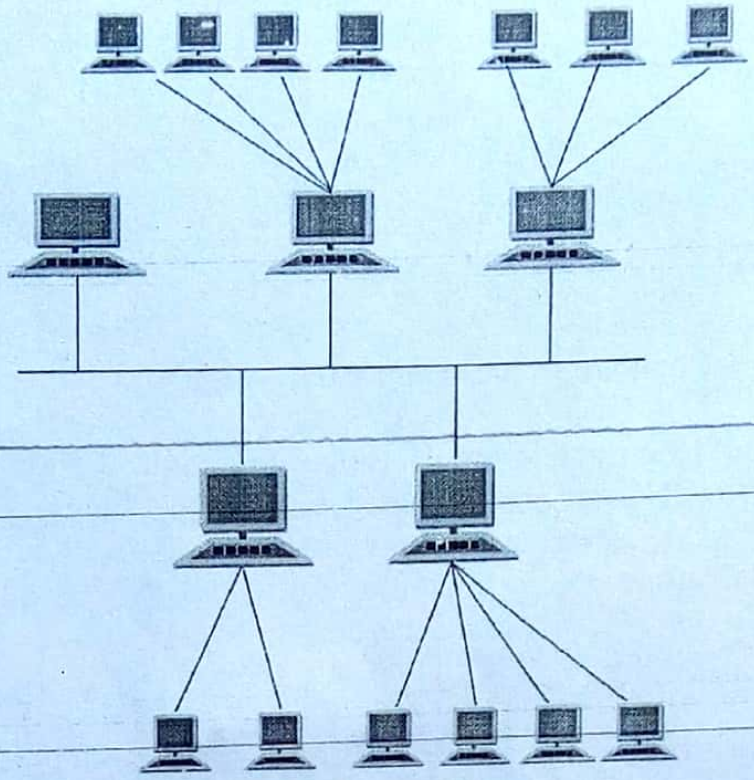


Figure 8.33: Hybrid Topology

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 above picture 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.

Daisy Chain

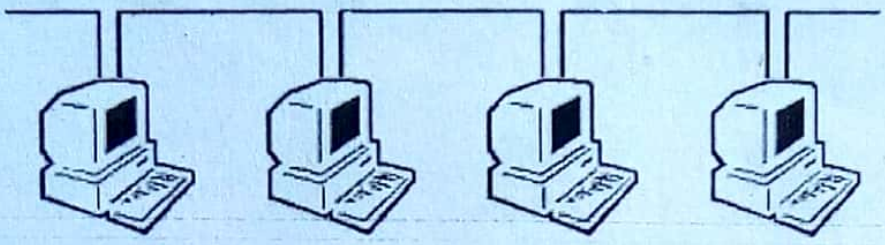


Figure 8.34: Daisy Chain Topology

This topology connects all its hosts in a linear fashion. Similar to Ring topology, all hosts in this topology are connected to two hosts only, except the end hosts. That is if the end hosts in Daisy Chain are connected then it represents Ring topology. Each link in Daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for its immediate hosts.

Email System

What is email?

Electronic mail (also known as **email** or **e-mail**) is one of the most commonly used services on the Internet, allowing people to send messages to one or more recipients. Email was invented by Ray Tomlinson in 1972.

Why use email?

The operating principle behind email is relatively simple, which has quickly made it the most popular service used on the Internet.

As with a traditional postal service, for your message to reach your recipient, all you need to know is their address. Its two main advantages over "paper mail" are the speed at which the email is sent (practically instantaneous) and the lower cost (included with the cost of an Internet connection). What's more, email can be used to instantaneously send a message to several people at once.

Email addresses

Email addresses (both for senders and recipients) are two strings separated by the character "@" (the "at sign"): **user@domain**

The right-hand part describes the domain name involved, and the left-hand part refers to the user who belongs to that domain.

An email address can be up to 255 characters long and can include the following characters:

- Lowercase letters from a to z;
- Digits
- The characters ".","_" and "-" (full stop, underscore, and hyphen)

In practice, an email address often looks something like this:

firstname.lastname@provider.domain