CHAPTER 1

INTRODUCTION TO INTERNET

1.1 INTRODUCTION

Friends, we are crossing the entry of a new information era in which we are developing tools that permit us to increase human intelligence and obtain the information needed to explore new systems of health care, education, science, manufacturing and business. This new information era is nothing but the "Computer Era".

Today computer is available in many offices and homes and therefore there is a need to share data and programs among various computers. With the advancement of data communication facilities the communication between computers has increased and thus it has extended the power of computer beyond the computer room. Now a user sitting at one place can communicate with computers of any remote site through communication channel. The aim of this lesson is to introduce you the various aspects of computer network.

➢ **Data Communication:**

In years past, we depended on the postal service, telephone, radio, books, or newspapers to send or receive information. The computer has opened a variety of ways to communicate more quickly and effectively. Computer systems that transmit data over communications lines such as telephone lines or cables are called **data communications systems.** These data communications systems have been evolving since the mid-1960s.

In the information technology, a network is a series of points or nodes interconnected by communication paths.

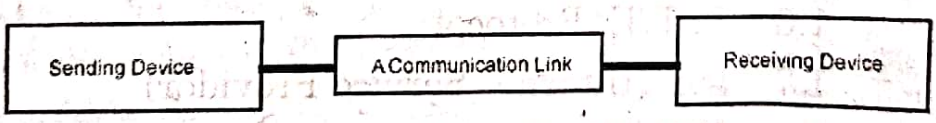
Computer network used for data communication in current information technology.

Computer network means group of two or more computer systems linked together through transmission media for sharing of data.

Example : Suppose a manager has to write several letters to various clients. First he has to use his PC and Word Processing package to prepare the letter, if the PC is connected to the entire client's PC through networking, he can send the letters to all the clients within minutes. Thus irrespective of geographical areas, if PCs are connected through communication channel, the data and information, computer files and any other programs can be transmitted to other computer systems within seconds. The modern form of communication like e-mail and Internet is possible only because of **computer networking.**

➢ **Basic Elements of a Communication System :**

As per the below diagram for sending and receiving information, we will see three elements for communication or network.



COMMUNICATION CHANNEL

(1) The sender (source) who creates the message to be transmitted

(2) A medium that carries the message

(3) The receiver (sink) who receives the message

In data communication four basic terms are frequently used. They are :

- **Data :** A collection of facts in raw forms that become information after Processing.
- **Signals :** Electric or electromagnetic encoding of data.

- **Signaling :** Propagation of signals across a communication medium.
- **Transmission :** Communication of data achieved by the processing of signals.

1.2 DEFINITION OF COMPUTER NETWORK

There is no fix or predefine definition of network but we consider a different no. of sources to define computer network definition.

A computer network, often simply referred to as a network, is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information.

- From: http://www.wikipedia.org

Computer network is a collection of autonomous computers. It means that, various computers connected to each other which should facilitate sharing of resources.

- From: http://www.networkingtipsblog.com

A computer with minimal memory, disk storage and processor power designed to connect to a network, especially the Internet. The idea behind network computers is that many users who are connected to a network don't need all the computer power they get from a typical personal computer. Instead, they can rely on the power of the network servers.

From: http://www.webopedia.com

A computer network is interconnection of various computer systems located at different places. In computer network two or more computers are linked together with a medium and data communication devices for the purpose of communication data and sharing resources. The computer that provides resources to other computers on a network is known as server. In the network the individual computers, which access shared network resources, are known as nodes.

A Computer Network- interconnection of various computer systems.

A common example of communication or network is that when one computer sends an e-mail to another computer. The first computer is sending device and another computer is receiving device. The two computers would probably use phone lines to send / receive their message called it communication link. Each computer will need one other piece of device [called it network device]-- modem.

1.3 TYPES OF NETWORKS

A computer network is a collection of computers and devices connected by communications channels that facilitates communications among users and allows users to share resources with other users. Networks may be classified by various characteristics. Among the characteristics, Common types of computer networks may be classified by their scope / range. These types of characteristic classification called it "area networks". There are three types of area networks:

[1] LAN [Local Area Network] :

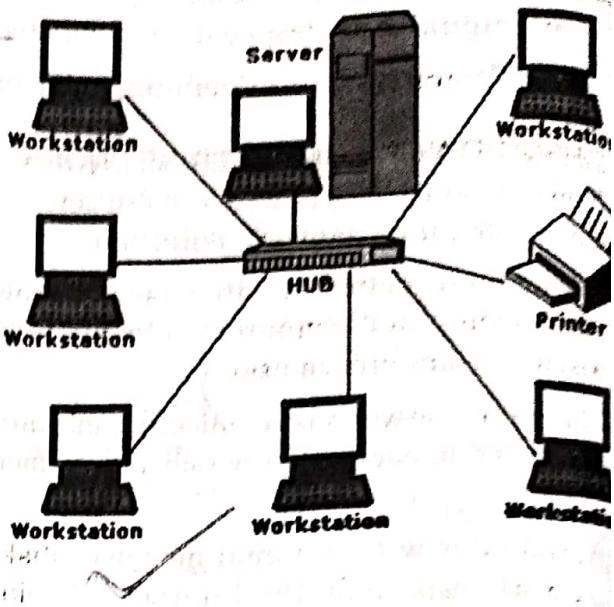
Local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building, a school, or a home). A LAN is useful for sharing resources like files, printers, games or other applications.

Local area network (LAN) is a group of computers and associated devices

Most local area networks are built with relatively inexpensive hardware such as Ethernet cables, network adapters, and hubs. Wireless LAN and other more advanced LAN hardware options also exist.

In Cable LAN, it required no. of computers and each and every computer connected with Hub, Repeater, L2 switches, Cables, Connectors.

In Wireless LAN, it required no. of computers and each and every computer connected with access point, Wireless LAN cards and Antennas.



Use : It used in small level company or organization or institute.

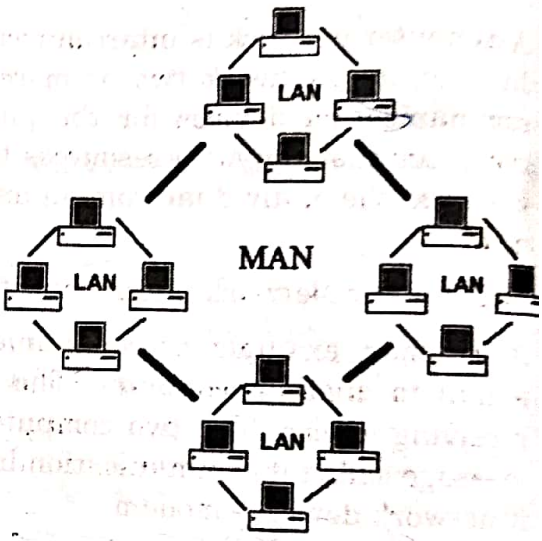
[2] MAN [Metropolitan Area Network] :

A metropolitan area network (MAN) is a large computer network that usually spans a city. A MAN usually interconnects a number of local area networks (LANs) using a high-capacity and hi-speed technology, such as switches or bridges and routers connected with fiber-optical links, and provides up-link services to wide area networks and the Internet.

In MAN, It required Layer 2 switches, bridges, Layer 3 switches and routers, wireless routers etc. for communicate different number of computers.

A Metropolitan Area Network (MAN) is a group of LANs

The best example of these types of network is cable television network.

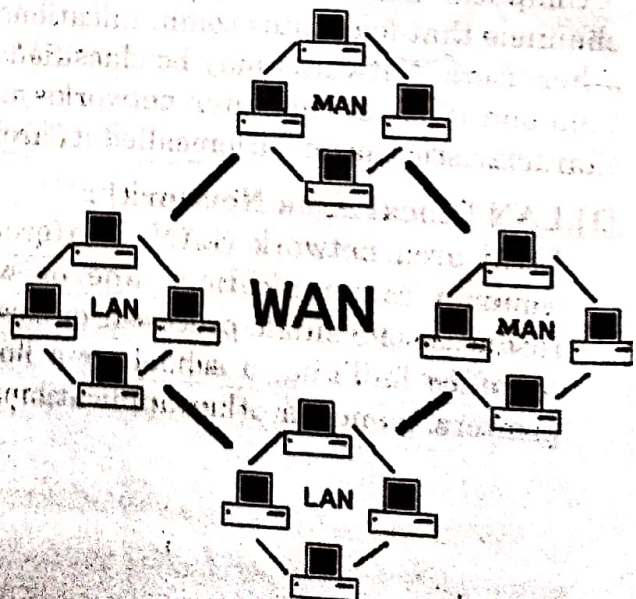


[3] WAN [Wide Area Network] :

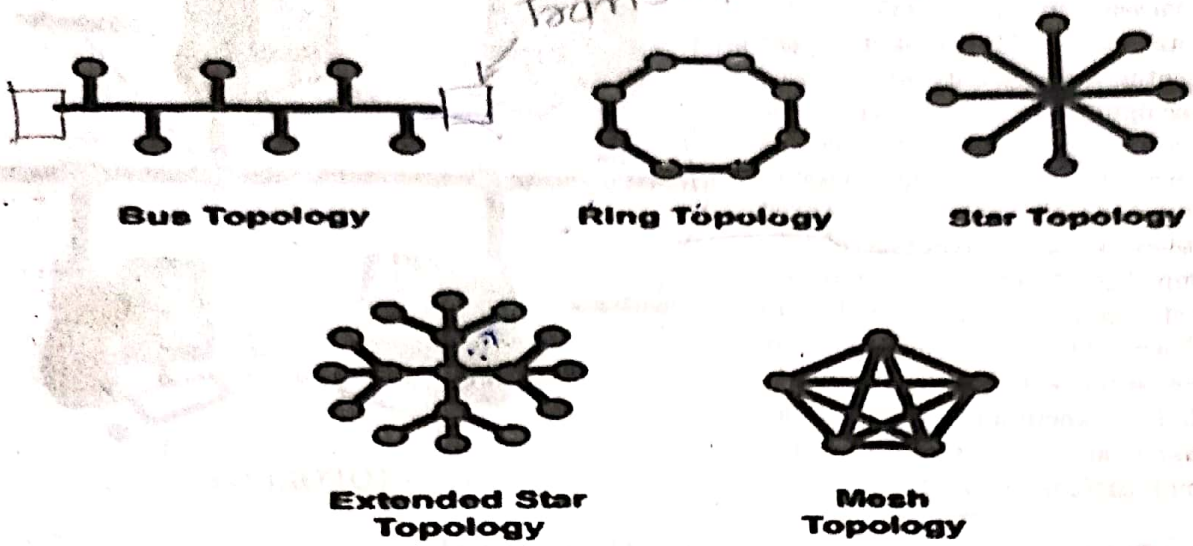
A WAN spans a large geographic area, such as a state, area or country. WANs often connect multiple smaller networks, such as local area networks (LANs) or metro area networks (MANs). The world's most popular WAN is the Internet.

A Wide Area Network (WAN) is a group of MANs.

WANs generally utilize different and much more expensive networking equipment than do LANs or MANs.



1.4 NETWORK TOPOLOGIES



Bus Topology | Ring Topology | Star Topology

Extended Star Topology | Mesh Topology

In Computer Networking, "topology" is basically defined as layout or design of the connected devices. These topologies can be either physical or logical design.

The **Physical Topology** refers to the physical layout of the devices connected to the network. It is also depend on the location and cable installation.

The physical topology means logical structure or layout of the network.

Physical topology always defines first after physical topology logical topology established.

The **Logical Topology** is based on transferring data from one device to other devices.

The logical topology transfer data from one node to another node using transmission media.

Logical topology starts communication

The choice of topology is dependent upon...

- Number of devices being used...
- Applications sharing and rate of data transfers...
- Required response times...
- Cost...

There are six different Networking Topologies

- bus
- ring
- star
- tree
- mesh
- Hybrid

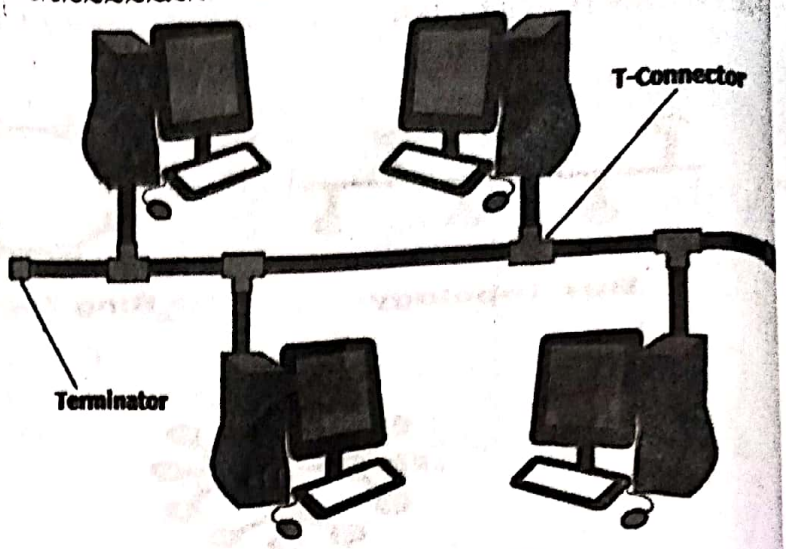
When networks are design using multiple topologies it is called Hybrid Networks, this concept is usually applied in complex networks were larger number of computer clients are required.

[1] Bus topology :

The Bus topology is one of the simplest from all types of topologies. In the bus network topology, every computer is connected to a main cable called the bus.

In bus topology co-axial cable is always used as a main communication cable.

When any computer sends out message in the network, the bus topology is broadcasted in the entire network but only proposed computer accepts the message and process it. Bus topology provide simplicity for passing token to the network, however there is big disadvantage of this topology, if main single network cable gets damaged, it will shut down the entire network no computer will run on network and no communication can be made among computers until main cable is replaced.



BUS TOPOLOGY

Bus Topology- every computer is connected to a main cable

Advantages of Bus Topology :

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.
- Addition of new computers to the network is easy.
- Configuration and maintenance cost is less.

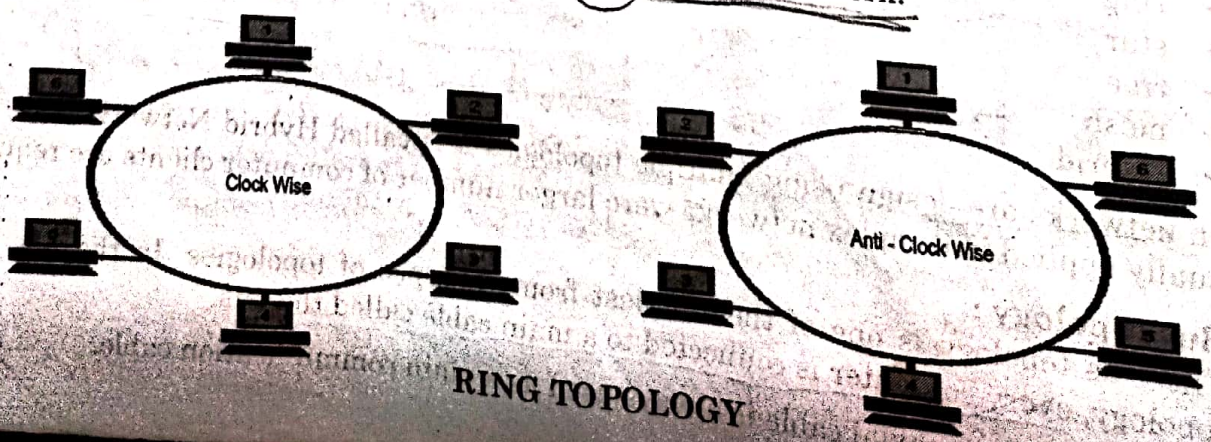
Disadvantages of Bus Topology :

- Entire network shuts down, if there is a break in the main cable.
- Terminators are required at both ends of the main cable.
- Multiple computers can not share data in bus topology.
- Difficult to find the problem if the entire network shuts down.
- If we increase number of computers in this topology then communication speed of network will be down.

[2] Ring Topology :

In ring network topology, computers and other networking devices are connected to each other in a circular way. All messages are passed in the same direction either **clockwise** or **anti-clockwise**. In case of failure of any device or cable the whole network will be down and communication will not be possible.

Ring topology network first implement in IBM company network.



RING TOPOLOGY

Ring Topology- computers and other networking devices are connected to each other in a circular way.

Another **disadvantage** of these types of network topology is more cabling required than bus. The main advantage of these types of network topology is transfer data clockwise and anti-clock wise in the network

Advantages of Ring Topology :

- The ring networks works well where there is no central site computer system. It is truly distributed data processing system.
- It is more reliable than a star network because communication is not dependent on a single host computer. If once line between any two computers breaks down, or if one of the computer breaks down alternate routing is possible.

Disadvantages of Ring Topology :

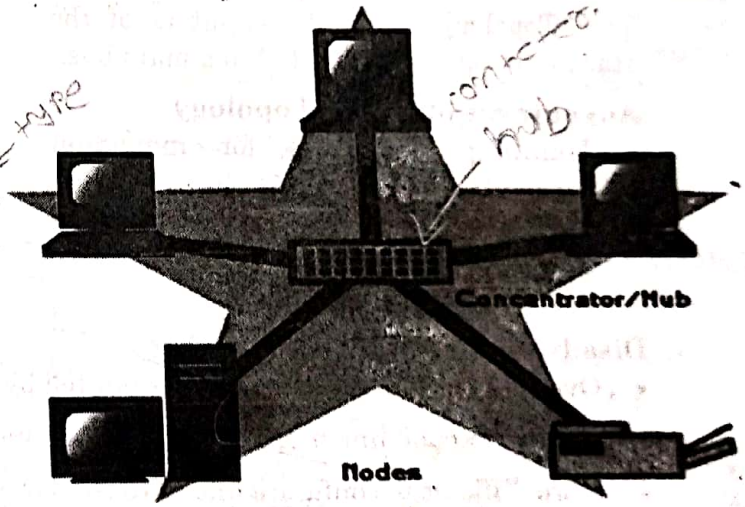
- In a ring network, communication delay is directly proportional to the number of nodes in the network. Hence addition of new nodes in the network increases the communications delays.
- The ring network is not as popular as star network because of its more complicated control software.
- It only share data between two different nodes of this topology so for communication other nodes must have to wait.

[3] Star topology :

This is the most commonly used network topology design in the network topologies. In Star, all computers are connected to central device called hub, router or (switches) using (Unshielded) Twisted Pair (UTP) or Shielded Twisted Pair cables.

Star Topology- all computers are connected to central device.

In star topology, we require more connecting devices like routers, hubs and cables unlike in bus topology where entire network is supported by single main cable.



STAR TOPOLOGY

The most practical point of Star topology success is that the entire network does not go shut down incase of failure of a computer or cable or device, it will only affect the computer whose cable failed. The rest of the network will be working fine. However, incase of failure of central communication device such as Hub, Router or Switch, the entire network will fall down. Star topology is widely used in homes, offices and in buildings because of its commercial success.

All messages are traveled in this topology is between central computers with particular client computer only.

Advantages of a Star Topology :

- Easy to install and remove nodes
- Easy to detect faults
- Transmission delays between two nodes do not increase by adding new nodes to network because any two nodes may be connected via two links only.
- If any of the local computers fails the remaining portion of the network is unaffected.

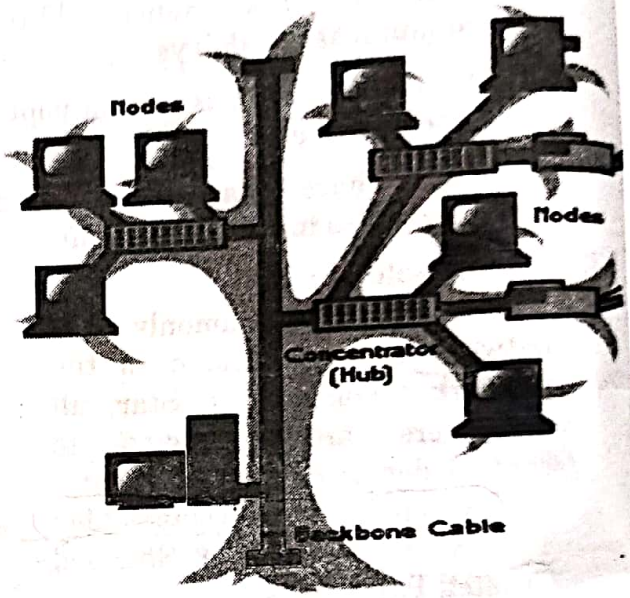
Disadvantages of a Star Topology :

- Requires more cable length than a bus topology.
- Central device failure, entire network failure
- More expensive than bus topologies because of the cost of the hubs, switches or etc.

[4] Tree topology :

A tree topology combines characteristics of bus and star topologies. Central computers of the star networks are connected to a main bus. So, a tree network is a bus network of star networks. The only difference is that the tree topology follows a hierarchy in structure and the entire tree is dependant on this hierarchy.

Tree Topology- Central computers of the star networks are connected to a main bus.



TREE TOPOLOGY

Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages of a Tree Topology:

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.
- Network expansion is difficult and it does not provide speed and performance.

[5] Mesh topology :

Mesh topologies involve the concept of routes. Against of each of the previous topologies messages sent on a mesh network can take any of several possible paths from source to destination.

In mesh topology each and every computer directly connected with all nodes so it requires complex cable configuration.

Advantages of a Tree Topology :

- This type of network is very reliable, as any line breakdown will affects on communication between the connected computers.
- Communication is very fast between any two nodes.

- Various routes available between source and receiver so if one route is fail then data communicates with other routes.

Disadvantages of a Tree Topology :

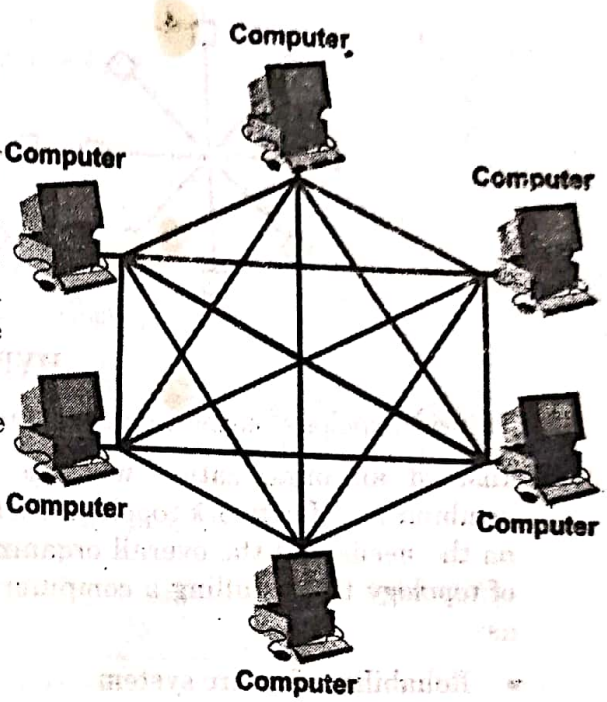
- It is most expensive system from the point of view of line cost. if there are (n) nodes in the network, then n (n-1)/2 links are required. Thus the cost of linking the system grows with the square of the numbers of the nodes.
- Additions of the new nodes to the network are difficult.
- Configuration and maintenance cost of mesh topology is high.

There are two types of mesh topology :

Fully connected Mesh topology :

The type of network topology in which all of the nodes are interconnected with each other nodes in a network called it fully connected mesh topology. The fully connected mesh topology is generally too costly and complex for networks, although the topology is used when there are only a small number of nodes to be interconnected.

Fully Connected- All of the nodes are interconnected.

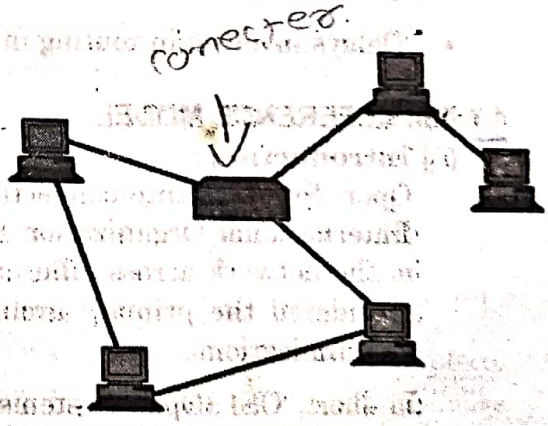


FULLY CONNECTED MESH TOPOLOGY

Partially connected Mesh topology :

The type of network topology in which some of the nodes of the network are connected to more than one other node in the entire network called it partially connected mesh topology.

Partially Connected- Some of the nodes of the network are connected to more than one other node

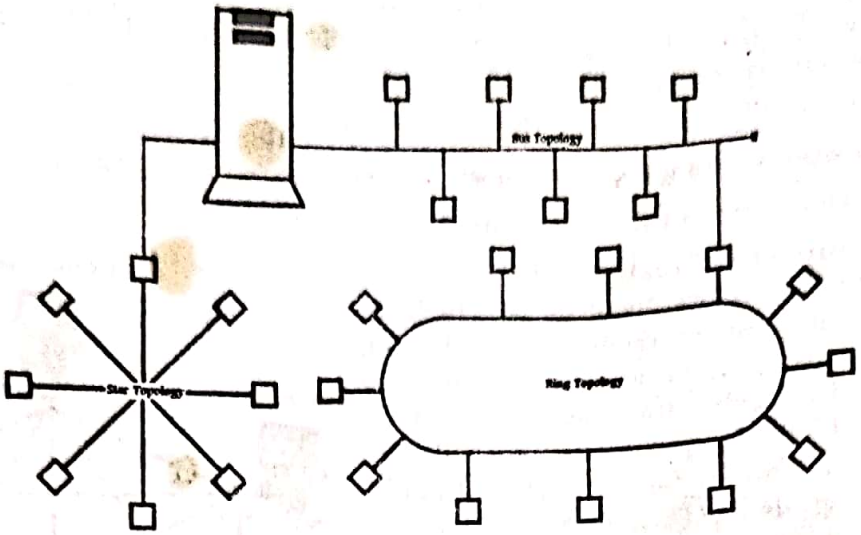


PARTIALLY CONNECTED MESH TOPOLOGY

[6] Hybrid topology :

Different networks configurations have their own advantages and disadvantages. Hence in reality, a pour star, ring, or completely connected network is rarely used.

BUS + Ring + Star



HYBRID TOPOLOGY

Hybrid Topology- a combination of network topologies.

Instead an organization will use some sort of hybrid network, which is simply a combination of network topologies. The exact shape of configuration of the network depends on the needs and the overall organizational structure of the company involved. The choice of topology for installing a computer network depends upon a combination of factors such as:

- Reliability of entire system
- Expandability of system
- Availability of communication lines
- Delays involved in routing information from one nodes to another.

1.5 OSI REFERENCE MODEL

[1] Introduction :

Open Systems Interconnection (OSI) model is a reference model developed by ISO (International Organization for Standardization) . it is a standards for communication in the network across different devices and applications by different vendors. It is now considered the primary architectural model for inter-computing and internetworking communications.

In short, OSI (Open Systems Interconnection) is a standard description or "reference model" for how data should be transmitted between any two points in a telecommunication network.

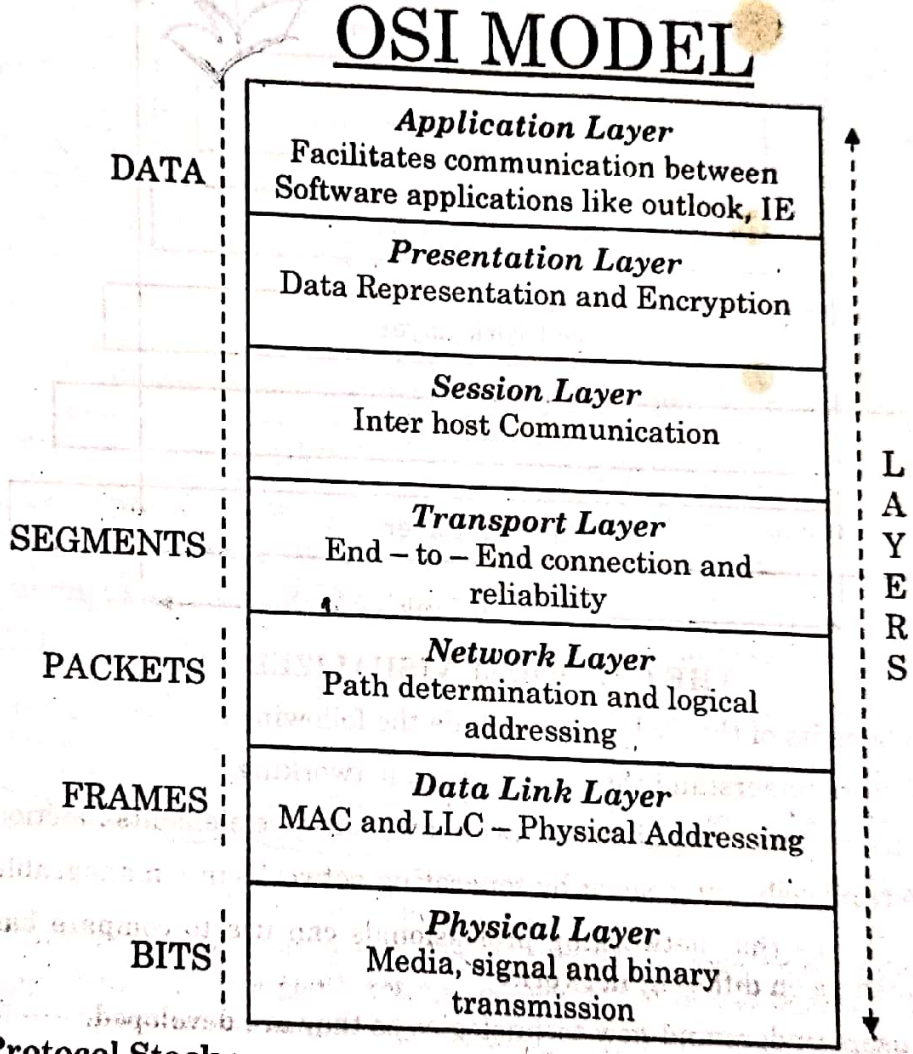
This model defines 7 Layers that describe how applications running upon network-aware devices may communicate with each other.

Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently.

The OSI 7 layers model has clear characteristics. Layers 7 to 4, deal with end-to- end communications between data source and destinations. Layers 3 to 1 deal with communications between network devices.

On the other hand, the seven layers of the OSI model can be divided into two groups: upper layers (layers 7, 6 & 5) and lower layers (layers 4, 3, 2, 1). The upper layers of the OSI model deal with application issues and generally are implemented only in software.

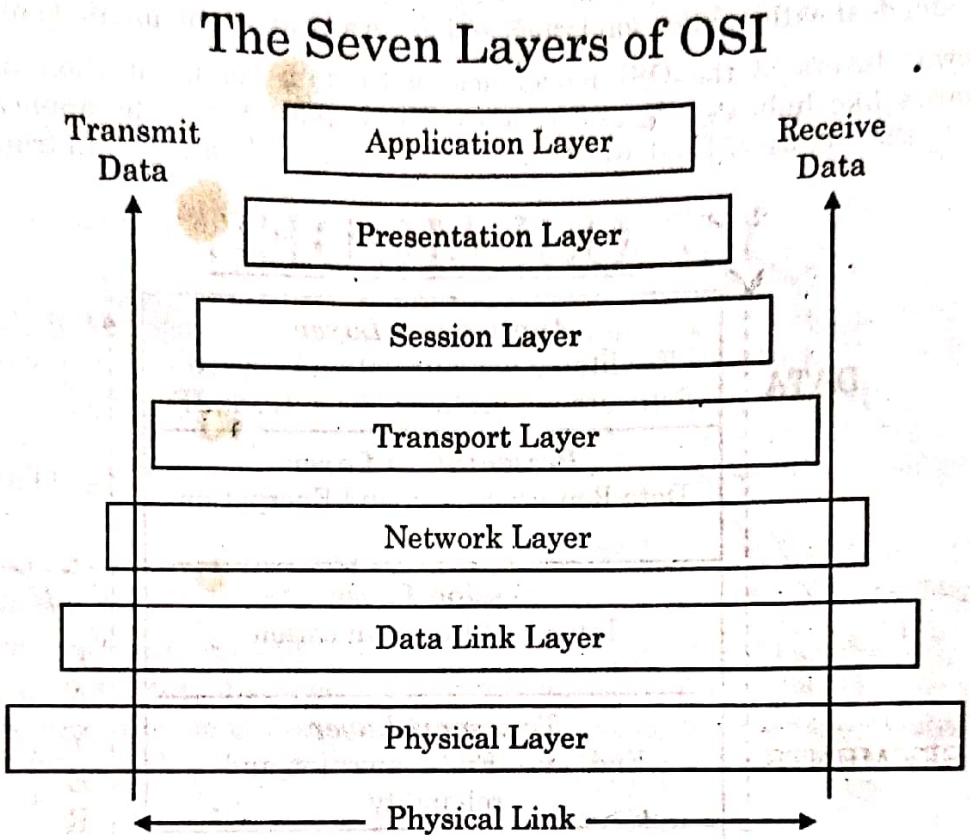
The lower layers of the OSI model deal with data communication using different hardware's like hub, switch, and routers. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues.



➤ **The Protocol Stack :**

The collection of communication layers is commonly referred to as the 'protocol stack', visualized as a stack of seven interconnecting sections. Each layer accomplishes its own task and then hands the information on to the next layer, using a variety of protocols (called it "communication standards") to interface with the user, for operating system functions, information conversion and the delivery of this information to the destination device. Communication between Layers The various layers pass network requests to each other using a particular protocol. Typically these protocols add control, encapsulation, conversion functions and/or routing information to the front or back of the original message. This allows seemingly transparent delivery of the message to the destination.

➢ **Communication between Layers :**
The various layers pass network requests to each other using a particular protoc
Typically these protocols add control, encapsulation, conversion functions and/or routi
information to the front or back of the original message. This allows seeming
transparent delivery of the message to the destination.



THE OSI MODEL VISUALIZED

The main benefits of the OSI model include the following :

- Helps users understand the big picture of networking.
- Helps users understand how hardware and software elements function together.
- Makes troubleshooting easier by separating networks into manageable pieces.
- Defines terms that networking professionals can use to compare basic. Functiona relationships on different networks.
- Helps users understand new technologies as they are developed.
- Aids in interpreting vendor explanations of product functionality.

[2] Description of OSI Model- Seven Layers :

In the OSI model, data communication starts with the top layer at the sending side, travel down the OSI model stack to the bottom layer, and then traverses the network connectio to the bottom layer on the receiving side, and up its OSI model stack.

➢ **Layer-1 Physical Layer :**
The physical layer of the OSI model defines connector and interface specifications, a well as the medium (cable) requirements. Electrical, mechanical, functional, an procedural specifications are provided for sending a bit stream on a computer network.

Components of the physical layer include :

- Cabling system components
- Adapters that connect media to physical interfaces
- Connector design and pin assignments
- Hub, repeater, and patch panel specifications
- Wireless system components
- Parallel SCSI (Small Computer System Interface)
- Network Interface Card (NIC)

Note : The Physical Layer of the OSI model is only part of a LAN (Local Area Network).

➢ **Layer-2 Data Link Layer :**

This layer deals with getting data across a specific medium and individual links by providing one or more data link connections between two network entities. End points are specifically identified, if required by the Network layer Sequencing. The frames are maintained in the correct sequence and there are facilities for Flow control and Quality of Service (QoS) parameters such as Throughput, Service Availability and Transit Delay.

The Data link layer performs the error check using the Frame Check Sequence (FCS) in the trailer and discards the frame if an error is detected. It then looks at the addresses to see if it needs to process the rest of the frame itself or whether to pass it on to another host. The data between the header and the trailer is passed to layer 3.

Common networking components that function at layer 2 include:

- Network interface cards
- Ethernet and Token Ring switches
- Bridges

➢ **Layer-3 Network Layer :**

This layer of the OSI model provides an end-to-end logical addressing system so that a packet of data can be routed across several layer 2 networks (Ethernet, Token Ring, Frame Relay, etc.). Note that, network layer addresses can also be referred to as logical addresses. Initially, software manufacturers, such as Novell, developed proprietary layer 3 addressing. However, the networking industry has evolved to the point that it requires a common layer 3 addressing system. The Internet Protocol (IP) addresses make networks easier to both set up and connect with one another. The Internet uses IP addressing to provide connectivity to millions of networks around the world.

To make it easier to manage the network and control the flow of packets, many organizations separate their network layer addressing into smaller parts known as subnets. Routers use the network or subnet portion of the IP addressing to route traffic between different networks. Each router must be configured specifically for the networks or subnets that will be connected to its interfaces.

When passing packets between different networks, it may become necessary to adjus their outbound size to one that is compatible with the layer 2 protocol that is bein used. The network layer accomplishes this via a process known as fragmentation. router's network layer is usually responsible for doing the fragmentation.

All reassembly of fragmented packets happens at the network layer of the final destination system.

Two of the additional functions of the network layer are diagnostics and the reporting of logical variations in normal network operation. While the network layer diagnostics may be initiated by any networked system, the system discovering the variation reports it to the original sender of the packet that is found to be outside normal network operation.

The variation reporting exception is content validation calculations. If the calculation done by the receiving system does not match the value sent by the originating system, the receiver discards the related packet with no report to the sender. Retransmission is left to a higher layer's protocol.

Some basic security functionality can also be set up by filtering traffic using layer 3 addressing on routers or other similar devices.

➢ **Layer-4 Transport Layer :**

This layer is responsible for the ordering and reassembly of packets that may have been broken up to travel across certain media. Some protocols in this layer also perform error recovery. After error recovery and reordering the data part is passed up to layer 5.

Some of the functions offered by the transport layer include :

- Application identification
- Client-side entity identification
- Confirmation that the entire message arrived intact
- Segmentation of data for network transport
- Control of data flow to prevent memory overruns
- Establishment and maintenance of both ends of virtual circuits
- Transmission-error detection
- Realignment of segmented data in the correct order on the receiving side
- Multiplexing or sharing of multiple sessions over a single physical link

The most common transport layer protocols are the connection-oriented TCP Transmission Control Protocol (TCP) and the connectionless UDP User Datagram Protocol (UDP).

➢ **Layer-5 Session Layer :**

The session layer provides various services, including tracking the number of bytes that each end of the session has acknowledged receiving from the other end of the session. This session layer allows applications functioning on devices to establish, manage, and terminate a dialog through a network.

Session layer functionality includes :

- Virtual connection between application entities
- Synchronization of data flow
- Creation of dialog units
- Connection parameter negotiations
- Partitioning of services into functional groups
- Acknowledgements of data received during a session
- Retransmission of data if it is not received by a device

➢ **Layer-6 Presentation Layer :**

This provides function call exchange between host operating systems and software layers. The presentation layer is responsible for how an application formats the data to be sent out onto the network. The presentation layer basically allows an application to read (or understand) the message.

Presentation layer functionality includes :

- Encryption and decryption of a message for security
- Compression and expansion of a message so that it travels efficiently
- Graphics formatting
- Content translation
- System-specific translation

➢ **Layer-7 Application Layer :**

The application layer provides an interface for the end user operating a device connected to a network.

This layer is what the user sees, in terms of loading an application (such as web browser or e-mail); that is, this application layer is the data the user views while using these applications.

Application layer functionality includes :

- Support for file transfers
- Ability to print on a network
- Electronic mail
- Electronic messaging
- Browsing the World Wide Web

➢ **The ISO / OSI 7 Layer Model Summary :**

LAYER NO.	LAYER NAME	DATA TRANSMISION FORMAT	DEVICES	PROTOCOLS	DESCRIPTON	LAYER FORMAT
7	APPLICATION			HTTP, SMTP, FTP, TELNET	The layer represents the services that directly support applications such as software for file transfers, database access, and electronic mail.	SOFTWARE LAYER
6	PRESENTATION			MIME, XML, JPEG	This layer manages security issues by providing services such as data encryption, and compresses data so that fewer bits need to be transferred on the network.	SOFTWARE LAYER
5	SESSION			NFX, X11, RPC	The session layer allows two applications on different computers	SOFTWARE LAYER

					to establish, use, and end a session. This layer establishes dialog control between the two computers in a session, regulating which side transmits, plus when and how long it transmits.	
4	TRANSPORT	SAGMENT		TCP, UDP	The transport layer handles error recognition and recovery. The receiving transport layer also sends receipt ack. Msgs.	COMMUNICATION LAYER
3	NETWORK	PACKET	ROUTER, LAYER3 SWITCHES	IP	The network layer addresses messages and translates logical addresses and names into physical addresses. It also determines the route from the soucre to the destination computer and manages traffic problems, such as switching, routing, and controlling the congestion of data packets.	HARDWARE LAYER
2	DATALINK	FRAME	SWITCHES, BRIDGES	MAC/LLC, HDLC, ARP	This layer is responsible for transferring frames from one computer to another, without errors. After sending a frame, it waits for an acknowledgment from the receiving computer.	HARDWARE LAYER
1	PHYSICAL	BIT	HUB, REPEATERS, LAN CARD, CABLES	Ethernet, Token Ring, FDDI, 802.11	The physical layer transmits bits from one computer to another and regulates the transmission of a stream of bits over a physical medium.	HARDWARE LAYER

1.6 TCP/IP PROTOCOL

Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry standard suite of protocols that is designed for large networks consisting of network segments that are connected by routers. TCP/IP is the protocol that is used on the Internet, which is the collection of thousands of networks worldwide that connect research facilities, universities, libraries, government agencies, private companies, and individuals.

[1] History :

The roots of TCP/IP can be traced back to research conducted by the United States Department of Defense (DoD) Advanced Research Projects Agency (DARPA) in the late 1960s and early 1970s. The following list highlights some important TCP/IP milestones:

- In 1970, ARPANET hosts started to use Network Control Protocol (NCP), a preliminary form of what would become the Transmission Control Protocol (TCP).
- In 1972, the Telnet protocol was introduced. Telnet is used for terminal emulation to connect dissimilar systems. In the early 1970s, these systems were different types of mainframe computers.
- In 1973, the File Transfer Protocol (FTP) was introduced. FTP is used to exchange files between dissimilar systems.
- In 1974, the Transmission Control Protocol (TCP) was specified in detail. TCP replaced NCP and provided enhanced reliable communication services.
- In 1981, the Internet Protocol (IP) (also known as IP version 4 [IPv4]) was specified in detail. IP provides addressing and routing functions for end-to-end delivery.
- In 1982, the Defense Communications Agency (DCA) and ARPA established the Transmission Control Protocol (TCP) and Internet Protocol (IP) as the TCP/IP protocol suite.
- In 1983, ARPANET switched from NCP to TCP/IP.
- In 1984, the Domain Name System (DNS) was introduced. DNS resolves domain names (such as www.example.com) to IP addresses (such as 192.168.5.18).
- In 1995, Internet service providers (ISPs) began to offer Internet access to businesses and individuals.
- In 1996, the Hypertext Transfer Protocol (HTTP) was introduced. The World Wide Web uses HTTP.
- In 1996, the first set of IP version 6 (IPv6) standards were published.

[2] TCP/IP :

- A The TCP/IP protocol suite (also commonly called the Internet protocol suite) was originally developed by the United States Department of Defense (DoD) to provide robust service on large internetworks that incorporate a variety of computer types.
- Main purpose of this protocol was for it to be hardware-independent.
- In some literature, the TCP/IP protocol suite is referred to as the DoD model.
- In recent years, the Internet protocols constitute the most popular network protocols currently in use.
- One reason for the popularity of TCP/IP is that no one vendor owns it, unlike the IPX/SPX, DNA, SNA, or AppleTalk protocol suites, all of which are controlled by specific companies.
- TCP/IP evolved in response to input from a wide variety of industry sources.
- TCP/IP is the most open of the protocol suites and is supported by the widest variety of vendors. Virtually every brand of computing equipment now supports TCP/IP.
- This has lead to some problems, though. Because TCP/IP is an open standard, sometimes one vendor's implementation of TCP/IP does not work with another's implementation.

OSI	TCP / IP (DoD)
Application (Layer 7)	Application (Process)
Presentation (Layer 6)	
Session (Layer 5)	
Transport (Layer 4)	Host to Host (Transport)
Network (Layer 3)	Internet
Data Link (Layer 2)	Network Access (Subnet)
Physical (Layer 1)	

- The model for the Internet protocol suite has four layers (refer to Figure). From t model, you can see the approximate relationships of the layers.

[3] The DoD(TCP/IP) model's layers function as follows :

- **The Network Access layer** corresponds to the bottom two layers of the OSI mo This orrespondence enables the DoD protocols to coexist with existing Data Link a Physical layer standards.
- **The Internet layer** corresponds roughly to the OSI Network layer. Protocols at t layer move data between devices on networks.
- **The Host-to-Host layer** can be compared to the OSI Transport layer. Host-to-Ho protocols enable peer communication between hosts on the internetwork. (At the ti these protocols were designed, personal computers and workstations didn't exist, and network computers were host computers. As a result, devices on TCP/IP networks a typically referred to as hosts. The concept of a client/server relationship didn't exist, a all communicating hosts were assumed to be peers.)
- **The Process/Application** layer embraces functions of the OSI Session, Presentatio and Application layers. Protocols at this layer provide network services.
- One huge advantage of using TCP/IP is that TCP/IP is required for communication ov the Internet; thus the Internet can be used as a communication backbone.
- A large number of protocols are associated with TCP/IP. These different protocols a grouped into the following unofficial categories :
  - General TCP/IP Transport Protocols
  - TCP/IP Services
  - TCP/IP Routing

Advantages :

- Supports networking services better than the other Windows XP protocols
- Multiple routing protocols
- Good error detection and handling
- Works with most kinds of computers

Disadvantages :

- Not fast
- Not easy to use
- Requires
  - Fair degree of expertise
  - Careful planning
  - Constant maintenance and attention
- Mass of information and detail work

[4] TCP and IP both are different protocol but it used for common purpose and the purpose is communication between two different nodes.

- **TCP (Transmission Control Protocol) :**
  TCP is used for transmission of data from an application to the network. TCP is responsible for breaking data down into IP packets before they are sent, and for assembling the packets when they arrive.

- **IP (Internet Protocol) :**
  IP takes care of the communication with other computers. IP is responsible for the sending and receiving data packets over the Internet.

  TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

  TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

  TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "stateless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone conversations that require a dedicated connection for the call duration). Being stateless frees network paths so that everyone can use them continuously. (Note that the TCP layer itself is not stateless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.)

  Many Internet users are familiar with the even higher layer application protocols that use TCP/IP to get to the Internet. These include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Telnet (Telnet) which lets you logon to remote computers, and the Simple Mail Transfer Protocol (SMTP). These and other protocols are often packaged together with TCP/IP as a "suite."

  Personal computer users with an analog phone modem connection to the Internet usually get to the Internet through the Serial Line Internet Protocol (SLIP) or the Point-to-Point Protocol (PPP). These protocols encapsulate the IP packets so that they can be sent over the dial-up phone connection to an access provider's modem.

  Protocols related to TCP/IP include the User Datagram Protocol (UDP), which is used instead of TCP for special purposes. Other protocols are used by network host computers for exchanging router information. These include the Internet Control Message Protocol (ICMP), the Interior Gateway Protocol (IGP), the Exterior Gateway Protocol (EGP), and the Border Gateway Protocol (BGP).

1.7 ISP (INTERNET SERVICE PROVIDER)

An ISP is also sometimes referred to as an IAP (Internet access provider). ISP is sometimes used as an abbreviation for *independent service provider* to distinguish a service provider that is an independent, separate company from a telephone company.

An Internet service provider (ISP) is an organization that provides access to the Internet.

- From www.wikipedia.org

Short for *Internet Service Provider*, it refers to a company that provides Internet services including personal and business access to the Internet. For a monthly fee, the service provider usually provides a software package,

- From www.webopedia.com

An Internet Service Provider (also known as an ISP or even as an IAP, internet access provider) is a firm that offers subscribers access to the internet.

- From www.whatismyipaddress.com

An ISP (Internet Service Provider) is a company that collects a monthly or yearly fee in exchange for providing the subscriber with Internet access.

- From www.wisegeek.com

An ISP might provide dial-up service, cable, DSL, or other types of Internet access. Some ISPs are local while others are national. A national ISP will provide access throughout most of the nation, while a local ISP will only serve subscribers in a limited geographical region.

When looking for an ISP the initial consideration is the type of access desired. Some ISPs only offer dial-up access which is the slowest type of connection. If you want cable service, you'll be checking with your local cable TV provider to see if cable access is offered. For DSL service, you may have multiple choices - or it could be that DSL is not yet available in your area. Often this can be remedied with a call to the phone company to upgrade local telephone lines.

ISP services range in price according to the package offered, and type of service. Dial-up is least expensive, and perks will vary greatly between ISPs. Some offer multiple email accounts, others vast amounts of webspace, and still others discounts for paying in advance. DSL and cable companies will also differ, so carefully read through offerings before deciding. If you are getting an ISP other than cable, you will likely have choices. There are many websites that offer reviews from present subscribers of various ISPs, which might be helpful in making a decision.

➢ **Types of an ISP :**

As per the Customer requirement, ISPs can be varied...

- **Hosting ISPs :**

  A web hosting service is a type of Internet hosting service that allows individuals and organizations to make their website accessible via the World Wide Web.

  The ISP provides web hosting related services like FTP, e-mail, SSL, Web server, Control Panel, etc...

- **Transit ISPs :**

  Internet transit *is the service of allowing network traffic to cross or "transit" a computer network, usually used to connect a smaller Internet service provider (ISP) to the larger Internet.*

  Just as their customers pay them for Internet access, ISPs themselves pay upstream ISPs for Internet access. An upstream ISP usually has a larger network than the contracting ISP and/or is able to provide the contracting ISP with access to parts of the Internet the contracting ISP by itself has no access to.

- **Virtual ISPs / Wholesale ISP :**
  A Virtual ISP (VISP) or Wholesale ISP is an operation which purchases services from another ISP which allows the VISP's customers to access the Internet using services and infrastructure owned and operated by the wholesale ISP.

- **Free ISPs :**
  This type of ISPs provides free of charge services. Many free ISPs display advertisements while the user is connected like commercial television, in a sense they are selling the users' attention to the advertiser. Other free ISPs, often called freenets, are run on a nonprofit basis, usually with volunteer staff.

1.8 URL (UNIFORM RESOURCE LOCATOR)

A uniform resource locator (URL) is a specific character string that constitutes a reference to an Internet resource. ***- From www.wikipedia.org***

URI is an acronym for Universal Resource Identifier.

It is a standard for identifying a resource (site, name, application, etc.) across a computer network (the biggest example being the Internet!) ***- From www.answers.com***

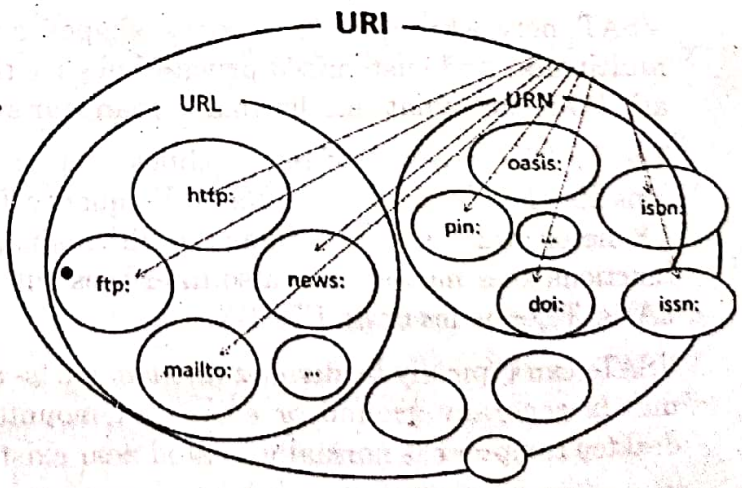
URL stands for Uniform Resource Locator. A URL is a formatted text string used by Web browsers, email clients and other software to identify a network resource on the Internet. Network resources are files that can be plain Web pages, other text documents, graphics, or programs. ***- From www.about.com***

The unique Internet address assigned to a Web document or resource by which it can be accessed by all Web browsers. ***- From www.answers.com***

➢ **URI (Uniform Resource Identifier) :**
URI is a method of identifying a unit of content on the internet. Content can be text page, image file, audio or video file or anything that exist on the web. Other methods (Such as URL or URN) are subset of URI.

➢ **URL (Uniform Resource Locator) :**
URL (a type of URI) is a unique address of the content unit on the web. For example 'http://www.test.com/temp' is the address of the webpage titled 'test' and uses HTTP protocol. Similarly, we can have address of image file, audio file, video file stored on web server. FTP is another protocol that can be used for transferring (or downloading) files. The address would start with ftp:// . Mailto is another protocol that can be used for identifying email address.

➢ **URN (Uniform Resource Name) :**
URN (a type of URI) is a name identifier of the file or content on the web. The idea was that the content can move from website to other. URN will still uniquely identify it irrespective of location stored.



URI- A compact sequence of characters that identifies an abstract or physical resource

➢ **The Difference Between Them :**
So what *is* the difference between URI and URL? It's not as clear cut as I would like, but here's my try at it.

One can classify URIs as locators (URLs), or as names (URNs), or as both. A Unif Resource Name (URN) functions like a person's name, while a Uniform Resource Loca (URL) resembles that person's street address. In other words: the URN defines an ite identity, while the URL provides a method for finding it.

- **For example,**
  The ISBN system for uniquely identifying books provides a typical example of the use URNs. ISBN 0486275574 (urn:isbn:0-486-27557-4) cites clearly a specific edition Shakespeare's play Romeo and Juliet. In order to gain access to this object and read book, one would need its location: a URL address. A typical URL for this book on Unix-like operating system would be a file path such file:///home/username/RomeoAndJuliet.pdf, identifying the electronic book saved in a on a local hard disk. So URNs and URLs have complementary purposes.

  A URL is a type of URI (Uniform Resource Identifier, formerly called Univers Resource Identifier.).

V-SAT

1.9 VSAT (VERY SMALL APERTURE TERMINAL)

In 1920s, Orbital Data Net specializes in the design and construction of VSAT networks as we as using other more exotic technologies. VSAT stands for "Very Small Aperture Terminal" an refers to receive / transmit terminals installed at dispersed sites connecting to a central hub v satellite using small diameter antenna dishes (.75 to 3.8 meter).

In other words, The term Very Small Aperture Terminal (VSAT) refers to a small fixed ear station. VSATs provide the vital communication link required to set up a satellite base communication network. VSATs can support any communication requirement be it voice, data or video conferencing.

VSAT technology represents a cost effective solution for users seeking an independen communications network connecting a large number of geographically dispersed sites. VSA networks offer value-added satellite-based services capable of supporting the Internet, LAN voice/fax communications, video, security, and provide powerful, dependable private and publi network communications solutions.

Generally, these systems operate in the Ku-band and C-band frequencies, and soon Ka-band Ku-band based networks are used primarily in Europe and North America and utilize th smaller sizes of VSAT antennas. C-band, used extensively in Asia, Africa and Latin America require larger antenna sizes.

VSAT networks come in various shapes and sizes ranging from point-to-point, point-to multipoint, and customized private hubs for thousands of sites. Mesh systems have tradition ally been somewhat smaller in size than star systems—5 to 30 sites is a good rule of thumb.

The VSAT comprises of two modules - an outdoor unit and an indoor unit. The outdoor uni consists of an Antenna and Radio Frequency Transceiver. (RFT). The antenna size is typically 1.8 meter or 2.4 meter in diameter, although smaller antennas are also in use. The indoor uni functions as a modem and also interfaces with the end user equipment like stand alone PCs LANs, Telephones or an EPABX.

VSATs can typically be divided into two parts- an outdoor unit and an indoor unit. The outdoo unit is generally ground or even wall mounted and the indoor unit which is the size of a desktop computer is normally located near existing computer equipment in your office.

The outdoor unit is connected through a low loss coaxial cable to the indoor unit. The typical limit of an IFL cable is about 300 feet.

- **Access Technologies in VSAT :**
  The primary objective and advantage of these networks is to maximize the use of common satellite and other resources amongst all VSAT sites. The method by which these networks optimize the use of satellite capacity, and spectrum utilization in a flexible and cost effective manner are referred to as satellite access schemes. Each of the above topologies is associated with an appropriate satellite access scheme.

  The most commonly used satellite access schemes are :
  - Time Division Multiple Access(TDMA)
  - Frequency Division Multiple Access(FDMA)
  - Code Division Multiple Access(CDMA)
  - Demand Assigned Multiple Access(DAMA)
  - Pre-Assigned Multiple Access(PAMA)
  - Frequency-Time Division Multiple Access(FTDMA)

  Advantages :
  If by now you believe that VSATs provide an edge over terrestrial lines only in cases where the land lines are difficult to install, say in the case of remote locations, then consider this. Close to 50 percent of the total VSAT population is installed in the US which also boasts of world's best terrestrial communications.

  Networking of business activities, processes and divisions is essential to gain a competitive edge in any industry. VSATs are an ideal option for networking because they enable Enterprise Wide Networking with high reliability and a wide reach which extends even to remote sites.

- **Last Mile Problem :**
  Let us begin with the situation where you have reliable high-speed links between city exchanges for meeting your communication requirements. But before you begin to feel comfortable, connections from the nearest exchange to your company's office often fail. Consequently, stretching what is technically called the last mile problem into much longer distances. VSATs located at your premises guarantee seamless communication even across the last mile.

- **Reach :**
  You must be well aware of the limitations faced by terrestrial lines in reaching remote and other difficult locations. VSATs, on the other hand, offer you unrestricted and unlimited reach.

- **Reliability :**
  Uptime of upto 99.5 percent is achievable on a VSAT network. This is significantly higher than the typical leased line uptime of approximately 80 to 85 percent.

- **Time :**
  VSAT deployment takes no more than 4-6 weeks as compared to 4 to 6 months for leased lines.

- **Network Management :**
  Network monitoring and control of the entire VSAT network is much simpler than a network of leased lines, involving multiple carriers at multiple locations. A much smaller number of elements needs to be monitored incase of a VSAT network and also the number of vendors and carriers involved in between any two user terminals in a VSAT network is typically one. This results in a single point of contact for resolving all your VSAT networking issues. A VSAT NMS easily integrates end-to-end monitoring and configuration control for all network subsystems.

➢ **Maintenance :**

A single point contact for operation, maintenance, rapid fault isolation and trouble sho makes things very simple for a client, using VSAT services. VSATs also enjoy a low m time to repair (MTTR) of a few hours, which extends upto a few days in the case of le lines. Essentially, lesser elements imply lower MTTR.

➢ **Flexibility :**

VSAT networks offer enormous expansion capabilities. This feature factors in change the business environment and traffic loads that can be easily accommodated o technology migration path. Additional VSATs can be rapidly installed to support network expansion to any site, no matter however remote.

➢ **Cost :**

A comparison of costs between a VSAT network and a leased line network reveals tha VSAT network offers significant savings over a two to three years timeframe. This does take into account the cost of downtime, inclusion of which would result in the VS network being much more cost - effective. Pay-by-mile concept in case of leased line se the costs spiraling upwards. More so if the locations to be linked are dispersed all over country. Compare this to VSATs where the distance has nothing to do with the co Additionally, in case of VSATs, the service charges depend on the bandwidth which allocated to your network in line with your requirements. Whereas with a leased line get a dedicated circuit in multiples of 64Kbps whether you need that amount of bandwi or not.

➢ **Some examples of uses we commonly see for receive only are :**

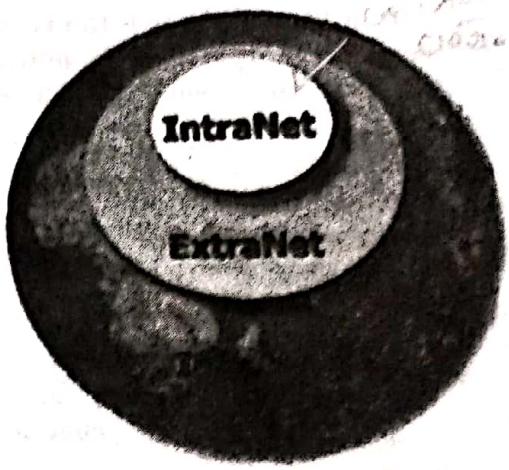
- Stock market & other news broadcasting
- Training or continuing education from a distance
- Distribute financial trends & analyses
- Introduce new products at geographically dispersed locations
- Update market related data, news, and catalog prices
- Distribute video or TV programs (Directv and DISH)
- Distribute music in stores & public areas
- Relay advertising to electronic signs in retail stores

➢ **Some examples of uses we see for receive/transmit are :**

- Interactive computer transactions .
- Internet
- Distance Learning Video Teleconferencing
- Database inquiries
- Bank transactions, ATM
- Reservation systems
- Distributed remote process control and telemetry
- VoIP communications
- Airport flight and weather data
- Emergency services
- Electronic fund transfer at Point-of-Sale
- E-mail
- Medical data transfer
- Sales monitoring & stock control
- Surveillance and monitoring

1.10 INTRANET TO A PRIVATE NETWORK

The Internet had made the sharing of data and other information between businesses, the customers and partners extremely easy, even if the users are located across great distances. Likewise, the navigation of the World Wide Web has been readily streamlined in such a way that information can be retrieved quickly, and requires little installed software beyond a Web browser. However, the downside of the Internet is that this information is also available in such a way that it can be found and accessed by other users, as well.



The first intranet websites and home pages began to appear in organizations in 1996-1997. Although not officially noted, the term intranet first became common-place among early adopters, such as universities and technology corporations, in 1992.

➢ **Definition of Intranet :**

An intranet is a computer network that uses Internet Protocol technology to share information, operational systems, or computing services within an organization.

- From www.wikipedia.org/

An Intranet is a network based on the internet TCP/IP open standard. An intranet belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others with authorization. *- From: www.webopedia.com/*

An "intranet" is the generic term for a collection of private computer networks within an organization. *- From www.about.com/*

For those interested in the background of the term "intranet", it's helpful to splice up the word and look at how it relates to the larger internet.

"Inter" means "between."

"Intra" means "within."

The "internet" is a web between many networks.

An "intranet" is a web within a network.

The internet connects many people to many websites and many networks. An intranet connects people within a network. So your intranet is simply a website within your company's network that (mostly) only employees can access.

"An Intranet is used to convey information," - says Charles Kolody, an analyst with IDC, a Framingham, Mass. research firm. He says that an Intranet is ideal for any company that wants to have a single point where employees can get information about the company. Information about training, benefits, products, or customers can be deployed on the company's Intranet, but that information will be protected from outsiders.

Unlike a LAN, an Intranet is also about more than merely accessing another computer's desktop or hard disc drives for file and print sharing. Intranets typically use a Web-styled browser, but also support other features such as FTP sites and e-mail for the sharing of information and communication with other users.

➢ **Protocols found with Intranet :**
Any of the well known Internet protocols may be found in an intranet, such as HTTP (web services), SMTP (e-mail), and FTP (file transfer protocol). Internet technologies are often deployed to provide modern interfaces to legacy information systems hosting corporate data.

➢ **Benefits :**
The main goal of an Intranet is to allow a company to share information among employees or partners, but it can also limit access to the outside world. Sometimes access to the Web is restricted so that workers don't spend a time surfing Web sites that have no relation to their work. For a small business, there are many benefits of an Intranet :

- Greater access for all employees, especially for a small or medium-sized business that must rely on the quick sharing of information between multiple offices or locations. This provides faster and easier access to more accurate company information.
- Ease of use for employees, because existing Web browsers can be used to navigate the Intranet. This reduces the need to install specialized programs in many cases, and further requires little additional training of applications.
- Ease of shared data, reducing the need for printouts or other hardcopies.
- Protection of sensitive material, as users log in to a closed network and data does not have to be sent out to users in different offices or those working remotely. Instead the data is access by the individual, thus limiting the chances that a person outside the company might access it.
- Updated information can be available to all users at the same time.

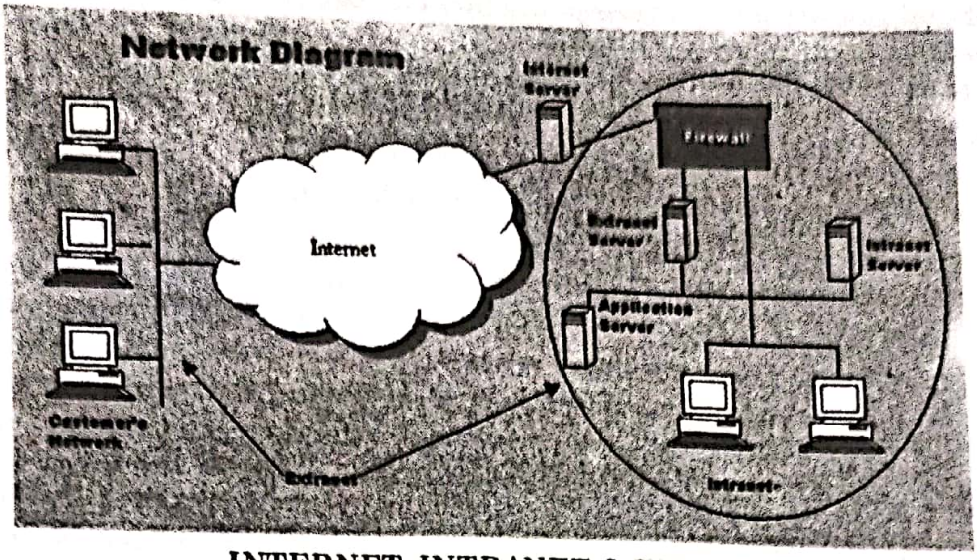
Typically, larger enterprises allow users within their intranet to access the public Internet through firewall servers that have the ability to screen messages in both directions so that company security is maintained. When part of an intranet is made accessible to customers, partners, suppliers, or others outside the company, that part becomes part of an extranet.

An "extranet" is a computer network that allows controlled access from the outside for specific business or educational purposes. Intranets and extranets are communication tools designed to enable easy information sharing within workgroups.

1.11 INTERNET, INTRANET & EXTRANET

➢ **Internet :**
The Internet is a global system of interconnected computer networks that use the standardized Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. The Internet carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

➢ **Intranet :**
An intranet is a private application of the same internetworking technology, software, and applications within a private network, for use within an enterprise. It may be entirely disconnected from the public Internet, but is usually linked to it and protected from unauthorized access by security firewall systems. More loosely, the term may include extranets, as well.



INTERNET, INTRANET & EXTRANET

The difference between an intranet and the Internet is defined in terms of accessibility, size and control. Unless content filters are being used or the government is censoring content, all the Internet's content is accessible to everyone. On the other hand an intranet is owned and controlled by a single organization that decides which members are allowed access to certain parts of the intranet. In general, an intranet is usually very small and is restricted to the premises of a single organization.

➢ **Extranet :**

An extranet is similar to an intranet but it is made accessible to selected external partners such as business partners, suppliers, key customers etc, for exchanging data and applications and sharing information.

As with an intranet, an extranet can also provide remote access to corporate systems for staff that spends lots of time out of the office, for instance those in sales or customer support, or home workers.

Extranet users should be a well-defined group and access must be protected by rigorous identification routines and security features.

Both intranets and extranets are owned, operated and controlled by one organization. However, the difference between intranets and extranets is defined in terms of who has access to the private network and the geographical reach of that network. Intranets allow only members of the organization to access the network, while an extranet allows persons from outside the organization (i.e. business partners and customers) to access the network. Usually, network access is managed through the administration of usernames and passwords, which are also used to determine which parts of the extranet a particular user can access.

1.12 WEB PORTALS

In 2008, Make a Difference Michiana is introducing a new initiative to help community groups connect to non-profits through customized websites called Portals.

Portals are built around the needs of a group of people--whether it be a business, a club, a church, a college dorm, a class, a neighborhood--to strengthen that group's relationship with its non-profit partners.

A web portal is a web site that brings together information from diverse sources in a unif way. Usually, each information source gets its dedicated area on the page for displayi information (a portlet); often, the user can configure which ones to display.

- *From www.wikipedia.o*

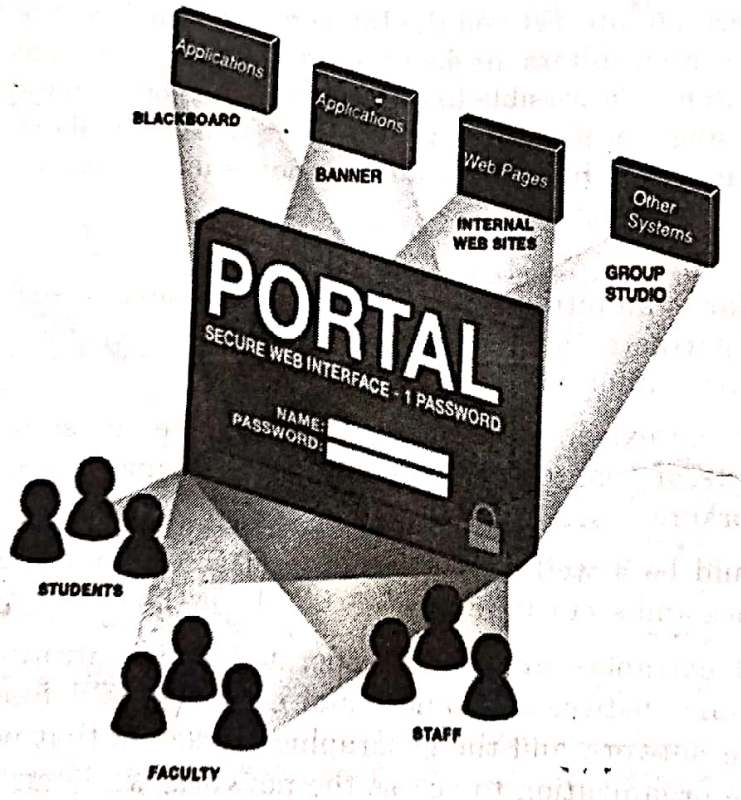
A *Web portal* or *public portal* refers to a Web site or service that offers a broad array resources and services, such as e-mail, forums, search engines, and online shopping malls.

- *From www.webopdia.co*

Web Portals are large multi-service web sites designed to be comprehensive one-st destinations for users. Portals are large, well-funded, and staffed by full-time employees.

- *From www.about.co*

A web portal is also known as a links page. It is similar to a standard search engine but al offers extra services such as email, horoscopes, and entertainment. Some popular portals a Yahoo, Excite, Lycos, Netscape, AltaVista, MSN, and AOL.com. There are also many small portals, known as "niche portals," for specific interests. These sites include C|net (f computers and technology), Fool.com (for investors), and Garden.com (for gardeners).



WEB PORTAL- MULTI-SERVICE WEB SITES

Most large portals have millions of Web pages indexed for visitors to search though. They als have large directories of Web sites, which are categorized by topic. Though the primary purpos of a portal is to find other sites for you, many now include a lot of information within their own sites.

[1] Basic Architecture of Portals :

Most of today's portal solutions meet the requirements of only single functionalities, thu providing a partial solution for particular problem areas. This is exactly were th theoretical distinction between horizontal and vertical portals becomes crucial.

➢ **Horizontal Portal :**
Horizontal portals target the entire Internet community. These sites, often referred to as "mega-portals", usually contain search engines and provide the ability for user to personalize the page by offering various channels (i.e. access to other information such as regional weather, stock quotes or news updates).

Yahoo! and Lycos constitute mega-portals. These portals are also gateways to contents and services of other offerors.

➢ **Vertical Portal :**
According to Gartner Group, vertical portals differ only in their more specific objects and contents from horizontal portals, the technology employed remains the same.

Most of the times, vertical portals offer information and services customized to niche audiences about a particular area of interest. Vertical industry portals, known as vortals, are sites that provide a gateway to information related to a particular industry, such as, insurance, automobiles, etc.

➢ **Types of web portals :**
www.portalsindia.com/ is the site which gives you all types of Indian web portal information.

- Personal portals
- News and Media portals
- Government web portals
- Cultural portals
- Enterprise / Corporate web portals:
- Stock portals
- Search portals
- Tender's portals
- Hosted web portals
- Domain-specific portals
- Educational Institute portals

➢ **Web Portal V/s Web Site :**
A web site is a page in the internet which provides to access to data and information.

A Web Portal is a subset of the website, which acts as a way or path to enter a particular domain you would like to enter. Just see the meaning of the word "Portal". It means "door" or "gateway" or "Entrance".

A Web portal is nothing special. Its is just a website, but is used as a entry point. For example, you can create your own page and name your home page as your web portal.

A portal is generally considered as a launching pad to other sites, Yahoo! and Google are considered "portals" where as something like www.foxnews.com/ or www.cnn.com/ or of your personal website somewhere or a company website are just that websites.

A portal is generally a vehicle by which to gain access to a multitude of 'services'. A web site is a destination in itself. As such the term website refers to a location on the Internet (see this) that is unique and can be accessed through a URL (see this). By that definition a web portal is in fact also a website.

However there is a distinction between the two terms based on the subject and co of the website.

A website is also a web portal if; It transmits information from several indepe sources that can be, but not necessarily are, connected in subject; thus offering a p service function for the visitor which is not restricted to presenting the view(s) o author.

[2] Typical Portal Attributes :

- Web portal is a Public & Private Interface (extranet, intranet, etc...)
- Offers Access for Multiple User Roles
- Personalization / Role specific functionality & content
- Endowed with Versatile / Enhanced functionality & flexibility
- The user can access to broad resources
- Supports the user in multiple task
- Offers content from diverse resources
- Spans content, collaboration and eCommerce
- Extensive & unfocused content can be created to accommodate unidentified users ne
- Searchable but not customizable, the content are created for every user.

[3] Typical Website Attributes :

- It's a Public Interface
- Supports the user in specific task (marketing or ecommerce)
- Provides targeted content from independent resources to specific audience
- Content is generally focused, eliminates the need of visiting different sites
- Select & organize the materials needed to be accessed
- Establish your presence in online global market
- Reach the targeted audience

1.13 DOMAIN NAME SERVER (DNS)

The Domain Name Server (DNS) is a hierarchical distributed naming system for computa services, or any resource connected to the Internet or a private network.

Short for *Domain Name System* (or *Service* or *Server*), an Internet service that transla *domain names* into IP addresses.

It is a standard technology for managing the names of Web sites and other Internet domains

The domain name system (DNS) is the way that Internet domain names are located a translated into Internet Protocol addresses. A domain name is a meaningful and easy- remember "handle" for an Internet address. Without DNS, we would have to remember the address of every site we wanted to visit, instead of just the domain name. Can you imag having to remember "17.254.3.183" instead of just "apple.com"? While I have some Comput Science friends who might prefer this, most people have an easier time remembering simp names.

The reason the Domain Name System is used is because Web sites are actually located by th IP addresses. For example, when you type in "http://www.adobe.com," the computer does

immediately know that it should look for Adobe's Web site. Instead, it sends a request to the nearest DNS server, which finds the correct IP address for "adobe.com." Your computer then attempts to connect to the server with that IP number. DNS is just another one of the many features of the Internet that we take for granted.

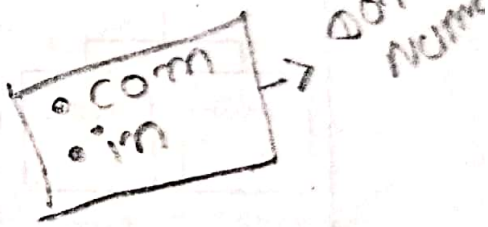
Fully qualified domain names (FQDNs) :

When using the Domain Name System, it is common to work with only a part of the domain hierarchy, such as the myDivision.myCorp.com domain. The Domain Name System provides a simple method of minimizing the typing necessary in this circumstance. If a domain name ends in a dot (for example, myDept.myDiv.myCorp.com), it is assumed to be complete. This is called a *fully qualified domain name (FQDN)* or an *absolute domain name*. However, if it does not end in a dot (for example, myDept.myDiv), it is incomplete and the DNS resolver may complete this by appending a suffix such as .myCorp.com to the domain name. The rules for doing this are implementation-dependent and locally configurable.

Generic domains :

The top-level names are called the generic top-level domains, and can be three characters or more in length. Below Table shows some of the top-level domains of today's Internet domain namespace.

Domain Name	Meaning
aero	The air transport industry
biz	Business use
cat	The Catalan culture
com	Commercial organizations
coop	Co-operatives
edu	Educational organizations
gov	Government agencies
info	Informative
int	International organizations
jobs	Employment related
mil	Military agencies
mobi	Mobile devices related
museum	Museum related



- **DNS- Generic Domains**

  These names are registered with and maintained by the Internet Corporation for Assigned Names and Numbers (ICANN). For current information, see the ICANN Web site at: http://www.icann.org

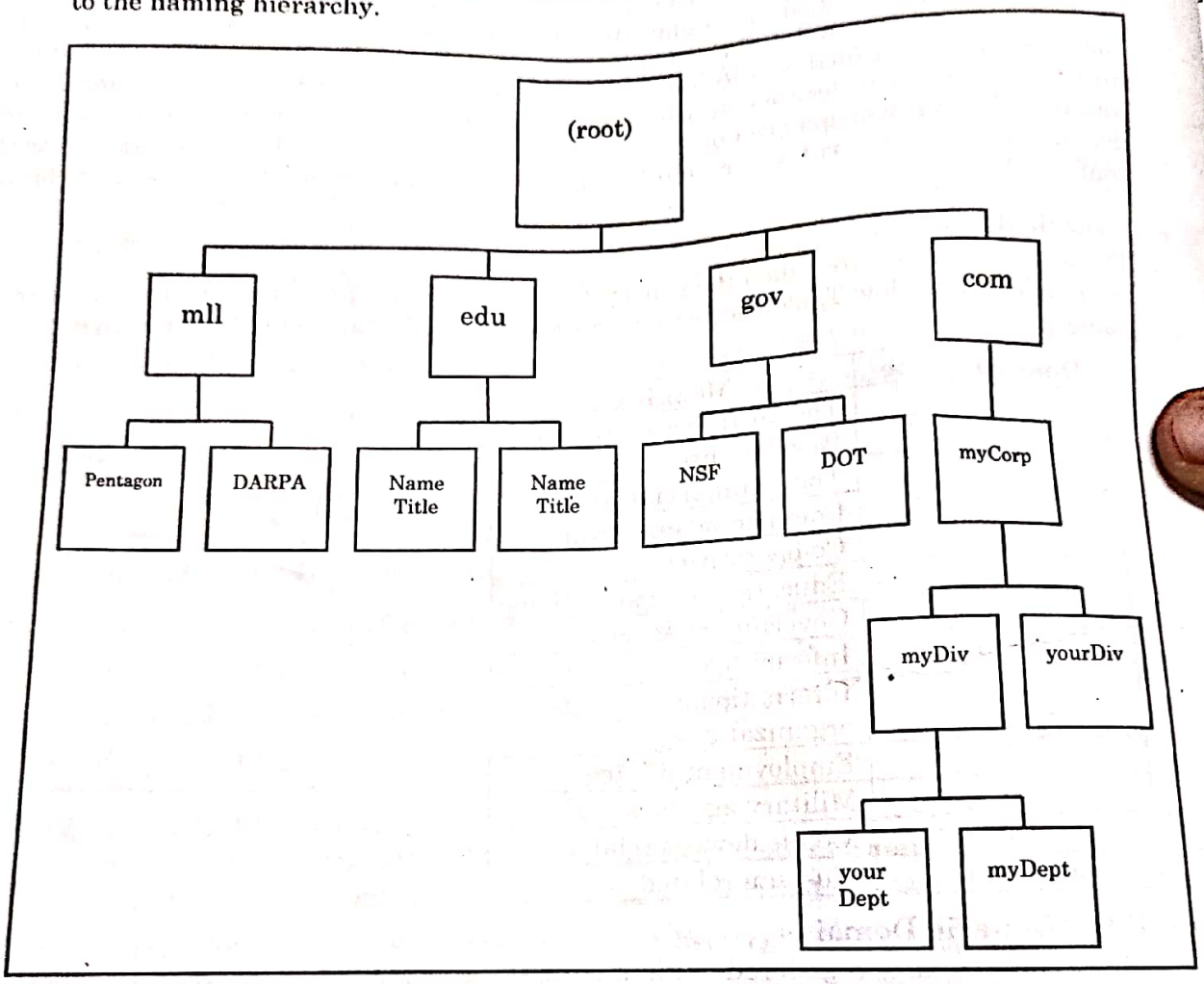
- **Country domains:**

  There are also top-level domains named for the each of the ISO 3166 international 2-character country codes (from *ae* for the United Arab Emirates to *zw* for Zimbabwe and *in* for India). These are called the *country* domains or the *geographical* domains. Many countries have their own second-level domains underneath which parallel the generic top-level domains. For example, in the United Kingdom, the domains equivalent to the generic domains *.com* and *.edu* are *.co.uk* and *.ac.uk* (ac is an abbreviation for academic). There is a .us top-level domain, which is organized geographically by state (for example, .ny.us refers to the state of New York).

➢ **Mapping domain names to IP addresses**

The mapping of names to addresses consists of independent, cooperative systems called name servers. A name server is a server program that holds a master or a copy of a name-to-address mapping database, or otherwise points to a server that does, and that answers requests from the client software, called a name resolver.

Conceptually, all Internet domain servers are arranged in a tree structure that corresponds to the naming hierarchy.



- **DNS- Naming hierarchy :**

Each leaf represents a name server that handles names for a single sub-domain. Links in the conceptual tree do not indicate physical connections. Instead, they show which other name server a given server can contact.