DATA COMMUNICATION
AND
COMPUTER NETWORKS

Written by
Dr.P.Premchand
Dept. of CSE, College of Engineering,
Osmania University, Hyd 500007

Edited by
K.Goverdhan Naidu
Jr.Lecturer, PCR Govt. Junior College,
Chittor

Dedicated to the fond memories of

Late Prof. S.V.L.N Rao garu,

my guruji, retired Professor IIT Kharagpur

who

taught me the courage in leading the academic life.

and

Late Prof. K.N.Raju garu,

Professor, A.U. College of Engg.Vishakhapatnam,
who taught me the technique in leading the worldly life.

This book, DATA COMMUNICATIONS AND COMPUTER NETWORKING attempts to provide an overview of the broad field of subject in a simple and lucid manner. The subject has been divided into 6 units, each unit targeted to cover basic principles and topics of fundamental importance. This book gives a clear insight to the reader regarding various aspects of the subject. In a competitive world like this, understanding these technologies is very essential.

The summary of the book is as follows:-

UNIT 1 Data communications: Covers the different types of communications which have evolved during the course of the time and techniques used to transmit the data.

Unit 2 Network Topology: Covers the different types of networks and the various types of network topologies.

Unit 3 LAN Components: This unit emphasizes on the LAN components like LAN Card, LAN cables, Hubs/switches etc in detail.

Unit 4 Communication Hardware: This unit gives an account of the various communication hardware existing today

Unit 5 Network environment This unit stresses on understanding UNIX and WIN NT operating system.

Unit 6 Network and Web applications: This unit covers network and Web Applications like email, FTP, TELNET etc in detail.

I would like to thank Mr. ***D. Kirthi Kumar*** *without whose co-operation this book would not have taken this form.*

Contents

1. Data Communications

2. Network Topologies

3. LAN Components

4. Communication Hardware

5. Network Environment

6. Network and Web Applications

1. Data Communications

Communication is defined as transfer of information, such as thoughts and messages between two entities. The invention of telegraph, radio, telephone, and television made possible instantaneous communication over long distances.

In the context of computers and information technology (IT), the data are represented by **bi**nary digi**t** or **bit** has only two values 0s and 1s. In fact any thing the computer deals with are 0s and 1s only. Due to this it is called discrete or digital. In the digital world messages, thoughts, numbers.. etc can be represented in different streams of 0s and 1s.

Data communications concerns itself with the transmission (sending and receiving) of information between two locations by means of electrical signals. The two types of electrical signals are analog and digital. Data communication is the name given to the communication where exchange of information takes place in the form of 0s and 1s over some kind of media such as wire or wireless. The subject-Data Communications deals with the technology, tools, products and equipment to make this happen.

Entire data communication system revolves around three fundamental concepts.

- **Destiny:** The system should transmit the message to the correct intended destination. The destination can be another user or another computer.
- **Reliability:** The system should deliver the data to the destiny faithfully. Any unwanted signals (noise) added along with the original data may play havoc!
- **Fast:** The system should transmit the data as fast as possible within the technological constraints. In case of audio and video data they must be received in the same order as they are produced without adding any significant delays.

1.1 Data Communication model

The figure 1.1(a) shows the block diagram of a typical communication model. The communication model has five sub systems viz., user, transmitter, communication channel, receiver and destiny.

- **User:** There will be a source that generates the message and a transducer that converts the message into an electrical signal. The source can be a person in front of a microphone or a computer itself sending a file. The user terminal is known as data terminal equipment (DTE).
- **Transmitter:** Can be a radio frequency modulator combining the signal coming out of the data equipment terminal. Here the radio frequency is acting as the carrier for the data signal. Or in case of direct digital transmission the transmitter can be Manchester encoder transmitting digital signals directly.

- **Communication channel: C**an be **guided media** (twisted pair, coaxial cable, fiber optic.,) or **unguided media** (air, water .,). In both the cases communication is in the form of electro magnetic waves. With guided media the electro magnetic waves are guided along a physical path. **Unguided media** also called wireless the transmitting electro magnetic waves are not guided along with a physical path. They are radiated through air/vacuum/water., etc.

- **Receiver:** The receiver amplifies the received signals removes any unwanted signals (noise) introduced by the communication channel during propagation of the signal and feeds to the destiny.
- **Destiny:** The user at the other end finally receives the message through the data terminal equipment stationed at the other side.

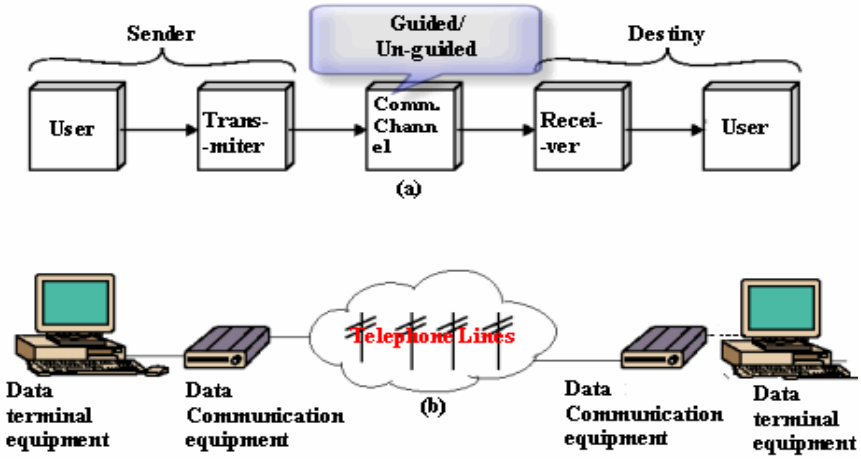


Fig 1.1 (a) The block diagram of a data communication model
(b) A typical dial-up network

Fig 1.1 (b) shows a typical dial-up network setup. The data communication equipment (DCE) at the transmitting end converts the digital signals into audio tones (modulation) so that the voice grade telephone lines can be used as guided media during transmission. At the far end the receiving audio tones, they are converted back to digital signals (Demodulation) by the data communication equipment (DCE) and fed to the far end data terminal equipment (DTE).

1.2 Signal conversions

There are two types of signals analog and digital. All naturally available signals are analog in nature. In data communications these signals are converted into digital form by means of A-to-D converters
(analog to digital converters).

The following figure illustrates the analog output of microphone and subsequent conversion into its digital counter part by A-to-D converter.

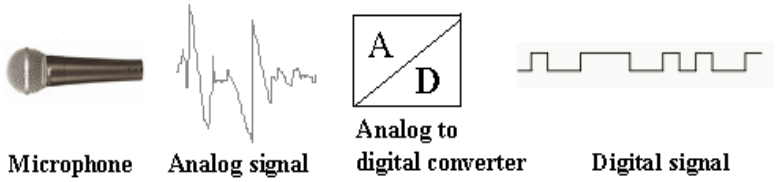


Fig 1.2.1 Example of analog and digital signal

1.3 Analog signal.

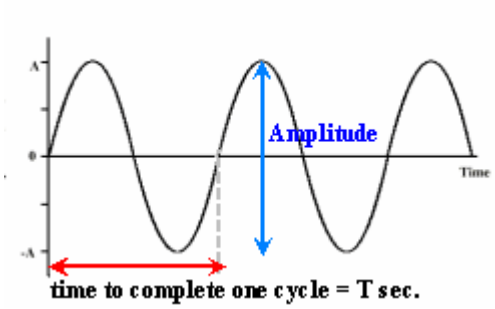


Fig 1.3.1 A simple sine wave and its parameters.

The sine wave is the simplest form of an analog signal. It has three parameters. Amplitude, frequency and phase. Normally amplitude in volts is denoted on Y-axis and time period is on X-axis. The time taken

to complete one cycle is called time period and measured in seconds. The reciprocal of time period is frequency and its unit is cycles per second(c/s) or Hz (Hertz).(See Fig.1.2)

1.4 Wave forms of different parameters

The following figures show the signals with different parameters and their inter-relationship

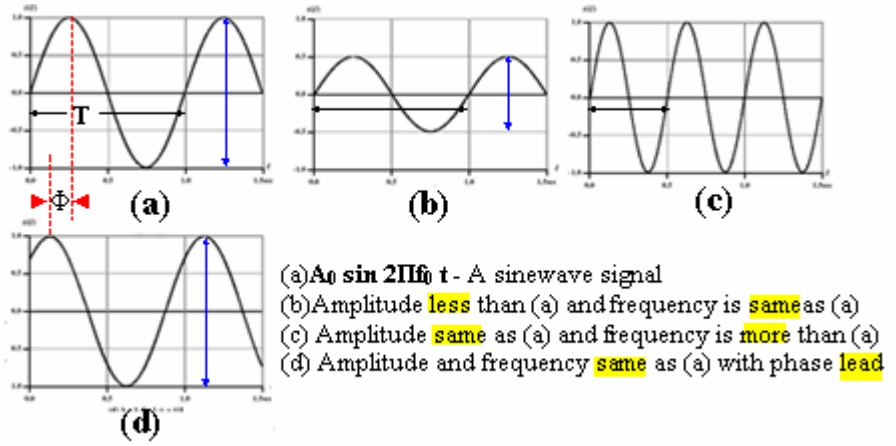


Fig 1.4.1 Different wave forms with different parameters

1.5 Bandwidth

Mathematically it can be shown that any complex waveform is a made of sine waveforms of different amplitudes and frequencies with varying phase relationships amongst each other.

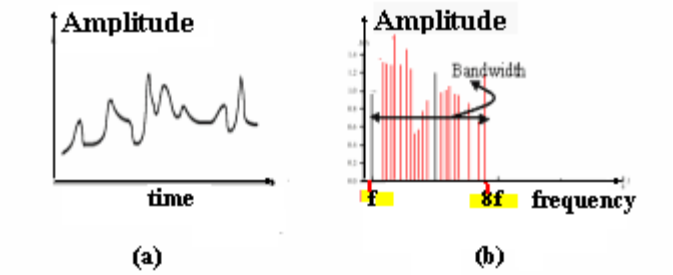


Fig 1.5.1 (a) An analog signal(b) Its various frequency components.

In the above figure the analog signal in fig 1.4(a) has several frequency components of different amplitude as shown in fig 1.4(b). Thus the analog signal encompasses a wide range of frequency spectrum. In

analog systems the difference between highest frequency to lowest frequency component is called bandwidth (here it is 8f~f = 7f).

Bandwidth merely specifies a range of frequencies, from the lowest to the highest, that the channel can carry or that are present in the signal. It is one way of describing the maximum amount of information that the channel can carry. Bandwidth is expressed differently for analog and digital circuits. In analog technology, the bandwidth of a circuit is the difference between the lowest and highest frequencies that can pass through the channel. Engineers measure analog bandwidth in kilohertz or megahertz.

Rate of transmission = (bits per second)

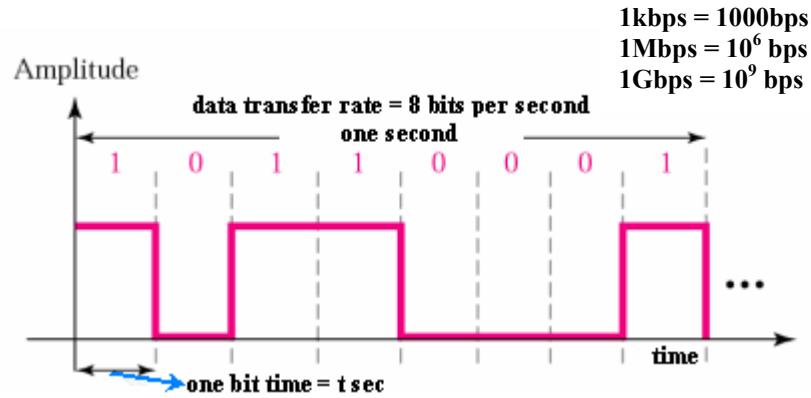


Fig 1.5.2 Relation between bit time and rate

In data communication, the bandwidth is the amount of information that can pass through the channel or medium. Engineers measure digital bandwidth in bits, kilobits, or megabits per second. The kilohertz of an analog bandwidth and the kilobits per second of digital bandwidth for the same circuit are not necessarily the same and often differ greatly.

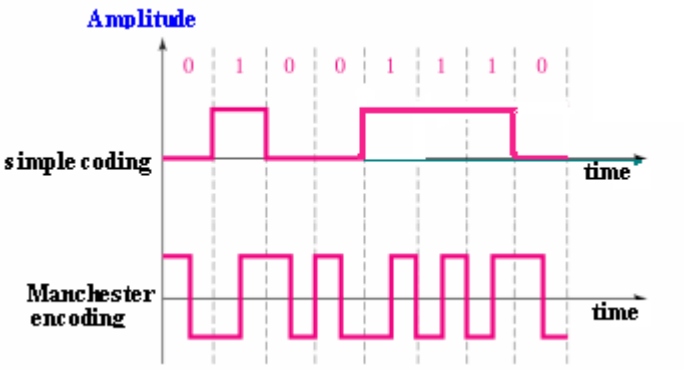


Fig 1.5.3 Manchester encoding

In principle digital signals require a large bandwidth (theoretically infinite!). The medium has to be of better quality to send digital signals. Most LANs use Manchester encoding because of its self-synchronizing property. Otherwise separate clock signals were to be transmitted along with data in order to inform about sender's transmission clock. In Manchester encoding there is a transition in each bit interval and this property serves as clock also.

1.6 Noise

In any type of communication, noise is the biggest impairment. The received signal at the receiver end will consist of transmitted message plus additional unwanted signal that are inserted somewhere between transmitter and receiver distorting the message.

There are several types of noise sources, which can abruptly affect the quality of reception signal. The following are some of them

- **Thermal noise:** Due to thermal agitation of electrons. Present in all electronic devices and is the function of temperature.

- **Impulse noise:** Due to electromagnetic interference (EMI). They may be present in power lines, or in nature (lightning.. etc)
- **Delay distortion:** Due to non-uniform velocities of signals of different frequencies traveling in a guided media. Various frequencies of a message signal will arrive at different delays resulting in distortion.

1.7 Channel capacity

The maximum rate at which data can be transmitted over a communication channel under given conditions is referred as the channel capacity.

There are four parameters involved in the evaluation of channel capacity.

- **Data rate:** The rate at which data can be transmitted. Measured in bits per second
- **Bandwidth:** The bandwidth of the transmitted signal. Measured in cycles per second (Hz).

- **Noise:** The average level of unwanted signals over communication path. Expressed as the ratio between signal and noise.
- **Error rate:** The rate at which error can occur.

Then the channel capacity (in cycles per second) according to **Shannon's** theorem is given by

$$\mathbf{C = B \log_2 (1+SNR)}$$

Where

- **C** in Cycles per second and this is error free capacity
- **B** is the bandwidth in Hertz.
- **SNR** = $10 \log_{10}$ (Signal power/Noise power)

Normally this theorem represents maximum channel capacity. Actual values maybe much less than as given by the formula. One reason for this is the SNR ratio. The SNR ratio assumes only white noise (thermal noise) where as other noise like impulse noise, attenuation noise and delay noise are not taken into account.

1.8 Types of communication

Based on the requirements, the communications can be of different types:

- **Point- to-point communication:** In this type, communication takes place between two end points. For instance, in the case of voice communication using telephones, there is one calling party and one called party. Hence the communication is point-to-point.

- **Point-to-multipoint communication:** In this type of communication, there is one sender and multiple recipients. For example, in voice conferencing, one person will be talking but many others can listen. The message from the sender has to be *multicast* to many others.

- **Broadcasting:** In a broadcasting system, there is a central location from which information is sent to many recipients, as in the case of audio or video broadcasting. In a broadcasting system, the listeners are passive, and there is no reverse communication path.

- **Simplex communication:** In simplex communication, communication is possible only in one direction. There is one sender and one receiver; the sender and receiver cannot change roles.

- **Half-duplex communication:** Half-duplex communication is possible in both directions between two entities (computers or persons), but one at a time. A walkie-talkie uses this approach. The person who wants to talk presses a talk button on his handset to start talking, and the other person's handset will be in receive mode. When the sender finishes, he terminates it with an over message. The other person can press the talk button and start talking. These types of systems require limited channel bandwidth, so they are low cost systems.

- **Full-duplex communication:** In a full-duplex communication system, the two parties the caller and the called can communicate simultaneously, as in a telephone system. However, note that the communication system allows simultaneous transmission of data, but when two persons talk simultaneously, there is no effective communication! The ability of the communication system to transport data in both directions defines the system as full duplex.

Depending on the type of information transmitted, we have voice communication, data communication, fax communication, and video communication systems. When various types of information are clubbed together, we talk of multimedia communications. Even a few years ago, different information media such as voice, data, video, etc. were transmitted separately by using their own respective methods of transmission. With the advent of digital communication and "convergence technologies," this distinction is slowly disappearing, and multimedia communication is becoming the order of the day.

1.9 Modes of transmission

When we talk of data communication we are primarily concerned with serial transmission although other types of transmission does exists. In serial transmission the data is transmitted bit by bit as a stream of 0s and 1s. Protocols are implemented for these types of transmissions so that the communication takes place in a well-defined manner. Protocols are mutually agreed set of rules and are necessary because the format of transmission should be understood by the receiver

The following key factors have to be observed regarding serial transmission:

- **Timing problem:** There should be some mechanism to know when the bit has arrived and at what rate the next bit is going to arrive at the serial input terminal of the receiver. We will see this can be accomplished in two ways.
- **Error detection:** Provision should be made (during transmission itself) to verify the integrity of the received data. Like parity, checksum bits.
- **Error correction:** Ability to correct the data in case of corrupted data reception.

Timing problems require a mechanism to synchronize the transmitter and receiver. There are two approaches regarding transmission of serial data.

- **Asynchronous transmission**
- **Synchronous transmission**

1.9.1 Asynchronous transmission

In asynchronous transmission data is transferred character by character and each character (frame by frame i.e. each character is an asynchronous frame in asynchronous transmission) and can be 5 to 8 bits long. The term “Asynchronous” means it is asynchronous at frame level. The bits are still synchronized at bit level during reception.

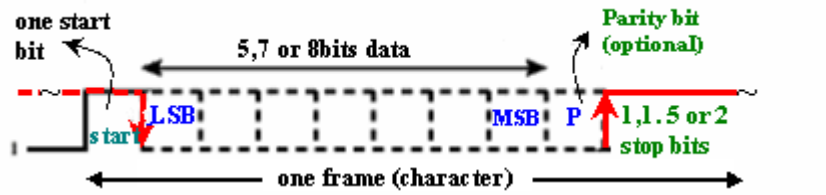


Fig 1.9.1 Asynchronous data format

- In a steady stream, interval between characters is uniform (length of stop element can be 1,1.5 or 2 stop bits - as programmed earlier)
- In idle state, receiver looks for transition 1 to 0 (start signal)
- Then samples next five, seven or eight intervals (as programmed earlier) Timing only needs maintaining within each frame (bit level).
- Looks for parity (if programmed earlier)
- Then looks for next 1 to 0 for next frame
- Simple
- Cheap. Minimum hardware & software requirement to impliment.
- Overhead of 2 or 3 bits per frame (~20%)
- Good for data with large gaps in between each frame (keyboard, low speed data..)

1.9.2 Synchronous transmission

In Synchronous transmission a block of data in the form of bits stream is transferred without start / stop bits. The block can be of any arbitrary length. In order to establish synchronization with remote computer the transmitter transmits synch pulses initially. When the receiver locks to the transmitter's clock frequency a block of data gets transmitted. See fig.1.9.2

The Characteristics are as follows

- Block of data transmitted without start or stop bits
- Initially synch pulses are transmitted (Clocks must be synchronized)

- Can use separate clock line (In that case synch pulses are not needed!)
- Good over short distances
- Subject to impairments
- Embed clock signal in data (Manchester encoding)
- Carrier frequency (analog) is used
- Need to indicate start and end of block
- Use preamble and post amble (to leave sufficient space between blocks)
- More efficient (lower overhead) than asynchronous transmission.

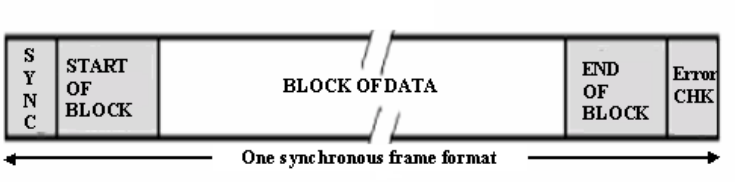


Fig 1.9.2 The synchronous frame format

1.10 Multiplexing

By **Multiplexing** different message signals can share a single transmission media (The media can be guided or unguided). All they need is they should either differ in their frequency slot or wavelength slot or in time slot.

1.10.1 Frequency domain multiplexing (FDM)

In this each message signal is modulated by different radio frequency signals called rf carriers. At the receiving end filters are used to separate the individual message signals. Then they are demodulated (removing the rf carrier) to retrieve back the original messages.

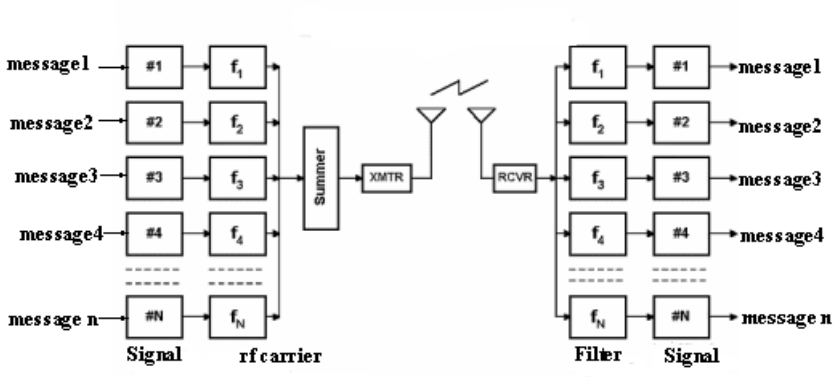


Fig 1.10.1 Frequency domain multiplexing

The Radio /TV broadcasting are the best examples for frequency domain multiplexing. Several individual stations broadcast their programs in their own allotted frequency band sharing the same unguided media. The receiver tunes his set according to his choice. The cable TV network is another example of Frequency domain multiplexing employing guided media.

1.10.2 Wavelength division multiplexing (WDM)

Wavelength division multiplexing is a type of FDM scheme used in fiber optical communications where various wavelengths of infrared light are combined over strands of fiber.

Optical communication with few exceptions are digital since light transmitters and receivers are usually poorly suited for analog modulation.

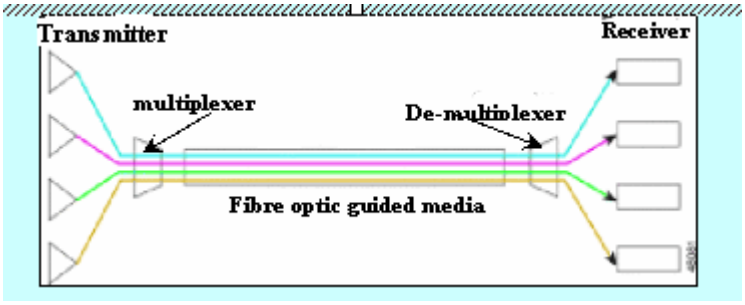


Fig 1.10.2 A Typical wavelength division multiplexer

1.10.3 Time domain multiplexing (TDM)

A type of multiplexing where two or more channels of information are transmitted over the same media by allocating a different time interval ("slot" or "slice") for the transmission of each channel. The channels take turns to use the media. Some kind of periodic synchronizing signal or distinguishing identifier is usually required so that the receiver can tell which channel is which.

A typical practical setup combines a set of low-bit-rate streams, each with a fixed and pre-defined bit rate, into a single high-speed bit stream that can be transmitted over a single channel.

The main reason to use TDM is to take advantage of existing transmission lines. It would be very expensive if each low-bit-rate stream were assigned a costly physical channel (say, an entire fiber optic line) that extended over a long distance.

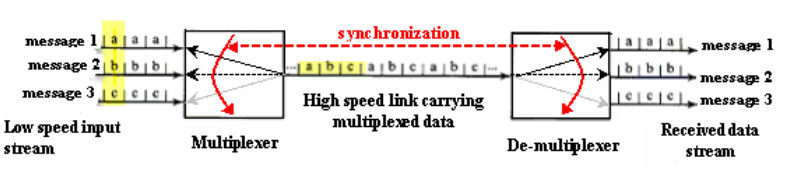


Fig. 1.10.3 Time division multiplexing.

1.11 Network Models

When people to people, machines to machines started communicating with each other the networking technology started picking up. Different vendors started manufacturing their proprietary configurations. In order to communicate systems with heterogeneous configurations there was a need for standardization. TCP/IP(Transmission Control Protocol / Internet Protocol) is the oldest one and has become defacto standard for all networks. OSI model is much more refined and let us hope all future models will be based on this.

Especially in data communications the way data traverses from the user to the destiny is a complex task that can be broken into several sub tasks, built one over the other like layers. Each layer takes input from the upper layer, performs its duty and hands over to the lower layer. Several

models were suggested out of which the Internet model is widely accepted. Later OSI (open systems interconnection) was developed as a theoretical model. Studying OSI model gives better perception of the various intricacies involved in data communication and networking.

1.11.1 The OSI Model

It has seven layers. They are separate but related. Each layer has well defined tasks and provides services to the corresponding lower layer while in transmission. In receiving mode the lower layer provides the necessary services to the upper layer. Any changes in one layer should not require changes in other layers.

This kind of standardization allows communication across all types of computers.

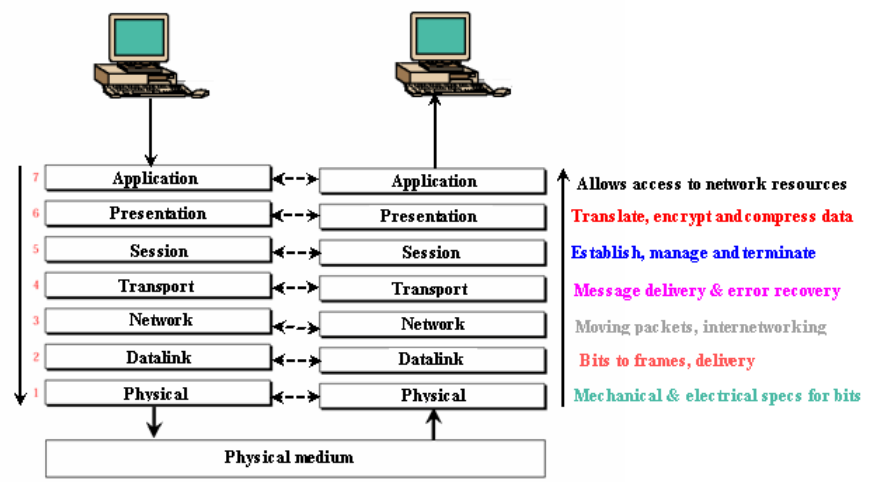


Fig 1.11.1 The OSI Layers and their functions

Easy to remember these layers!……
Please **D**o **N**ot **T**ouch **S**hiva's **P**et **A**lligator

The Seven Layers of OSI and their conceptual services -

- **Application - (layer 7)** Allows applications to use the network. The user may want to access the network for various purposes. Like for sending e-mail, transferring a file, surfing the web, accessing remote computer's resources etc.. For every task mentioned above there is a dedicated service.

Services **–** e-mail, news groups, web applications, file transfer, remote host, directory services, network management, file services

- **Presentation - (layer 6)** Translates data into a form usable by the application layer. The redirector operates here. Responsible for protocol conversion, translating and encrypting data, and managing data compression. messages are sent between layers
  Services – POP, SMTP (e-mail, Post office protocol, Simple Mail Transfer Protocol), Usenet (for news groups), HTTP (hyper text transfer protocol for web applications), FTP, TFTP (File transfer protocol, trivial FTP for file transfer), Telnet (Terminal Network, A general purpose program enabling remote login into some other computer and function as if it is directly connected to that remote computer), Domain name server (finding ip addresses for domain names), SNMP (Simple Network Management Protocol).

- **Session - (layer 5)** Allows applications on connecting systems to standard ports & establish a session. Provides synchronization between communicating computers. Messages are sent between layers

  Services **–** Various port numbers are POP(25), USENET(532), HTTP(80), FTP(20/21), Telnet(23), DNS(53), SNMP(161/162) etc..

- **Transport - (layer 4)** Responsible for packet handling. Ensures error-free delivery. Repackages messages (while receiving), divides messages into smaller packets (while transmitting), and handles error handling. segments of message fragments are sent between layers

  Services **-** TCP - connection-oriented communication for applications to ensure error free delivery;
  UDP - connectionless communications and does not guarantee packet delivery between transfer points

- **Network - (layer 3)** Translates system names into addresses. Responsible for addressing, determining routes for sending,

managing network traffic problems, packet switching, routing, data congestion, and reassembling data. Datagrams are sent between layers.

Services **-** Software & hardware addresses and packet routing between hosts and networks (IP). Two versions IP4(32 bits) & IP6(128 bits)

- **Data link - (layer 2)** Sends data from network layer to physical layer. Manages physical layer communications between connecting systems. Data frames are sent between layers

  Services **–** SLIP/PPP, 802.2 SNAP, Ethernet

- **Physical - (layer 1)** Transmits data over a physical medium. Defines cables, cards, and physical aspects. Data bits are sent.

  Services **-** ISDN, ADSL, ATM, FDDI, CAT 1-5, Coaxial cable

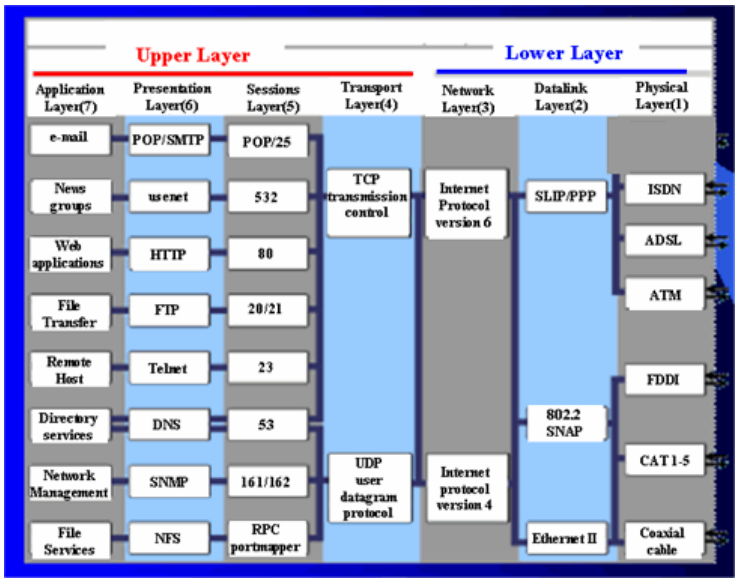


Fig 1.11.2 The OSI Model an their example services

1.11.2 The Internet model

There are four layers in this model. They are I) Application Layer II) Transport Layer III) Network Layer IV) Data Link & Physical Layer.

- **Application Layer:** Most of the responsibilities of the three top most layers of OSI model are in application layer of Internet model. The services are as depicted in the fig.
- **Transport Layer:** It has two protocols. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP is a reliable protocol that allows two application layers to converse with each other. While transmitting it divides the stream of characters into manageable segments. While receiving it creates stream of characters for application layer from received segments from network layer. Its function is much more than as depicted in OSI model. Some of the responsibilities of OSI's session layer are dissolved into Internet model's transport layer.
  The other protocol UDP is a simpler protocol. It ignores some of the duties of the transport layer defined in OSI model. It is used when fast delivery of packets is needed without worrying much about error control.
- **Network Layer:** The main protocol is IP (Internet Protocol) is responsible for creating network layer packets called IP datagrams. The datagrams travel network to network or LAN to WAN and the packets may reach out of sequence. It is the responsibility of upper layers to put them into proper order.
- **Datalink & physical Layer:** The Internet model does not discuss much about these layers making this protocol machine independent to a large extent. It is left to the user to choose the proper standard or protocol according to what they desire.

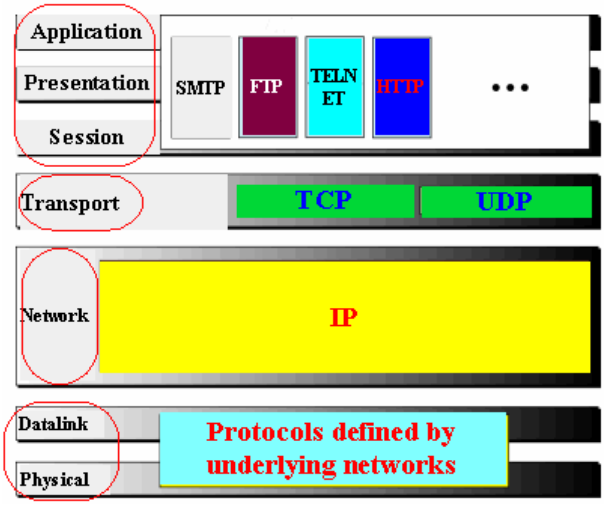


Fig 1.14 The Internet model

Summary:

Data communications concerns itself with the transmission (sending and receiving) of information between two locations by means of electrical signals. The media can be guided (physical) wires or unguided (radio links). The two types of electrical signals are analog and digital.

Analogue signals have three main characteristics which define them, being amplitude, frequency and phase. Speech is an example of an analogue signal.

In data communications the channel bandwidth is represented in bits/sec and Shannon's theorem imposes a bandwidth restriction for low noise transmission.

Many aspects of data transmission are covered in this unit. There are six types of communication point-point, point-multipoint, broadcast, simplex, half duplex and full duplex.
Two modes of transmission are synchronous and asynchronous. Protocols (mutually agreed set of rules) are necessary to implement this type of serial communication system.

Several digital signals can be transmitted simultaneously over guided/unguided media using three basic techniques time domain multiplexing, frequency domain multiplexing and wavelength division multiplexing.

When people to people, machines to machines started communicating with each other- the networking technology started picking up. Different vendors started manufacturing their proprietary configurations. In order to communicate systems with heterogeneous configurations there was a need for standardization. TCP/IP is the oldest standard and has become defacto standard for all networks. OSI model is much more refined and let us hope all future models will be based on this.

Short questions:

1). The three parameters associated with analog signal are:
2). Furnish an example for guided media:
3). According to Shannon's if bandwidth increases noise…….
4). The example for simplex transmission…….
5). State an example for half-duplex transmission

6). Thermal noise is due to ……..
7). On telephone lines digital signals are transmitted as ……..
8). State the practical use of a multiplexer
9). What are the seven layers of OSI
10). State the services in sessions layer

Long questions:

1). Define data communication. How it is different from other types of communication?
2). Draw the block diagram of typical data communication model and explain its constituents.
3). Explain the term- bandwidth. How analog bandwidth is different from data communication bandwidth
4). Enumerate different types of communication. Site examples for each of them?
5). What is noise? How many types of noise are there?
6). Discuss in detail about multiplexing.
7). What are the factors involved in serial transmission?
8). Why Protocols are needed?
9). Explain TCP/IP model
10). Narrate the seven layers of OSI model

2. Network Topologies

A network is a set of equipments (often referred as data terminal equipment / DTE, or simply terminals or nodes ..) connected by a communication channel, which can be either guided/unguided media. DTE equipment can be a computer, printer or any device capable of sending and/or receiving data generated by other nodes on the network.

2.1 Why networking?

- **Sharing of hardware**
  Computer hardware resources
  Disks
  Printers..
- **Sharing of software**
  Multiple single user licenses are more expensive than multi-user license.
  Easy maintenance of software

- **Sharing of information**
  Several individuals can interact with each other
  Working in groups can be formed

- **Communication**
  e-mail
  internet telephony
  audio conferencing
  video conferencing

- **Scalability**
  Individual subsystems can be created and combine it into a main system to enhance the overall performance.

- **Distributed systems**
  In a networked environment computers can distribute the work load among themselves keeping transparency to the end user

2.2 Types of networks

2.2.1 Point to point

Figure 2.1.1 shows a communication system used to interconnect two computers. The computers output electrical signals directly through the serial port. The data can be passed directly through the communication medium to the other computer if the distance is small (less than 100 meters).

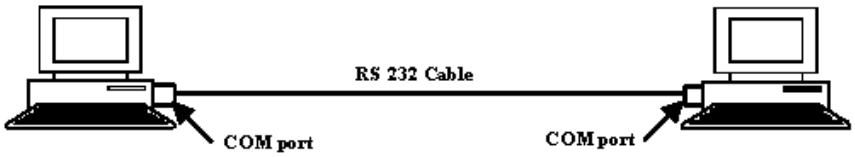


Fig.2.2.1 PC to PC communication using com ports

Figure 2.1.2 shows a communication system in which two PCs communicate
with each other over a existing say local telephone exchange (PABX) network. In this system, we introduced device called DTE data terminal equipment. The example here for DTE is modem (modulator-demodulator) connected at both ends. The PCs send digital signals, which the modem converts into analog signals and transmits through the medium (copper wires). At the receiving end, the modem converts the incoming analog signal into digital form and passes it on to the PC.

Fig.2.2.2 PC to PC communication over existing telephone network

2.3 Local Area Network (LAN)

A LAN is a local area network that is a small collection of computers in a small geographic area of less than couple of kilometers and is very fast in data transfer. Depending on technology implementation a LAN can be as simple as two PCs and a printer got connected in a small office or it can extend through out an organization and include multimedia (text, voice, video) data transfers.

The LANs may be configured in many ways. The peer-to-peer configuration is the simplest form. In this configuration computers are connected together to share their recourses among themselves. In such configurations it is very difficult impose security features.

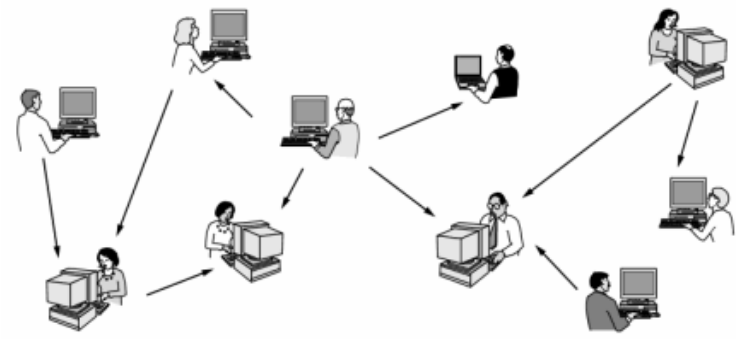


Fig 2.3.1 In a peer-to-peer configuration there is no security

On the other hand LANs can also be architectured in a client server model with full control over security and protection. Today Ethernet is a dominant LAN technology.

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Although the client/server idea can be used by programs within a single computer, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client/server model are very common. For example, to check your bank account from your computer, a client program in your computer forwards your request to a server program at the bank. That program may in turn forward the request to its own client program that sends a request to a database server at another bank computer to retrieve your

account balance. The balance is returned back to the bank data client, which in turn serves it back to the client in your personal computer, which displays the information for you.

The client/server model has become one of the central ideas of network computing. Most business applications being written today use the client/server model. So does the Internet's main program, TCP/IP. In marketing, the term has been used to distinguish distributed computing by smaller dispersed computers from the "monolithic" centralized computing of mainframe computers. But this distinction has largely disappeared as mainframes and their applications have also turned to the client/server model and become part of network computing.

In the usual client/server model, one server, sometimes called a daemon, is activated and awaits client requests. Typically, multiple client programs share the services of a common server program. Both client programs and server programs are often part of a larger program or application. Relative to the Internet, your Web browser is a client program that requests services (the sending of Web pages or files) from a Web server (which technically is called a Hypertext Transport Protocol or HTTP server) in another computer somewhere on the Internet. Similarly, your computer with TCP/IP installed allows you to make client requests for files from File Transfer Protocol (FTP) servers in other computers on the Internet.

Other program relationship models included master/slave, with one program being in charge of all other programs, and peer-to-peer, with either of two programs able to initiate a transaction.

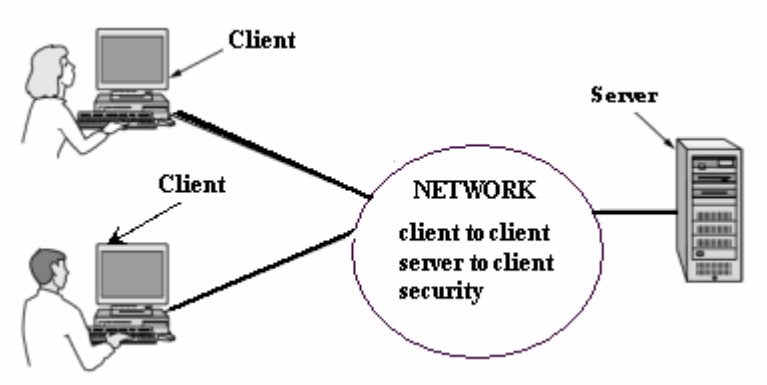


Fig 2.3.2 Client server model

A typical LAN in a corporate office links a group of related computers, workstations. One of the best computers may be given a large capacity disk drive and made as server and remaining computers as clients.

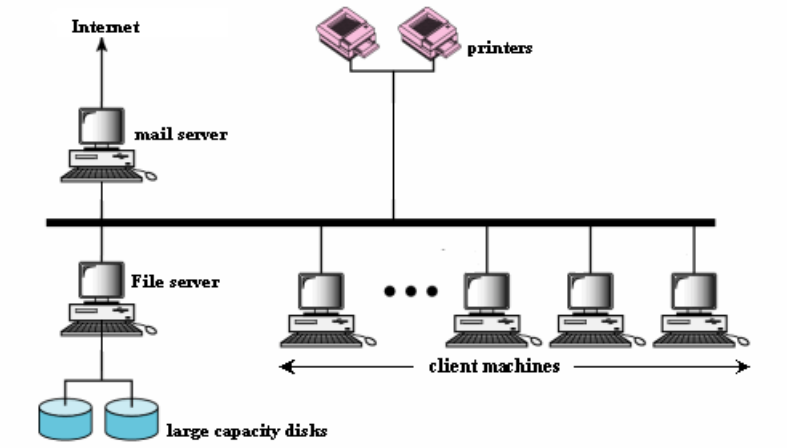


Fig2.3.3 A LAN setup

2.4 Metropolitan Area Network (MAN)

The metropolitan area network is designed to cover an entire city. It can be a single network such as cable TV or a number of LANs connected together within a city to form a MAN. Privately laid cables or public leased lines may be used to form such network.

For instance a business organization may choose MAN to inter connect all its branch offices within the city.

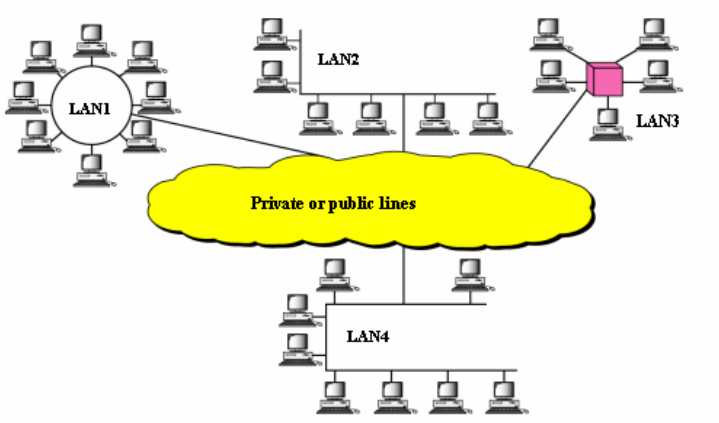


Fig 2.4.1 Typical Metropolitan area network

2.5 Wide Area Network (WAN)

A WAN is a data communications network that covers a relatively broad geographic area, often a country or continent. It contains a collection of machines intended for running user programs. These machines are called hosts.

The hosts are connected by subnet. The purpose of subnet is to carry messages from hosts to hosts. The subnet includes transmission facilities, switching elements and routers provided by common agencies, such as telephone companies. Now a days routers with satellite links are also becoming part of the WAN subnet. All these machines provide long distance transmission of data, voice, image and video information.

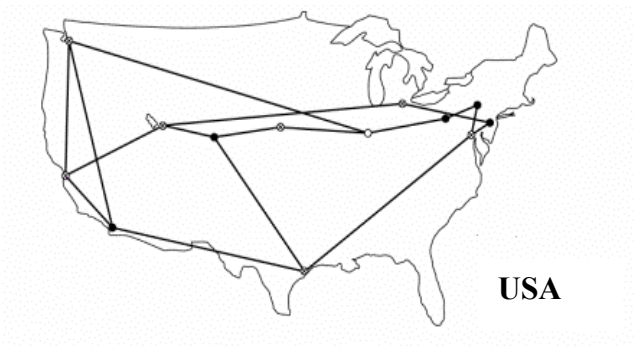


Fig 2.5.1 A typical WAN covering entire United States

Unlike LAN which depend on their own hardware for transmission, WANs may utilize public, leased, or private communication devices when it come across and therefore span an unlimited number of kilometers. A network device called a router connects LANs to a WAN.

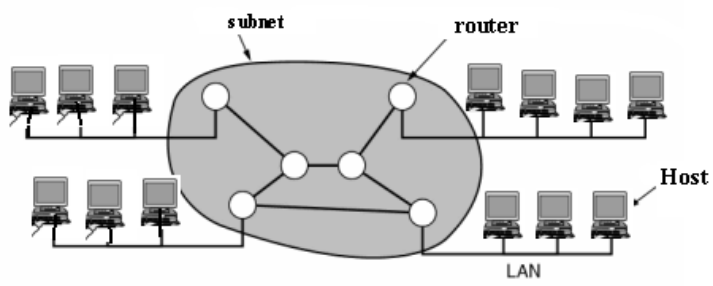


Fig 2.5.2 Typical WAN setup with hosts, routers and subnet.

The Internet is the largest WAN in existence.

2.6 Value added Network (VAN)

#Value-added networks (VAN) are communications networks supplied and managed by third-party companies that facilitate electronic data interchange, Web services and transaction delivery by providing extra networking services.

A value-added network (VAN) is a private network provider (sometimes called a turnkey communications line) that is hired by a company to facilitate electronic data interchange (EDI) or provide other network services. Before the arrival of the World Wide Web, some companies hired value-added networks to move data from their company to other companies. With the arrival of the World Wide Web, many companies found it more cost-efficient to move their data over the Internet instead of paying the minimum monthly fees and per-character charges found in typical VAN contracts. In response, contemporary value-added network providers now focus on offering EDI translation, encryption, secure e-mail, management reporting, and other extra services for their customers.

Value-added networks got their first real foothold in the business world in the area of electronic data interchange (EDI). VANs were deployed to help trading and supply chain partners automate many business-to-business communications and thereby reduce the number of paper transfers needed, cut costs and speed up a wide range of tasks and processes, from inventory and order management to payment.

In today's world, e-commerce is increasingly based on XML, though EDI remains an important part of business and still relies on value-added networks. But other types of VANs have begun to appear, including Web services networks and transaction delivery networks.

#Transaction Delivery Networks (TDN): The newest evolution of VANs, which first appeared in 2000, are the transaction delivery networks (TDN) that provide services for secure end-to-end management of electronic transactions.

Also called transaction processing networks or Internet utility platforms, TDNs can guarantee delivery of messages in addition to providing high security and availability, network performance monitoring and centralized directory management.

TDNs typically use a store-and-forward messaging architecture that's designed to adapt readily to a wide range of disparate systems and support any kind of transaction. Most TDNs offer secure encryption using a public-key infrastructure and certificate authorization for trading partners.

#Internetworks: Internetwork or simply the internet are those when two or more networks are get connected. Individual networks are combined through the use of routers. Lowercase internet should not be confused with the world wide Internet.

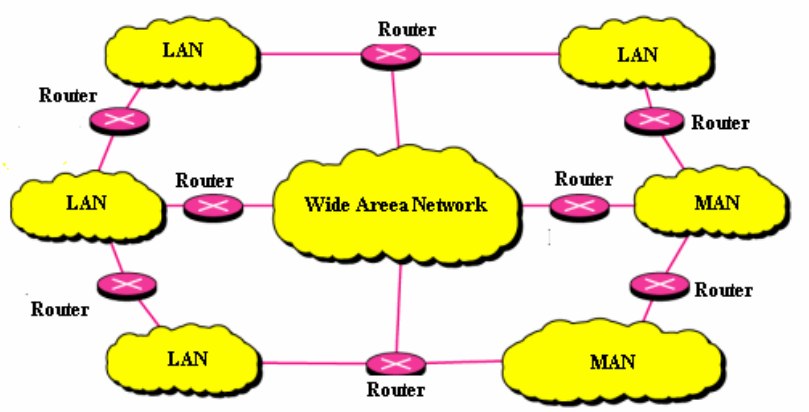


Fig 2.6.1 Typical internetwork connecting LANs and MANs

2.7 Network Topology

The topology defines how the devices (computers, printers..etc) are connected and how the data flows from one device to another. There are two conventions while representing the topologies. The physical topology defines how the devices are physically wired. The logical topology defines how the data flows from one device to another.

Broadly categorized into I) Bus II) Ring III) Star IV) Mesh

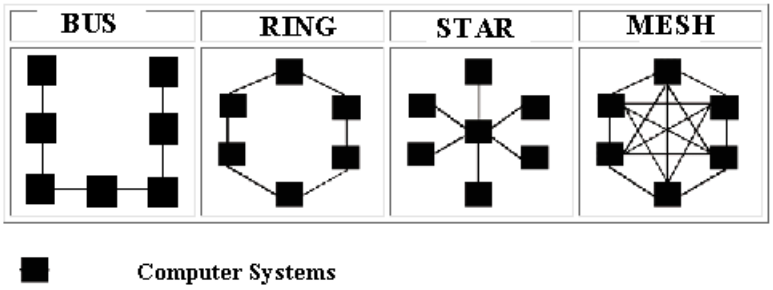


Fig 2.7.1 Outlines of various types of topologies

2.7.1 Bus topology:

In a bus topology all devices are connected to the transmission medium as backbone. There must be a terminator at each end of the bus to avoid signal reflections, which may distort the original signal. Signal is sent in both directions, but some buses are unidirectional. Good for small networks. Can be used for 10BASE5(thick net), 10BASE2(thin net) or 10BROAD36 (broad band) co-axial bus standards.

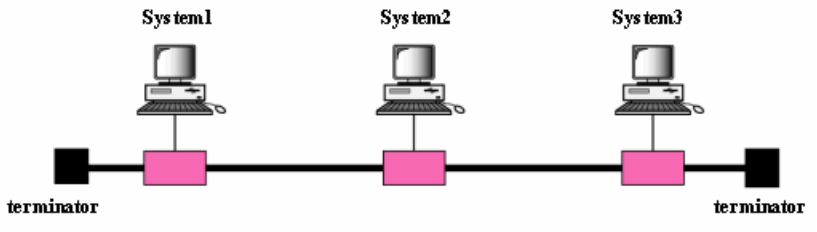


Fig 2.7.2 Physical topology of bus topology.

The main problem with the bus topology is failure of the medium will seriously affect the whole network. Any small break in the media the signal will reflect back and cause errors. The whole network must be shutdown and repaired. In such situations it is difficult to troubleshoot and locate where the break in the cable is or which machine is causing the fault; when one device fails the rest of the LAN fails.

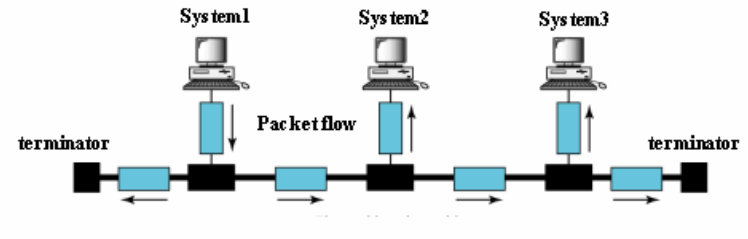


Fig 2.7.3 Logical topology illustration of bus topology.

2.7.2 Ring Topology

Ring topology was in the beginning of LAN area. In a ring topology, each system is connected to the next as shown in the following picture.

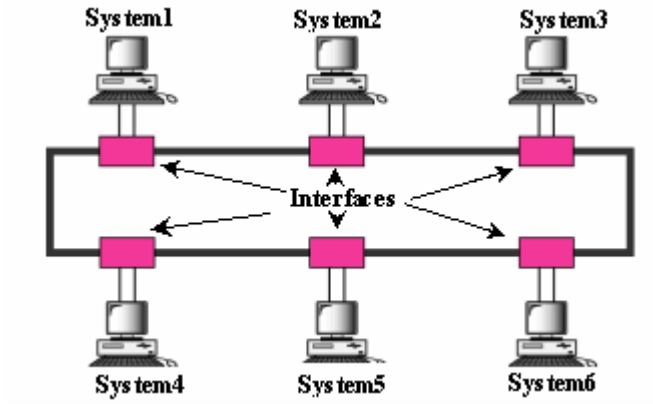


Fig. 2.7.4 Ring topology illustration.

Each device has a transceiver which behaves like a repeater which moves the signal around the ring; ideal for token passing access methods. In this topology signal degeneration is low; only the device that holds the token can transmit which reduces collisions. If you see its negative aspect it is difficult to locate a problem cable segment; expensive hardware.

2.7.3 Star topology

In a star topology each station is connected to a central node. The central node can be either a hub or a switch. The star topology does not have the problem as seen in bus topology. The failure of a media does not affect the entire network. Other stations can continue to operate until the damaged segment is repaired.

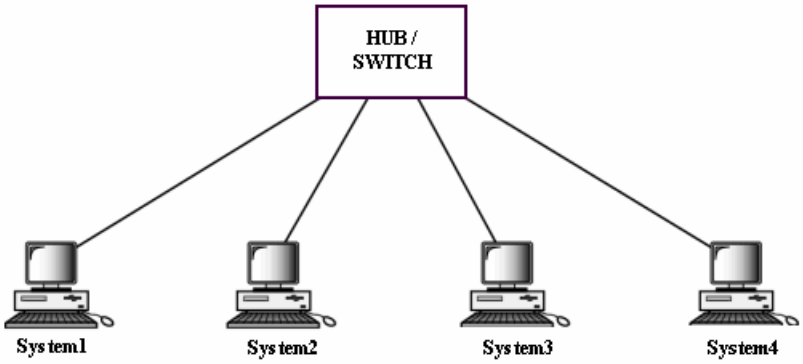


Fig 2.7.5 Physical topology of Star topology.

Commonly used for 10BASE5, 10BASE-T or 100BASE-TX types.

The advantages are cabling is inexpensive, easy to wire, more reliable and easier to manage because of the use of hubs which allow defective cable segments to be routed around; locating and repairing bad cables is easier because of the concentrators; network growth is easier.

The disadvantages are all nodes receive the same signal therefore dividing bandwidth; Maximum computers are 1,024 on a LAN. Maximum UTP (Un shielded twisted pair) length is 100 meters; distance between computers is 2.5 meters.

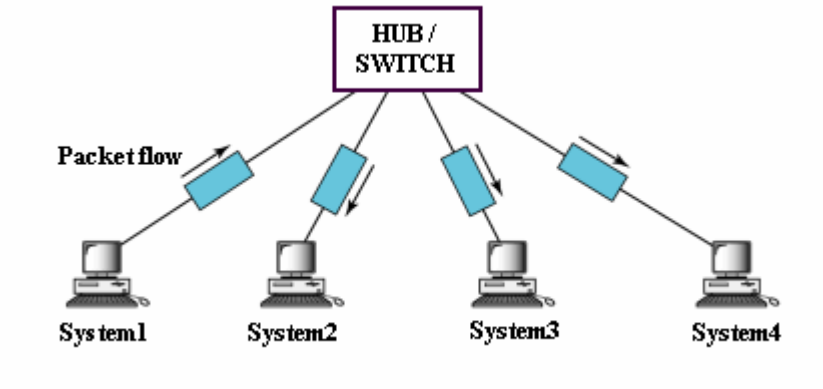


Fig 2.7.6 Logical topology of Star topology.

This topology is the dominant physical topology today.

2.7.4 Mesh topology

A mesh physical topology is when every device on the network is connected to every device on the network; most commonly used in WAN configurations
Helps find the quickest route on the network; provides redundancy. Very expensive and not easy to set up.

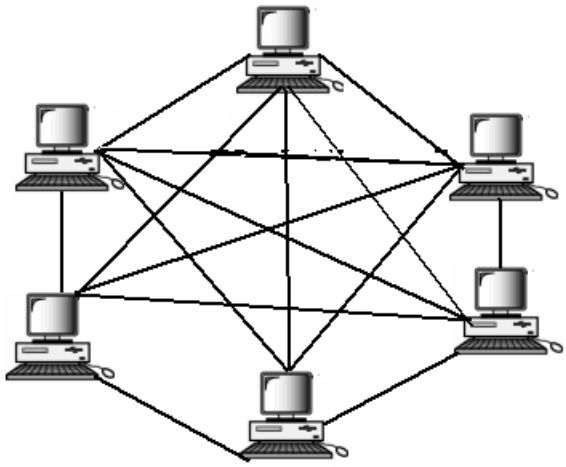


Fig 2.10.1 Physical topology of Mesh topology.

2.8 Hybrid topology

A hybrid topology is a combination of any two or more network topologies in such a way that the resulting network does not have one of the standard forms. For example, a tree network connected to a tree network is still a tree network, but two star networks connected together exhibit hybrid network topologies. A hybrid topology is always produced when two different basic network topologies are connected.

Summary:

Networking not only enables sharing information and resources among the users but also distributed processing.

There are five types of network. Point-point, LAN, MAN, WAN and VAN. Point-point allows sharing of files at a very low speed. LANs are networks distributed over a small geographical area. They can be configured peer-peer or much powerful client/server model. MANs cover entire metropolitan area and may have private lines. WANs cover relatively large geographical area. Here machines are called hosts connected by subnets. The Internet is the largest WAN. VANs are communications networks supplied and managed by third-party companies that facilitate electronic data interchange, Web services and transaction delivery by providing extra networking services.

The network topology defines how the devices (computers, printers..etc) are connected and how the data flows from one device to another. They

are broadly categorized as bus, ring, star, mesh and hybrid. In a bus topology all devices are connected to the transmission medium as backbone. Ring topology was in the beginning of LAN area. In a star topology each station is connected to a central node. The central node can be either a hub or a switch. A mesh physical topology is when every device on the network is connected to every device on the network; most commonly used in WAN configurations. A hybrid topology is a combination of any two or more network topologies in such a way that the resulting network does not have one of the standard forms.

Short questions:

1). State any two benefits of networking.
2). In point-point configuration, machines are connected via …..
3). LAN covers ……area.
4). WANs are spread over …….
5). Site an example for distributed processing
6). Why peer-peer configuration is not preferred?
7). The Internet is living example for …..
8). Normally backbones are of …… topology
9). The one advantage of star topology is:
10). VANs are run by:

Long questions:

1). Why networking?-Elaborate
2). Discuss about client/server model
3). What are value added networks?
4). How many types of networks are there?
5). State the characteristics of LAN
6). Describe WAN and its associated terms
7). Compare a break in the medium of a LAN with a bus topology to a break in a star topology
8). State the various topologies that are possible with LAN
9). Discuss in detail about hybrid topology
10). How many ways a MAN is different from LAN and WAN?

A Local Area Network, LAN is a combination of hardware and software. The physical component of the network system is hardware. The invisible part, that is programs enabling the network to function properly is the software.

3.1 LAN Hardware

The hardware part of the network consist of I) Workstation II) File server III) Gateways IV) Hubs/Switches V) Cables VI) Network interface cards (LAN card, Ethernet card ..)

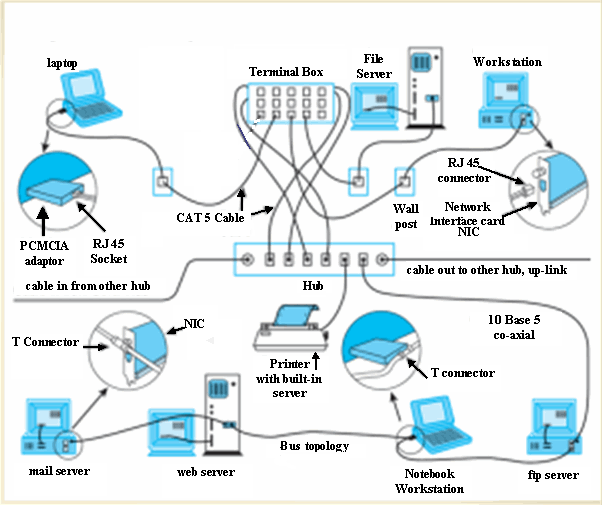


Fig 3.1.1 A LAN setup with its components

3.2 Workstation

A powerful, single-user computer. A workstation is like a personal computer, but it has a more powerful microprocessor and a higher-quality monitor. A typical workstation has a graphic terminal, central processor, digitizer, graphics tablet (optional), and a mouse.

The term "workstation" is often ambiguous because it commonly takes two definitions. The term derives from the function of the machine. It is the computer at which an office worker stations himself.

In some circles, the term "workstation" is reserved for a PC that is connected to a network server. Because the server is often also a PC, the term "PC" doesn't distinguish the two machines from one another. Consequently, people often refer to a PC that functions as a network node as a workstation, and the machine linking the workstations together is the server. (The term "node" can't substitute for workstation because devices other than PCs can also be nodes).

The other application of the term "workstation" refers to powerful, specialized computers still meant to be worked upon by a single individual. For instance, a graphic workstation typically is a powerful computer designed to manipulate technical drawings or video images at high speed. Although this sort of workstation has all the characteristics of a PC, engineers distinguish these machines with the workstation term because the machines do not use the Intel-based microprocessor architecture typical of PCs.

Of course, the term "workstation" also has a definition older than the PC, one that refers to the physical place at which someone does work. Under such a definition, the workstation can be a desk, cubicle, or workbench. In the modern office, even this kind of workstation includes a PC.

Some of the leading makers of workstations are DEC, HP, NeXT, Silicon Graphics, Sun Microsystems etc,.

3.3 File Server

A term often used synonymously with *operating system*, a platform is the underlying hardware or software for a system and is thus the engine that drives the server

In the client/server model, a file server is a computer responsible for the central storage and management of data files so that other computers on the same network can access the files. A file server allows users to share information over a network without having to physically transfer files by floppy diskette or some other external storage device. Any computer can be configured to be a host and act as a file server. In its simplest form, a file server may be an ordinary PC that handles requests for files and sends them over the network. In a more sophisticated network, a file server might be a dedicated network-attached storage (NAS) device that also serves as a remote hard disk drive for other computers, allowing anyone on the network to store files on it as if to their own hard drive.

A program or mechanism that enables the required processes for file sharing can also be called a file server. On the Internet, such programs often use the File Transfer Protocol (FTP). There are several types of servers adding scalable performance to the overall system.

3.4 FTP Servers:

One of the oldest of the Internet services, File Transfer Protocol makes it possible to move one or more files securely between computers while providing file security and organization as well as transfer control.

3.5 Mail Servers:

Almost as ubiquitous and crucial as Web servers, mail servers move and store mail over corporate networks (via LANs and WANs)and across the Internet.

3.6 Proxy Servers:

Proxy servers sit between a client program (typically a Web browser) and an external server (typically another server on the Web) to filter requests, improve performance, and share connections.

3.7 Telnet Servers:

A Telnet server enables users to log on to a host computer and perform tasks as if they're working on the remote computer itself.

3.8 Web Servers:

At its core, a Web server serves static content to a Web browser by loading a file from a disk and serving it across the network to a user's Web browser. The browser and server talking to each other using HTTP mediate this entire exchange.

3.9 Gateways:

The Internet is the collection of heterogeneous computers with different hardware and software platforms. Without gateways computers will never be able to understand and communicate with each other. Essentially, gateways perform protocol translation between networks. Gateways are generally designed and used for LAN-WAN connections and not for inter LAN communications. Gateways function is to do any necessary conversion of protocols between networks. Gateways are customized and designed to perform a specific function and are used on a case-by-case basis. Gateways may do anything from converting protocols to converting application data.

Gateways make a connection between two totally different networks

- Transform the packet format
- Transform the address format
- Transform the protocol

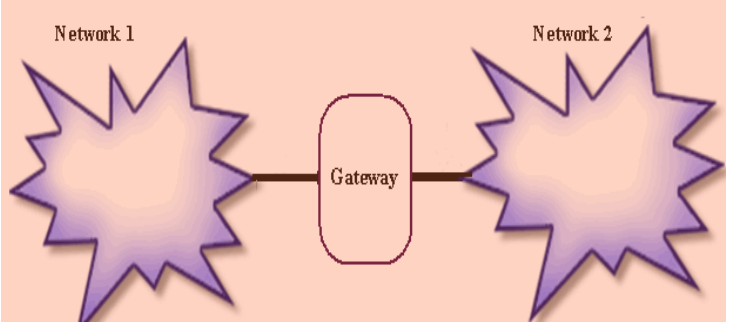


Fig 3.9.1 Gateway between two different networks

3.10 Network interface cards

Network interface cards (NIC), also called network cards and network adapters include a cable socket allowing computers to be connected to the network. All NICs have a unique address (sometimes called a MAC address), placed in them by their manufacturer.

Before sending data onto the network, the network card also organizes data into frames and then sends them out on the network. Notebook computers often use NICs that are plugged into the PCMCIA port. Wireless LAN adapters are needed for WLANs.

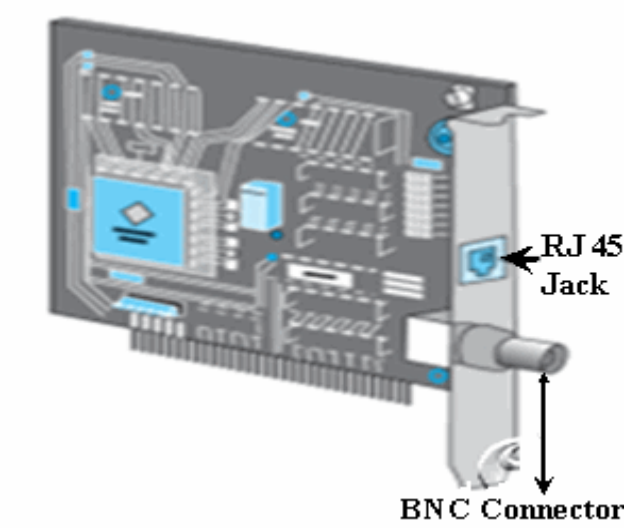


Fig 3.10.1 A commercially available NIC card

NIC card functions:

LAN adapters have their own onboard architectures and they carry NIC Functions out several important functions including

- Monitoring activity on the communication medium
- Providing each workstation/server with a unique identification address (MAC)
- Recognizing and receiving data transmitted to the computer
- Creating (building) the frames needed to transmit data on the communication medium
- Controlling LAN transmission speed
- Transmission error detection and recovery

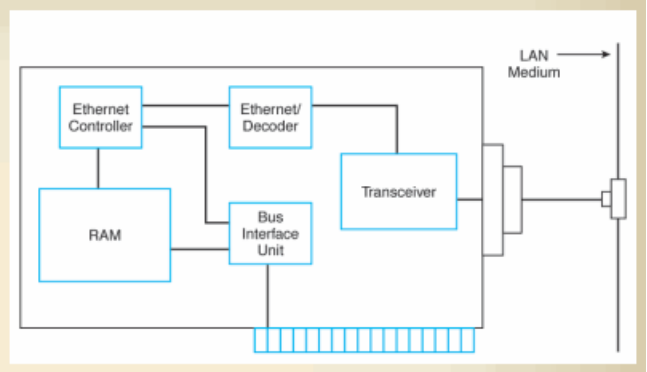


Fig 3.10.2 Block diagram of NIC

3.11 Hubs/Switches

Hubs act as junction boxes, linking cables from several computers on a network. Hubs are usually sold with 4, 8, 16 or 24 ports. Some hubs allow connection of more than one kind of cabling, such as UTP and coax. Hubs also repeat (reconstruct and strengthen) incoming signals. This is important since all signals become weaker with distance. The maximum LAN segment distance for a cable can therefore be extended using hubs.

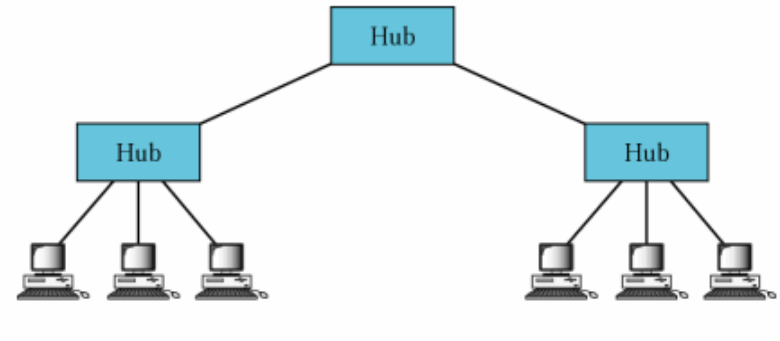


Fig 3.11.1 Creation of levels of hierarchy with Hubs

In general use Hub can be referred to any connecting device and can be considered as multipoint repeater. Hubs can be used to create tree structure like topology (Technically it is bus topology). Network point of view it is a logical device and does not have an address. The added benefit of using Hub is it removes the length restriction 100 meters in 10BaseT

Fig 3.11.2 A commercial Network Hub.

A Switch is more sophisticated than hub and can remember and check node addresses. In fact this phenomenon can affect logical topology of the network! They physically resemble hubs and like hubs, they vary in number of ports, stand-alone vs. stackable, and managed vs. unmanaged.

While a hub broadcasts data frames to all ports, the switch reads the destination address of the data frame and only sends it to the corresponding port. The effect is to turn the network into a group of point-to-point circuits and thus changes the logical topology of the network from a bus to a star.

When a switch is first turned on, its internal forwarding table is empty. It then learns which ports correspond to which computers by reading the source addresses of the incoming frames along with the port number that the frame arrived on. If the switch's forwarding table does not have the destination address of the data frame, it broadcasts the frame to all ports.

Thus, a switch starts by working like a hub and then works more and more as a switch as it fills its forwarding table. Thus they work at machine address level.

Switched Ethernet still uses CSMA/CD media access control, but collisions are less likely as each network segment operates independently.

The network's modified topology also allows multiple messages to be sent at one time.

For example, computer A can send a message to computer B at the same time that computer C sends one to computer B. If two computers send frames to the same destination at the same time, the switch stores the second data frame in memory until it has finished sending the first, then forwards the second.

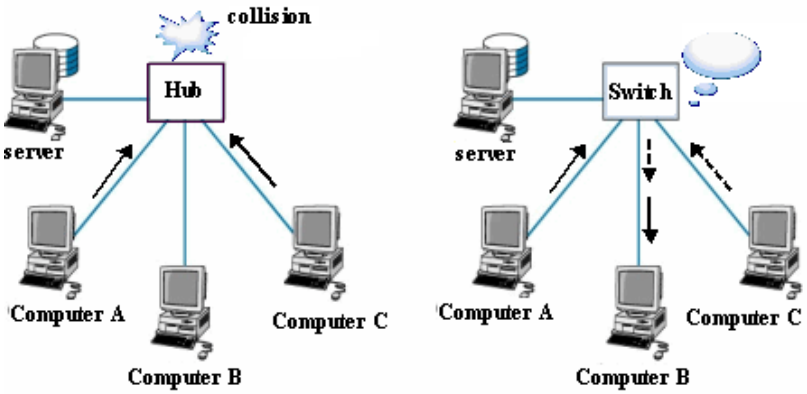


Fig 3.11.3 Hub vs. switches

Switched Ethernet can dramatically improve network performance. Shared Ethernet 10BaseT networks are only capable of using about 50% of capacity before collisions are a problem. Switched Ethernet, however, runs at up to 95% capacity on 10BaseT.

Using a 10/100 switch that uses a 100BaseT connection for the server(s) and/or routers, i.e., the network segments experiencing the highest volume of LAN traffic, can make another performance improvement.

3.12 LAN Cables

One of the biggest problems faced by network system designers is keeping radiation and interference under control. All wires act as antenna, sending and receiving signals. As frequencies increase and wire lengths increase, the radiation increases. The pressure is on network designers to increase both the speed (with higher frequencies) and reach of networks (with longer cables) to keep up with the increasing demands of industry.

Two strategies are commonly used to combat interference from network wiring. One is the coaxial cable, so called because it has a central conductor surrounded by one or more shields that may be a continuous braid or metalized plastic film. Each shield amounts to a long thin tube, and each shares the same longitudinal axis: the central conductor. The surrounding shield typically operates at ground potential, which prevents stray signals from leaking out of the central conductor or noise seeping in. Because of its shielding, coaxial cable is naturally resistant to radiation. As a result, coax was the early choice for network wiring.

Coaxial cables generally use single-ended signals. That is, only a single conductor, the central conductor of the coaxial cable, carries information. The outer conductor operates at ground potential to serve as a shield. Any voltage that might be induced in the central conductor (to become noise or interference) first affects the outer conductor. Because the outer conductor is at ground potential, it shorts out the noise before it can affect the central conductor. (Noise signals are voltages in excess of ground potential; so, forcing the noise to ground potential reduces its value to zero.) Figure 23.4 shows the construction of a typical coaxial cable.

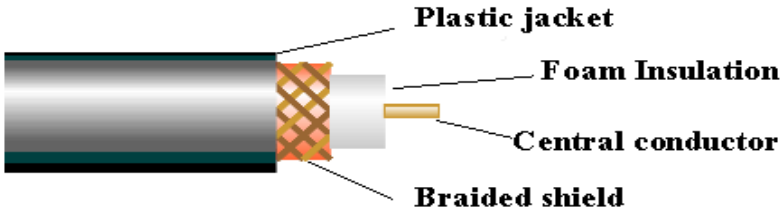


Fig 3.12.1 Components of a coaxial cable.

The primary alternative is twisted pair wiring, which earns its name from being made of two identical insulated conducting wires that are twisted around one another in a loose double-helix. The most common form of twisted pair wiring lacks the shield of coaxial cable and is often denoted by the acronym UTP, which stands unshielded twisted pair. Figure 23.5 shows the construction of a typical twisted-pair cable.

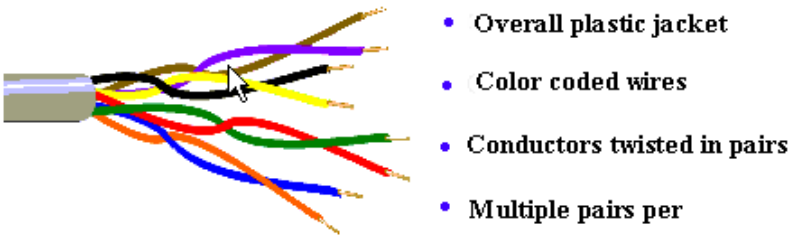


Fig 3.12.2 Components of a twisted pair wiring cable.

Most UTP wiring is installed in the form of multi-pair cables with up to several hundred pairs inside a single plastic sheath. The most common varieties have 4 to 25 twisted pairs in a single cable. The pairs inside the cable are distinguished from one another by color-coding. The body of the wiring is one color alternating with a thinner band of another color. In the two wires of a given pair, the background and banding color are opposites—that is, one wire will have a white background with a blue band and its mate will have a blue background with a white band. Each pair has a different color code. The most common type of UTP cable conforms to the AT&T specification for D-Inside Wire (DIW). The same type of wiring also corresponds to IBM's Type 3 cabling specification for Token Ring networking.

To minimize radiation and interference, most systems that are based on UTP use differential signals. Each conductor carries the same information at different polarities (plus and minus), and the equipment signal subtracts the signal on one conductor from the other before it is amplified (thus finding the difference between the two conductors and the name of the signal type). Because of the polarity difference of the desired signals on the conductors, subtracting them from one another actually doubles the strength of the signal. Noise that is picked up by the wire, however, appears at about equal strength in both wires. The subtraction thus cancels out the noise. Twisting the pair of wires together helps assure that each conductor picks up the same noise. In addition,

any radiation from the wire tends to cancel itself out because the signals radiated from the two conductors are added together. Again, the twist helps ensure that the two signals are equally radiated.

For extra protection, some twisted pair wiring is available with shielding. As with coaxial cable, the shielding prevents interference from getting to the signal conductors.

In practical application, twisted pair wiring has several advantages over coaxial cable. It's cheaper to make and sell. It's more flexible and easier to work with. And zillions of miles of twisted pair wire are installed in offices around the world (it is telephone wire). On the other hand, coaxial cable holds the advantage when it comes to distance. Coaxial cable provides an environment to signals that's more carefully controlled. In general, its shielding and controlled impedance allow for the handling of higher frequencies, which means that network signals are less likely to blur and lose the sharp edges necessary for unambiguous identification as digital values.

Each major wiring standard has its own cabling requirements. Although the limits the standard set for each cabling scheme seem modest (up to a 100 or so PCs), these limits apply to only a single network cable. You can link multiple cables together using network concentrators, or you can extend the reach of a single cable over a long range using a repeater, which is simply an amplifier for network signals. The repeater boosts the signal on the network cable (and may offer ports to link together several network buses) without changing the data on the bus.

Summary:

A Local Area Network, LAN is a combination of hardware and software. The physical component of the network system is hardware. The invisible part, that is programs enabling the network to function properly is the software.

The hardware part of the network consist of I) Workstation II) File server III) Gateways IV) Hubs/Switches V) Cables VI) Network interface cards (LAN card, Ethernet card ..)

Short questions:

1). What is workstation?
2). State the functions of File Server
3). UTP stands for …….
4). What are the hardware components of LAN?
5). State the functions of NIC?
6). What is the segment length in LAN?
7). Contrast hubs with repeater.
8). What are the advantages of shielded wire?
9). How many strands are there in cat5 cable?
10). MAC address stands for ……..

Long questions:

1). How a PC is different from workstation?
2). Discuss about any three types of servers.
3). Draw the block diagram of typical NIC.
4). What are the functions of Gateways?
5). State the advantages of switches over hubs
6). Describe the construction of a co-axial cable
7). Where shielded wire is preferred over ordinary wire?
8). Why proxy servers are employed?
9). Describe various speeds available on Ethernet
10). How switched Ethernet improves the net?

4.1 Modem

Computers can be networked using the existing telephone/or intercom lines. Since telephone lines have a bandwidth of 4kHz maximum, it cannot be directly used for transmission of digital signals. Theoretically digital transmission requires infinite bandwidth. Here the modem comes into picture. The modem (modulator and demodulator) converts the digital signals into audio tones (modulate) while transmitting and converts the incoming audio tones into digital form (demodulate) while receiving.

At the COM port PC outputs its data in serial form. The modem acts as a signal converter that mediates communication between a computer and the telephone network. The PC is called as Data Terminal Equipment (DTE) and the modem as Data Communication Equipment (DCE).

The modem consists of-

- Interface circuitry for linking with the host PC
- Circuits to prepare data for transmission by adding the proper start, stop, and parity bits.
- The modulator that converts PCs digital signals into analog signals.
- The user interface that gives you commands of the modem's operation.

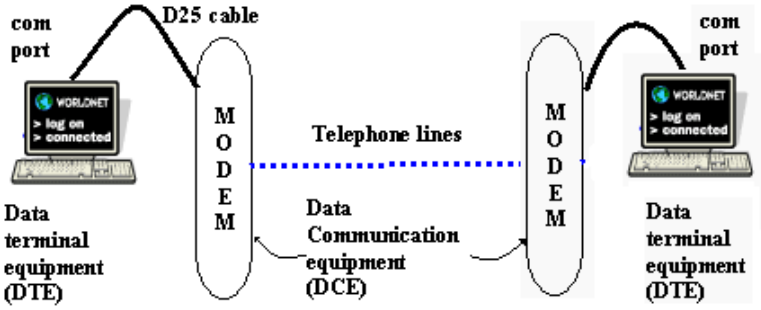


Fig 4.1.1 A Modem's interface to PC

External modems have indicator lights, which allow monitoring the operation of the modem and the progress of a given call.

- **Carrier Detect (CD)** indicates that modem is linked to another modem across the telephone connection. It allows to rule out line trouble if your modem does not seem to be getting a response. This light glows throughout the period modem is connected.

- **Off-Hook (OH)** glows whenever your modem opens a connection on telephone line. It lights when modem starts to make a connection and continues to glow through dialing, negotiations, and the entire connection.
- **Terminal Ready (TR)** glows when the modem senses that PC is ready to communicate with it. When this light is lit, it assures that connected modem to PC that PC's communications software has properly taken control of sender's serial port.

- **Modem Ready (MR)** glows whenever the modem is ready to work. It should be lit whenever the modem is powered up and not in its test state.
- **High Speed (HS)** indicates that the modem is operating at its fastest possible speed. Some modems have separate indicators for each speed increment they support. Others forego speed indicators entirely.

- **Auto Answer (AA)** lights to let you know that your modem is in its answer mode. If your telephone rings, your modem will answer the call (at least if its connected to the line that is ringing).

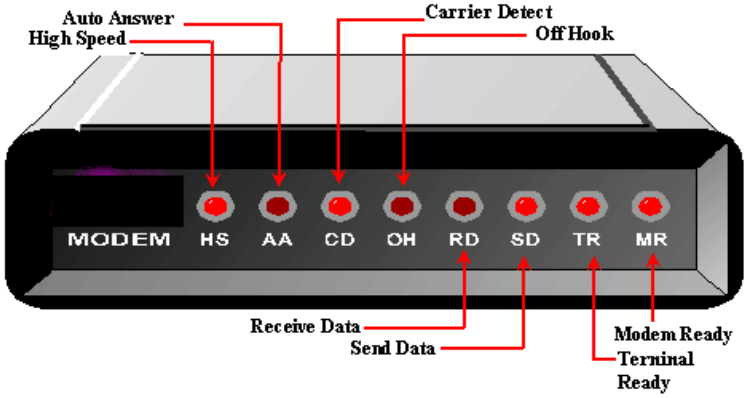


Fig 4.1.2 Modem's indicator signals

4.2 V-SAT

VSAT (Very small Aperture Terminal) Systems uses a satellite connection as a high-speed digital link between a customers' location and the Internet backbone. The data travels from the satellite equipment at the customers' location to the satellite, and then to the teleport for routing to the Internet.

Keeping in view the growing demand for high speed Internet access National Informatics Center (NIC) have employed three types of technologies namely FTDMA (Frequency time division multiple access), Direct PC and IP advantage.

4.3 FTDMA

The FTDMA VSAT system is a private communication network designed for bi-directional traffic that includes interactive transactions, batch file transfers, data broadcast and voice communications. Broadcast of audio and video can also be included as add-on options.

The FTDMA features a unique and patented two-dimensional satellite access scheme, which combines the TDMA slotted and FDMA techniques.

The star topology of a FTDMA network is well suited for use in configurations where corporate headquarters or data centers communicate with hundreds or thousands of geographically dispersed locations. The system supports a variety of data protocols and applications as well as voice, providing central 'host-to-remote terminal' and remote terminal-to-remote terminal connectivity.

A FTDMA network consists of the following components:

- A Master Earth Station and a control facility or Hub.
- A number of VSATs located at the customers' remote sites.
- **K_u**-band satellite channels, which provide the transmission medium interconnecting the Hub and the VSATs.

The FTDMA network supports multiple outbound (256kbps) and multiple inbound (76.8 kbps). The modular hub design allows each customer's network to be sized cost-effectively to meet the existing and future needs. It also permits an easy incorporation of new features as

well as independent sizing of host ports and in-bound and out-bound bandwidths

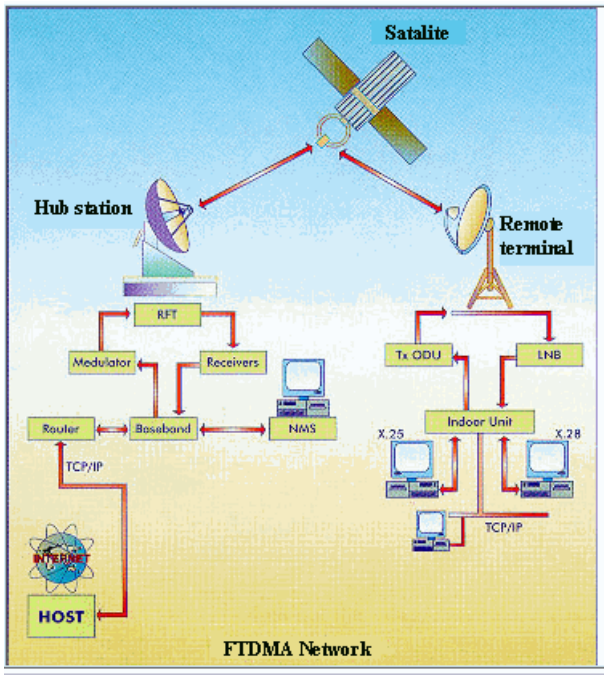


Fig 4.3.1 FTDMA Network

Components of the FTDMA VSAT

- A small outdoor antenna (1.2/1.8/2.4 metres)
- A low power Out Door Unit (ODU)
- An In Door Unit (IDU)

The VSAT supports TCP/IP, X.25 and X.28 protocols. The IDU provides the following interfaces for connecting the user's machines :

- LAN port with UTP (RJ45) interface.
- Four Serial ports which could be configured for X.25 or X.28.
- Voice port with RJ11 interface (optional)
- The system utilizes a "Television Receive Only" technology by using mass produced Low Noise Blocks (LNBs) on the VSAT receipt channel.

The various applications supported on the FTDMA network include:

- Corporate communication
- E-mail
- EDI (Electronic data interchange)
- Internet/Intranet Solutions
- Web enabled database access
- Point-to-Point voice communication
- Data broadcast
- Multimedia Broadcast

4.4 DirectPC

The System provides a 12 Mbps broadcast channel from a single uplink earth station called Network Operations Center (NOC). Data Encryption Standard (DES) encryption-based conditional access ensures that a receiver PC may only access that data which it is authorized to receive.

The DirecPC system primarily offers the following three kinds of services to Intel x86 PC servers and workstations:

Digital Package Delivery: This is a service that uses the broadcast nature of DirecPC's satellite communication technology to provide an efficient mechanism to transfer any collection of PC files (called a Package) to widely distributed multiple receiving PCs. Packages are stored-and-forwarded through the DirecPC NOC.

As such, Package Delivery is not a real- time service. DirecPC package takes advantage of the broadcast nature of satellite communication in greatly reducing the cost of transferring relatively large packages such as those occupying more than 100 MB , to multiple locations by having a single broadcast received in parallel by all addressed sites. The service is typically used with a selective retransmission technique to ensure error free delivery to each location.

Multimedia Service: DirecPC's multimedia service provides IP multicast transport via the DirecPC service. The NOC relays a configurable set of IP multicast addresses across the space link. The information provider passes IP multicast packets to the NOC via an Ethernet link or by any wide area network connection. Remote DirecPC adapter card accesses the IP multicast through the standard Winsock API

allowing many off-the-shelf applications to operate with no modification.

Turbo Internet Access: This allows a PC high-speed (up to 400kbps) access to the Internet. At the remote host, an NDIS device driver operates with the native TCP/IP stack for Win95. Reception from the Internet takes place via the DirecPC. Transmission into the Internet takes place via a dial-up Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol (PPP) connection into an Internet access provider. The DirecPC architecture is open, thus allowing the information provider, complete control over their content and the user interface with it.

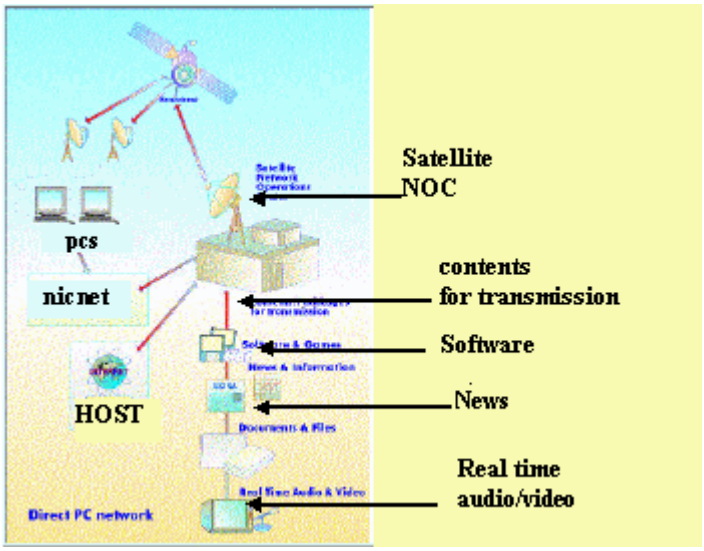


Fig.4.4.1 DirectPC

4.5 IP Advantage

The IP Advantage VSAT comprises of ISBN (Integrated Satellite Business Network) and DirecPC. ISBN is a two-way transmission system for data traffic between a HUB and many remote locations or Personal Earth Stations (PES). All ISBN traffic is carried digitally between the HUB and remote PES via one or more transponders aboard a Geostationary Satellite.

A single large sophisticated HUB station supports many small PES stations. The HUB-to-PES direction of transmission is termed as "out route", while the PES-to-HUB transmission is termed as "in route".

Since the remote stations have small antenna and low transmit power levels, the in route signals are relatively weak. The HUB, with its high power amplifier, transmits a sufficiently strong signal for reception by the small remote stations ; and the large HUB antenna with its large receive gain compensates for the weak signals transmitted by the remote stations.

The Time Division Multiplexed Outbound is a 512kbps continuous bit stream, consisting of concatenated (i.e. linked together) variable length packets. The ISBN inbound, from the remote station to the Hub, consists of multiple independent Time Division Multiple Access of 64kbps bit streams. The in route data is packetized and transmitted as bursts. The assignment of time slots in which each user is permitted to transmit its burst of traffic is centrally controlled at the Hub and can be tailored to the needs of each user.

The IP Advantage network supports multiple outbound (512kbps) and multiple inbounds (64kbps). The modular hub design allows each customer's network to be sized cost-effectively to meet the existing and the future needs. It also permits easy incorporation of new features as well as independent sizing of host ports and inbound and outbound bandwidths.

Components of IP Advantage VSAT

- A small outdoor antenna (1.2/1.8/2.4 metres)
- A low power outdoor unit (ODU)
- An indoor unit (IDU)

The VSAT supports TCP/IP X.25 and X.28 protocols. The IDU provides the following interfaces for connecting the user's machines:

- LAN Port with BNC (10base2) or UTP (RJ45)
- Two serial ports which can be configured for X.25 or X.28.
- TVRO out which is used to connect to DirecPC adapter card installed in the PC.
- The System utilizes a television receive only (TVRO) technology by using mass produced Low Noise Blocks (LNBs) on the VSAT receipt channel.

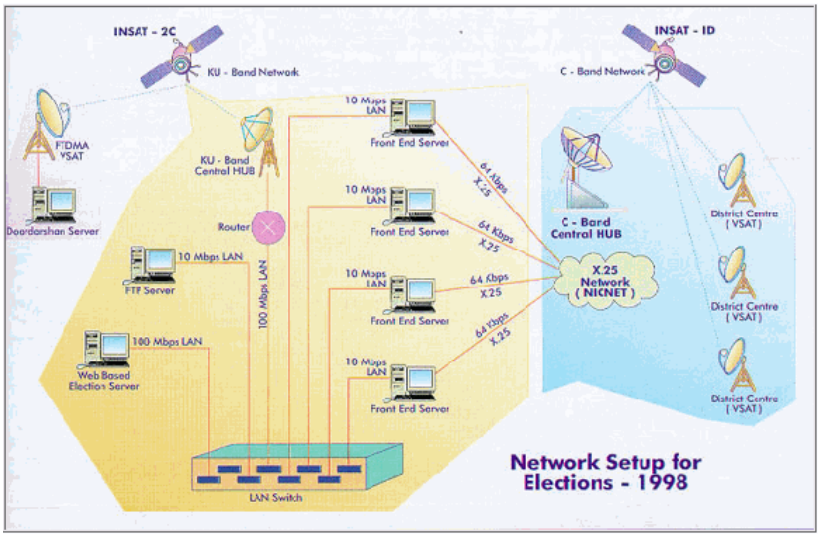


Fig. 4.5.1 Network setup – 1998 elections

The applications supported on the IP Advantage network include:

- Corporate communication
- E-mail
- EDI
- Internet/Intranet Solutions
- Web enabled database access
- Data and Video Broadcast
- Multimedia Broadcast
- Package Delivery

The entire NICNET has been fully converted to TCP/IP based network.

4.6 Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is a high performance, cell oriented switching and multiplexing technology that utilizes fixed length packets to carry different types of traffic.

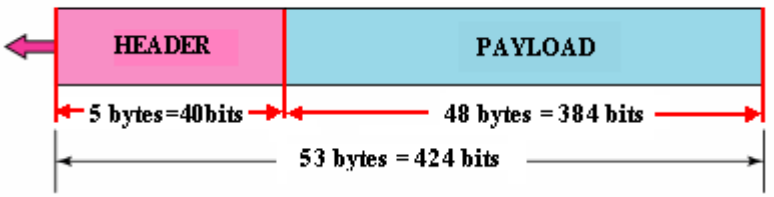


Fig.4.6.1 ATM format

ATM differs from more common data link technologies like Ethernet in several ways. For example, ATM utilizes no routing. Hardware devices known as ATM switches establish point-to-point connections between endpoints and data flows directly from source to destination. Additionally, instead of using variable-length packets as Ethernet does, ATM utilizes fixed-sized cells. ATM cells are 53 bytes in length that includes 48 bytes of data and five (5) bytes of header information.

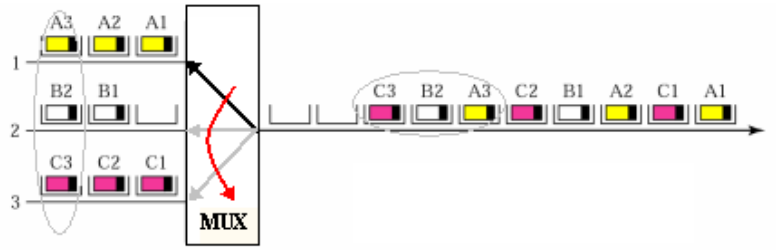


Fig.4.6.2 Asynchronous TDM

ATM uses asynchronous time division multiplexing that is why it is called asynchronous transfer mode

ATM technology is designed to improve utilization and quality of service (QoS) on high-traffic networks. Without routing and with fixed-size cells, networks can much more easily manage bandwidth under ATM than under Ethernet, for example. The high cost of ATM relative to Ethernet is one factor that has limited its adoption to "backbone" and other high-performance, specialized networks.

Most serial communications and practically all LAN communications are asynchronous, but most data transfers in and out of your microprocessor, the traffic on your parallel port, and the traffic on your computer's bus, are synchronous. Given a steady stream of data, synchronous transmission tends to be more efficient than asynchronous, while asynchronous transmission tends to be more flexible and resilient.

Benefits of ATM

- High performance via hardware switching
- Dynamic bandwidth for bursty traffic
- Class-of-service support for multimedia
- Scalability in speed and network size
- Common LAN/ WAN architecture
- Virtual circuit architecture

Summary:

Modems, V-SATs, ATMs: all these equipments are examples of communication hardware category with diversified technologies. The modem (modulator and demodulator) converts the digital signals into audio tones (modulate) while transmitting and converts the incoming audio tones into digital form (demodulate) while receiving.
VSAT (Very small Aperture Terminal) Systems uses a satellite connection as a high-speed digital link between a customers' location and the Internet backbone. The data travels from the satellite equipment at the customers' location to the satellite, and then to the teleport for routing to the Internet.
Asynchronous Transfer Mode (ATM) is a high performance, cell oriented switching and multiplexing technology that utilizes fixed length packets to carry different types of traffic.

Short questions:

1). Modem stands for ……
2). Telephone lines have a bandwidth of ……
3). When does CD lamp in the modem lits ?
4). To which port the external modem is usually connected?
5). DTE and DCE stands for…
6). Is V-SAT is confined to only digital signals?
7). Which topology FTDMA is based on?
8). List the various protocols that FTDMA support.
9). ATM stands for ….
10). The ATM packet size is …..

Long questions:

1). Discuss in detail about modem's interface to PC
2). Identify the various panel lamps of a modem
3). Draw the block diagram and operation of PC with modem
4). Describe in detail about various technologies employed in V-SAT for Internet access.
5). List the components of FTDMA technology
6). Enumerate the services offered by DirectPC
7). Describe the packet delivery mechanism in DirectPC
8). What are the components of IP advantage
9). Justify the benefits of ATM.
10).Discuss in detail about ATM.

5.1 Network Operating System

The core of a network is the network operating system. Just as a computer cannot operate without an operating system, a network of computers cannot operate without a network operating system.

A network operating system implements protocol stacks as well as device drivers for networking hardware. Some network operating systems, like Windows, also add custom networking features like Internet Connection Sharing (ICS).

Every network operating system provides basic services to the computers on its network. These services include:

- Coordinating the activities of the various devices on the network to ensure that communication takes place as and when required.
- Providing clients with access to network resources, including files and such peripheral devices as printers and fax machines.
- Ensuring the security of data and devices on the network through centralized administration tools.

5.2 Features of Network Operating System

A network operating system must support mechanisms that enable applications to communicate with one another: for example, applications that enable multiple computers to work jointly on a single task, such as a mathematical calculation. A network operating system must also support multiple processors, clusters of disk drives, and data security features. Finally, a network operating system must be reliable and be able to recover quickly from errors.

Depending upon the network operating system manufacturer, desktop Computer's networking software can be added either to the computer's own operating system or be integrated with it. Network operating system software is integrated into a number of popular operating systems, including Microsoft Windows 2000, Windows NT, Windows 98, Windows 95, and Apple Macintosh.

Network operating systems have existed for more than thirty years. The UNIX operating system was designed from the beginning to support networking. In its early forms, Windows did not support networking, so Novell NetWare became the first popular network operating system for the personal computer (Windows 95 and Windows for Workgroups were Microsoft's first network operating system products).

Today, nearly any consumer operating system qualifies as a NOS due to the popularity of the Internet and the obvious need to support Internet Protocol (IP) networking at a minimum.

5.3 UNIX

The UNIX operating system was designed to let a number of programmers access the computer at the same time and share its resources.

The operating system coordinates the use of the computer's resources, allowing one person, for example, to run a spell check program while another creates a document, lets another edit a document while another creates graphics, and lets another user format a document -- all at the same time, with each user oblivious to the activities of the others.

The operating system controls all of the commands from all of the keyboards and all of the data being generated, and permits each user to believe he or she is the only person working on the computer.

This real-time sharing of resources make UNIX one of the most powerful operating systems ever.

Although UNIX was developed by programmers for programmers, it provides an environment so powerful and flexible that it is found in businesses, sciences, academia, and industry. Many telecommunications switches and transmission systems also are controlled by administration and maintenance systems based on UNIX.
While initially designed for medium-sized minicomputers, the operating system was soon moved to larger, more powerful mainframe computers. As personal computers grew in popularity, versions of UNIX found their way into these boxes, and a number of companies produce UNIX-based machines for the scientific and programming communities. The features of UNIX are:

- **Multitasking capability:**
  Lets a computer do several things at once, such as printing out one file while the user edits another file.

- **Multi-user capability:**
  Permits multiple users to use the computer. The computer can take the commands of a number of users -- determined by the design of the computer -- to run programs, access files, and print documents at the same time.
- **Portability:**
  Permitting it to move from one brand of computer to another with a minimum of code changes.
- **Library of application software:**
  There are hundreds of UNIX applications that can be purchased from third-party vendors, in addition to the applications that come with UNIX.

5.3.1 UNIX Communications

E-mail is commonplace today, but it has only come into its own in the business community within the last 10 years. Not so with UNIX users, who have been enjoying e-mail for several decades.

UNIX e-mail at first permitted users on the same computer to communicate with each other via their terminals. Then users on different machines, even made by different vendors, were connected to support e-mail. And finally, UNIX systems around the world were linked into a world wide web decades before the development of today's World Wide Web.

The UNIX system is functionally organized at three levels:

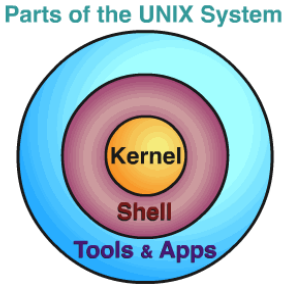


Fig.5.3.1 Onion skin diagram of Unix system

- The **kernel**, which schedules tasks and manages storage;
- The **shell**, which connects and interprets users' commands, calls programs from memory, and executes them. Known as command interpreter
- The **tools and applications** that offer additional functionality to the operating system

5.3.2 Unix Shell

There five types of shells are there written by different people

- **Bourne (sh):** this is the original Unix shell, available in nearly every flavor of Unix.
- **Korn (ksh):** a backwards-compatible upgrade to the Bourne shell, developed by David G. Korn at AT&T Bell Laboratories.
- **Bash (bash):** Bourne-again shell, a public domain shell containing features of the Bourne, Korn and c-shell.
- **C-Shell (csh) and T-C-Shell (tcsh):** The c-shell is similar to C programming language; t-c-shell extends csh.
- **Z-Shell (zsh):** an open-source Unix shell

5.3.3 Unix file

A file is a collection of information, which can be data, an application, documents; in fact, under UNIX, a file can contain anything. When a file is created, UNIX assigns the file a unique internal number (called an inode).

- **File Link (creating alias name for a file)**

A file link is a directory entry which points to an original file somewhere else. A link is made to an existing file using the **ln** command. This creates a directory entry which points to the existing file (it does not make a copy of the existing file). This allows more than one reference to an existing file.

For instance, a person can give another access to a file and let them create a link to it. In this way they both can access and work with the same file, ensuring that the information they enter into the file is up-to-date. Only the original owner of the file may delete the file.

- **Security associated with files and directories**

UNIX provides three sets of security rights for each file and directory entry. These sets are for the owner, the group to the owner belongs, and any other users on the system.

Each user belongs to a group (only one at a time). Group membership facilitates the sharing of common files. A user can change their membership to another group by using the **newgrp** command.

The security rights are

- read (read, display, copy the file contents)
- write (modify and append to the file contents)
- execute (run the file as a program)

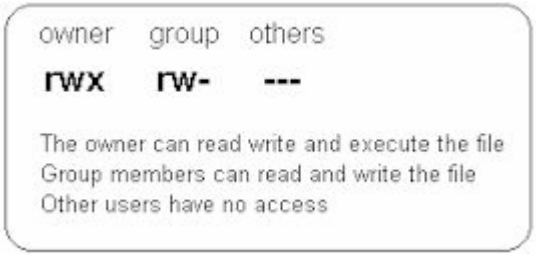


Fig 5.3.2 Security settings for a file

- **Viewing files**

ls command shows the security rights associated with the file, as well as the owner (ram), the group that the owner belongs to, the size of the file and other information.

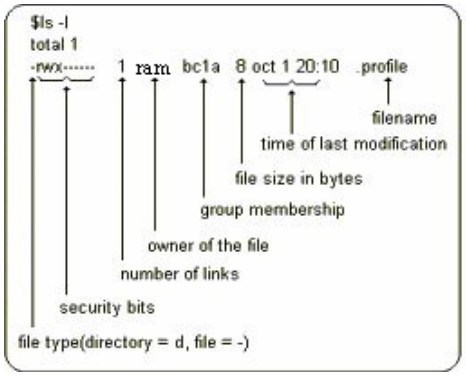


Fig.5.3.3 Output display for **ls** command

- **Mountable File Systems**

All UNIX systems have at least one permanent non-removable hard disk system. The root directory and the directories below it are stored on this disk. Its structure is known as the root file system.

If an additional hard disk is added, UNIX creates a separate new file system on this disk. Before it can be used, it must be attached to the root file system. This is called mounting an additional file system.

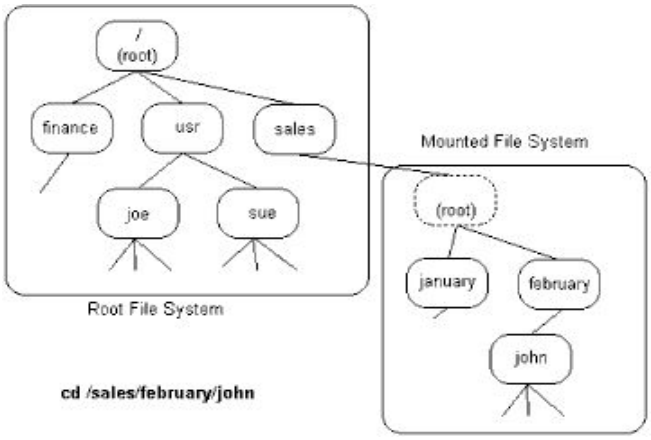


Fig.5.3.4 Mountable File system

An empty directory on the root file system is selected as the mount point, and using the UNIX mount command, the new file system will appear under this directory.

- **Unix Networking**

UNIX systems are usually interconnected using TCP/IP (Transmission Control Protocol, Internet Protocol). This is a protocol mechanism that is widely used by large networks worldwide to interconnect computers of different types.

A protocol is a set of rules that governs how computers talk to each other. TCP/IP is a widely used and very popular protocol. With TCP/IP, different computer systems can reliably exchange data on an interconnected network. It also provides a consistent set of application programming interfaces (API's) to support application development.

- **Network File Systems (NFS)**

This allows you to manipulate files on a remote TCP/IP host as if they reside on the local machine. NFS supports a hierarchical file structure. Using NFS, a system administrator can mount a directory structure that resides on another computer into the directory structure of the local computer.

- **Network Services**

To provide services such as ftp, telnet and WWW servers, they are enabled on the host computer by running the appropriate software, called a system **daemon** process. For example, to configure a computer as an ftp server requires the installation, configuration and running of the ftpd process (most system processes end in d, which means daemon).

If the daemon process is not started, the service is not available on that host computer. In other words, you cannot ftp into a host, which is not running the ftp daemon service.

When a UNIX host starts up, it usually runs an inetd service, which reads the file **/etc/inetd.conf** which contains a list of the networking services for the host to run. A system administrator would edit this file and include the various services that are required to run when the system starts.

- **Remote Execution (rexec)**

This allows executing a command on another host and receiving the results on your local machine. This means you can take advantage of better processing power or unavailable software which your local machine does not have.

A host machine, username, password and the command to execute are passed to the host machine. If the authentification succeeds, the command is executed, and responses returned to the local machine.

- **Remote Shell (rsh)**

This allows you to execute a command on another host. Unlike rexec, it neither requires or allows you to provide a password. You must have a user account on the host server however.

- **File Transfer Protocol (ftp)**

This allows you to transfer files between your host and another host machine. A shell is provided which enables you to

- Change directories on the host or local machine
- Display directories and files
- Change the file transfer mode (binary or text)
- Execute commands
- Delete or rename files
- Open and close connections to a host

- **Terminal Emulation (telnet)**

This allows you to logon to a host using terminal emulation. You can execute commands on the host and run application software.

5.4 Domain Name Servers

This is a hierarchical naming system for identifying host computers on networks or the Internet. Each host name is comprised of domain labels separated by periods. If your machine is connected to the Internet, you assign local domain name host names only, and your higher level domain name is assigned to you.

For example, the domain name assigned to Osmania University is **osmania.ac.in** has the higher level domain names of ac (academic) and in (India). Examples of the host computers at Osmania University are called staff, results, and www. Their host names in the domain are
staff.osmania.ac.in
results.osmania.ac.in
www.osmania.ac.in

Users are also assigned names. Consider the user web master, who has an account on the host machine staff .The domain name for this user is,
webmaster@staff.osmania.ac.in

When you send email or access resources on other computers, the domain names need to be resolved in order that a connection is made to the correct computer. One host computer in the network acts as a name resolver (domain name server), which resolves domain names to computers. For example, if you want to ftp to the local host *staff*, your

computer sends a request to the designated name domain server, which if it knows about the host *staff*, will send back the computer TCP/IP address, which your computer then uses to initiate a connection request.
The name domain server uses a special file called **hosts** to resolve host names and their TCP/IP addresses.

5.5 **Simple Network Management Protocol (snmp)**

This provides a means for managing a network environment. Each host, router or gateway running SNMP can be interrogated for information related to the network.
Examples of information are,

- Names
- Packets transmitted and received
- Errors
- Routing information

5.6 Boot Protocol (bootp)

This service allows a local computer to get its Internet address (TCP/IP configuration details) from a designated bootp server. The bootp server has a list of network card addresses for each computer and the TCP/IP addresses to use for those computers stored in a file (**/etc/bootptab**). When it receives a request from a computer, it looks at this file for a match and responds with the assigned TCP/IP address.

5.7 **Sockets**

Sockets are an end-to-end numbered connection between two UNIX machines communicating via TCP/IP. Standard packages are assigned special socket numbers (telnet is port 23). The socket numbers for various protocols and services are found in **/etc/services**.
A programming socket interface provides calls for opening, reading, writing and closing a socket to another host machine. In this way, the programmer need not be concerned with the underlying protocol associated with the socket interface.

5.8 **Networking Commands**

Following is discussion of some of the common networking commands.

- **arp (address resolution protocol)**

  This command displays and modifies the Internet to physical hardware address translation tables. As computers establish connections to other computers (via telnet, ftp or other means), the details of these are kept locally in a buffer store called the *arp cache*. The system administrator can view this cache and modify its contents using the **arp** command.

  $ arp
  address/HW type/ HW address/mask /Interface
  johny-osmania.ac.in/either/0:40:19:77:88:00/C/eth0

- **netstat (network status)**

This command displays the network status of the local host. It provides information about the TCP connections, packet statistics, memory buffers and socket information**.**

$ netstat
// a typical output
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 126 staff.osmania.ac.in:telnet flame.iit.ac.nz:1756 ESTABLISHED
tcp 0 0 staff.osmania.ac.in:telnet dhcp-78-8.iit.ac.in:1100 ESTABLISHED
tcp 0 0 luni.cit.ac.nz:telnet dhcp-78-3.iit.ac.in:1130 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags Type State I-Node Path
unix 2 [ ] STREAM 830794 /dev/log
unix 2 [ ] STREAM CONNECTED 830793
unix 1 [ ] STREAM 830746
unix 2 [ ] STREAM 830697 /dev/log
unix 2 [ ] STREAM CONNECTED 830696
unix 2 [ ] STREAM 830680 /dev/log
unix 2 [ ] STREAM CONNECTED 830679
$

- **ping**

This command sends an echo request to a host. It is a diagnostic tool for testing **whether a host can be found**. When the request reaches the host, it is sent back to the originator.

$ ping staff
PING staff.osmania.ac.in (202:54:62:202) 56 data bytes
64 bytes from 202:54:62:202: icmp_seq=0 ttl=128 time=0.8 ms
64 bytes from 202:54:62:202: icmp_seq=1 ttl=128 time=0.8 ms
64 bytes from 202:54:62:202: icmp_seq=2 ttl=128 time=0.8 ms
--- staff.osmania.ac.in ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.8 ms
$

- **route**

  This command manually manipulates the network routing tables, which are used to connect to other hosts.

  Example
  $ route add net 129.34.10.0 129.34.20.1 1
  ; add a new network 129.34.10.0 accessible via the gateway
  ;129.34.20.1 and there is one metric hop to this destination

- **nslookup**

This command is used to query a domain name server and return information about a designated host.

$ nslookup
Default Server: www.osmania.ac.in Address: 202:54:62:204
> **staff**
Server: osmania.ac.in
Address: 202:54:62:203
Name: staff.osmania.ac.in
Address: 202:54:62:202
> **exit**
$

- **traceroute**

This command is similar to ping, but traces the path (or route) that data travels across the network to a specific host computer.

$ traceroute
traceroute to tukutuku.cit.ac.nz (202.54.60.198), 30 hops max, 40 byte packets
1 route64.iit.ac.in (202.54.60.1.1) 1.87 ms 1.737 ms 1.727 ms
2 staff.iit.ac.in (202.54.61.102) 2.815 ms 2.862 ms 3.101 ms
$

- **Some networking files**

The following files are associated with networking and are generally found in the /etc subdirectory

/etc/bootptab Used by bootpd
/etc/gateways Used by routed and identifies the accessible gateway machines.
/etc/hosts Used by clients and servers to resolve host names if a name server is unavailable.
/etc.inetd.conf Used by inetd to start services when computer boots
/etc/ftpusers Used by ftpd to restrict or block specific users accessing ftp
/etc/resolv.conf Used by clients and servers to provide a domain name and name server address.

5.9 System Administrators

A system administrator is responsible for the day to day running of the computer. This involves the following activities

- Creation, modification and deletion of user accounts
- Generate daily reports from log files
- Monitor system activity and perform auditing
- Ensure sufficient dish space exists and ensure file system integrity is maintained
- Install, configure and remove software packages as required
- Perform daily maintenance tasks, monitoring mail, print and other applications

- Start and shutdown the system
- Perform backups
- Install, mount and configure peripheral devices such as terminals and disk drives
- A system administrator has unrestricted access, thus can delete any file (including system files that are part of UNIX), and execute any program.
- For the most part, a system administrator can automate some activities to reduce the amount of work they are required to do, but other tasks, such as resetting user passwords and unlocking terminals or user accounts require the administrator to log on to the computer system using the administrator account (**root**).

5.9.1 **Log on as an administrator**

There are two ways that you can log on as a system administrator. If you are already logged on as a user, you can use the su (super user) utility to assume the administrator identity.

$ su
Password ####### _

When you are logged in as a system administrator, the system prompt changes to #.
The other way you can log on as a system administrator is to use the special administrator account, named **root**.

Login: **root**
Password ######

5.9.2 System administrator account

When you are logged in as root, the UNIX system gives you unrestricted access to every file and directory. This means can delete, rename, copy or move any file, including vital system files required for UNIX to function correctly. If a file is accidentally erased, there is no way to undelete the file other than to restore it from tape backup, or failing this, reinstalling the operating system.

5.9.3 The /etc directory and system administrators

This directory contains important system files, user and group account information, and special scripts that configure the system. Some of these are shown below:

- /etc/adduser.conf
  Specifies default configuration for creating user accounts
- /etc/bootptab
  Holds computer names and IP addresses for remote booting workstations
- /etc/crontab
  List of jobs to be executed
- /etc/fstab
  List of filesystems to mount when UNIX boots
- /etc/group
  List of groups
- /etc/inittab
  Lists the processes that are started when UNIX boots
- /etc/passwd
  The password file, usernames, passwords, group membership, shell
- /etc/motd
  Message of the day
- /etc/mtab
  List of currently mounted file systems

5.10 Windows NT Server

A modern personal computer is a powerful tool that can be used in countless ways, if you can tap into its potential. Unfortunately, for years computers have been intimidating and difficult for the average person to use. In recent years, however, computer developers have concluded that since most people learn, work and think visually, it would be best to present computer functions visually. With this in mind a number of companies experimented with various Graphical User Interfaces (GUI) most of which make use of a mouse or another pointing device. This has simplified computer usage and has thus opened up the potential of using computers to a much larger audience.

Graphical User Interface essentially means, "you control the system with pictures". Thus, by interacting with (clicking and moving) the symbols on your screen, you are able to accomplish your tasks.

A **network** is a group (two or more) of computers that are connected by means of some digital media for the purpose of exchanging information or sharing resources. Just as the operating system plays a key role in the management of information and resources on a PC, the operating system also plays a key role in the sharing of information and resources between computers. All versions of Windows were designed to participate in a network but Windows NT was specifically designed as a network operating system.

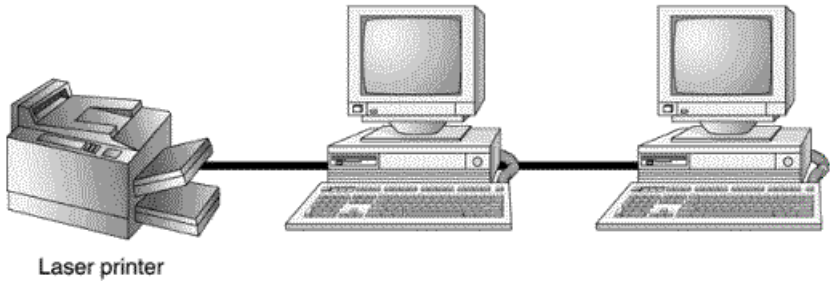


Fig.5.10.1 Printer sharing

The whole purpose of a network is to share resources. Well, what are resources? A resource could be a printer, a drive, a folder, or even a file. In Windows, a computer connected to a network may share its resources with other computers. To do such is to provide a "service" thus, a machine providing a service is acting as a **server**. The resource that is made available to others is fittingly called a **share** (it is usually a folder or a printer that is being shared). When another computer makes use of this service it is acting as a **client**. When you open Network Neighborhood you are looking at all of the computers that your computer is aware of that are acting as servers. If you double-click on one of the listed computers and see folders or printers, you are viewing the shares on that computer.

Shares can be made freely available to all who would conceivably request (in fact, with Windows this is the default when a new share is created), but in most cases this would not be prudent. Therefore, the option exists to give varying levels of access to specific users. Windows provides tools to assign such access settings. The specifications of a user's access, password and other setting is called an **account**. From

then on each individual attempting to access a shared resource must supply some means of identification (like a username) and a password. The computer being accessed will validate the information against the stored account information and only if permission had been specifically granted to that client would he be able to use the share. This is the process of **logging on** in its most fundamental sense.
There are essentially three different ways to use Windows PC's together as a network - **peer-to-peer**, **client/server**, and **domain**. Microsoft generally recommends, for the most part, the domain scheme. Nevertheless, just so that we know a little bit more about domain as the other types of networks have been covered earlier.

5.10.1 Domains

A domain is an arrangement of client and server computers that act together as one system. A domain is referenced by a specific name and all of the computers in it share a single security permissions database. In a domain, a user doesn't log into a specific server but rather logs into the domain as a whole. He may then have access to several different servers all at once.

Using a domain, the various servers can still carry out specialized roles but to a user it all works together as one. Any of the network resources that may be accessed must still be "shared" for others to use but all security is centrally managed making this task workable. The way it is often implemented, when you log on to the Domain, once you are recognized, a special program called a **logon script** starts running and you are granted an **access token**. The logon script does a number of things including connecting you to the network shares that you need access to. The access token is like your personal key that let's you into the resources that you have been granted permission to use. All of this works together so that each user of the network can make use of the many network resources that will assist him in accomplishing his assignment - as if it were all sitting right in front of him. See fig.5.10.2

General Features of Windows NT Server

- Exceptional file and print services
- Support for thousands of client/server applications
- Built-in Security and advanced fault tolerance

- Runs on your choice of scaleable hardware including Intel ®x86, Pentium®, Alpha AXP, MIPS® Rx400, and PowerPC;
- Supports MS-DOS® , Windows®, OS/2® , UNIX and Macintosh®
- Integrates with NetWare®, LAN Manager, UNIX,

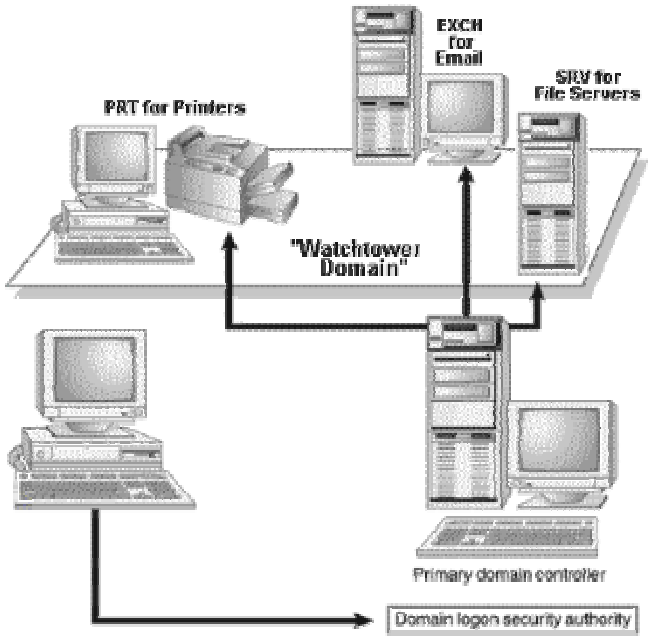


Fig 5.10.2 NT Domains

- and other network systems
- Built-in Migration Tool for NetWare
- File & Print Services for NetWare
- Instantly accessible and up-to-date information
- Hardware autodetect and CD-ROM-based Express Setup
- Easy-to-use graphical environment
- Directory service that aids in the management and control of network resources
- TCP/IP, Macintosh support, and Remote Access Service at no extra charge
- DNS, DHCP, FTP, WWW, Gopher, Wins Services built in

5.10.2 System Administrator functions:

The following are few system administrative functions. They are not exhaustive but knowledge of these operations are essential to a system administrator.

- **Server Manager**

  This tool is for managing servers in a Windows NT domain. The features it provides are,
  Server Manager is started by
  Start->Programs->Administrative Tools->Server Manager
  The Options Menu: This allows you to selectively view according to

  - servers
  - workstations
  - domain members
  - all computers

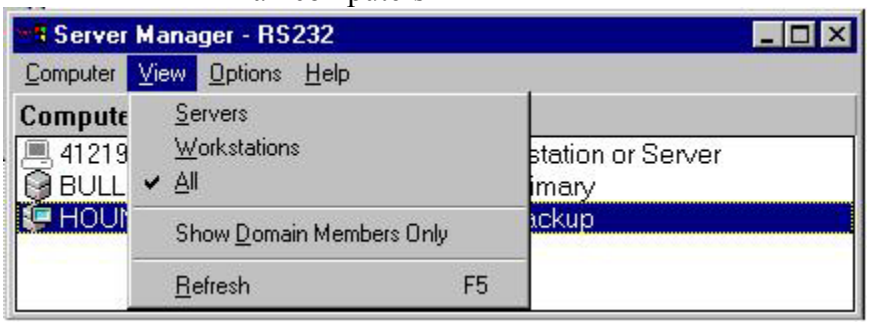


Fig.5.10.3 Server Manager

- **USER ACCOUNTS**

A user account consists of the following information

- username
- password
- group memberships
- rights for using a particular system
- full name
- account description
- list of logon workstations
- allowed logon hours

As can be seen from the window bellow, it is split into two parts, users and groups.

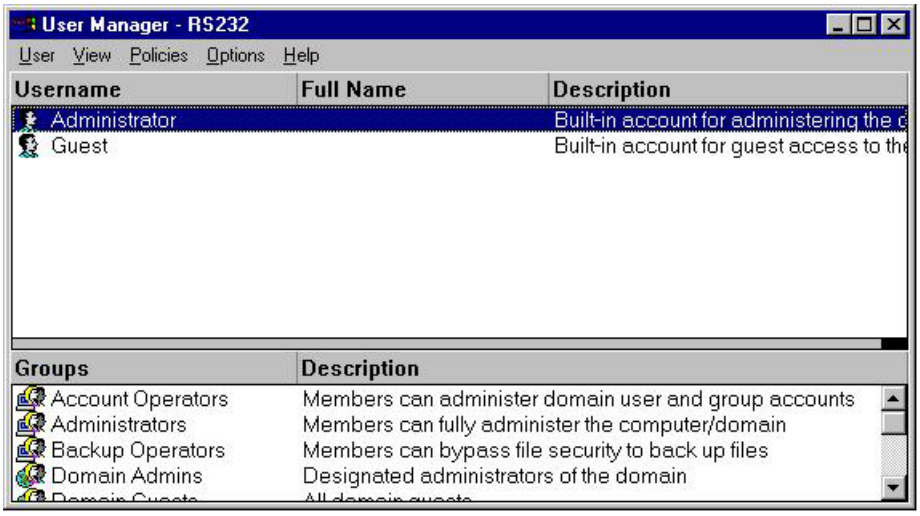


Fig.5.10.4 User Manager

- **Windows NT Server Groups**

Microsoft looked what users do, and created a number of default groups with special permissions that suit these tasks.
Groups

- contain users or other groups
- give members the permissions that belong to the group
- provide easier management of users

There are **THREE** main groups used in Windows NT Server
Local Groups
Are used to assign permissions in the local domain. Can contain users and Global groups, including Global groups from other trusted domains.
Global Groups
Contains user accounts only. Used to export user accounts to other domains, where they can be imported into Local Groups on trusting domains
Special Groups
Used by Windows NT Server for system access, and do not contain user or group accounts

5.10.3 **NTFS SECURITY**

This section discusses Windows NT NTFS file and directory security. Windows NT explorer can be used to set and modify permissions on shares, files and directories.
In order to alter any permissions on a file or directory, you must either have

- full control access to the resource
- change permission rights
- ownership of the resource
- Directory and File Auditing

Windows NT provides auditing of file and directory access on NTFS partitions. When auditing is enabled, an event detailing the type of access is written to the Security log, which can be viewed using event viewer. Both successful and unsuccessful attempts can be audited.

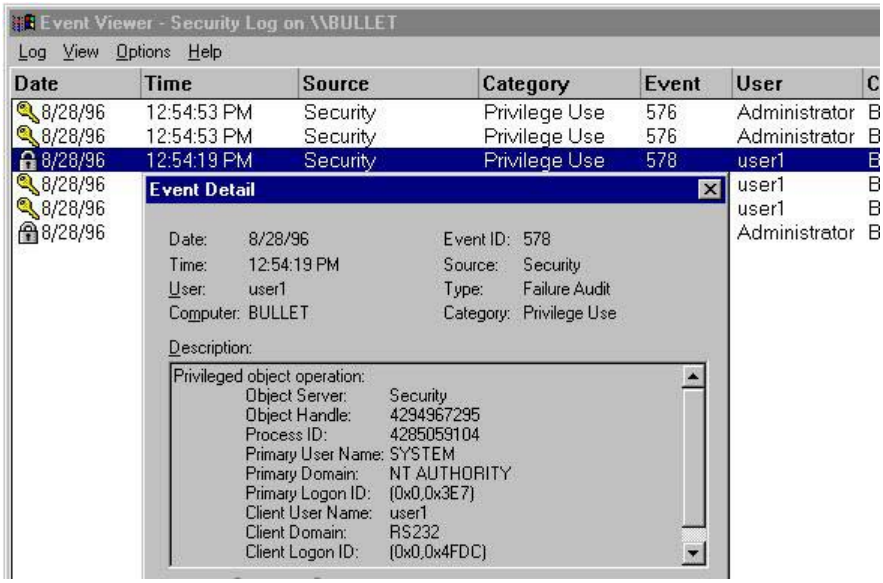


Fig.5.10.5 Event viewer security logon

5.10.4 PRINTING

Windows NT refers to printers as *printing devices*. These are the actual printers from which the paper is output. In contrast, *printers* in Windows NT refers to a software interface. It thus becomes possible to connect multiple printers to a single printing device, and assign different properties to printers, such as priority and hours of use.
Jobs submitted to a printer are normally *spooled* before being sent to the printing device for printing. Printing devices can be connected *physically* [by attaching to a hardware port such as LPT1 or COM1], or *logically* [by attaching to a remote server like \\servername\printername].

A *printer pool* refers to multiple printing devices which are associated with a single printer. Each printer in the pool uses the same printer driver, so all the printing devices in the pool should be the same type.
Under Windows NT, when a user accesses a **remote printer** [a printer on another computer], the printer driver for that printer is downloaded onto the local computer for use. A **local printer** is one which resides on the same computer.
Printers are managed and created using *Print Manager*, accessible from

Start->Settings->Control Panel->Printers

5.10.5 EVENT VIEWER

The Windows NT Event Viewer is under the Administrator Tools folder, and allows the user to look at various events generated by the system, applications, or services, which run on the computer. If auditing has been enabled, then audit events will also be included in the event logs.

Event viewer can view events on either the local computer, or a remote computer to which the user has the required Administrative permissions. There are THREE log files that can be viewed

- **System**
  This log contains events from the Windows NT internal services and drivers, such as failure to start a service.
- **Security**
  This log contains events when auditing is enabled, such as user log on, file and directory access, and printing requests.
- **Application**
  This log contains events generated by applications, such as tape

back up programs, Web servers, or other application programs. The default size of log files is 512K bytes, and log files are overwritten every seven days. This is configurable, and log files can be saved for future analysis in either log, text or comma delimited format.

Because log files can fill up rather quickly, it becomes important to be able to selectively view [filter] the information in the log file. Events can be sorted [by date and time], and filtered [over a specific time period and according to the source and category of event].

The following diagram gives an example of the type of criteria which can be specified when filtering events in a log file.

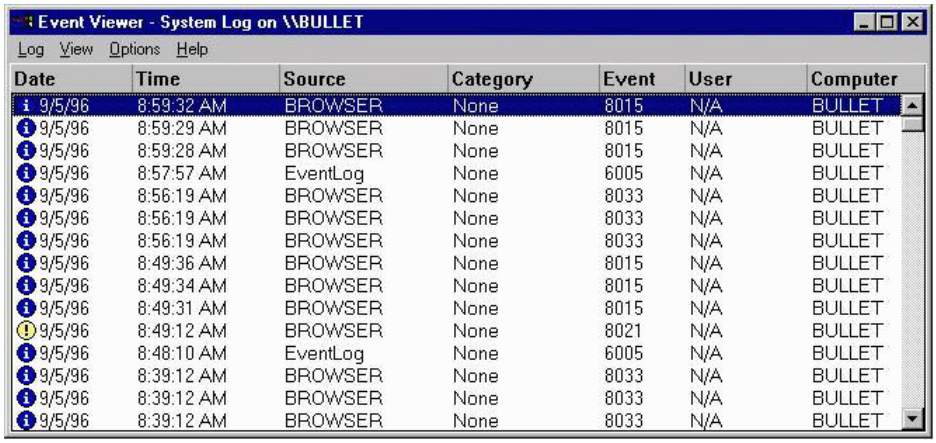


Fig.5.10.6 Event viewer system logon

- **EMERGENCY REPAIR DISK**

When Windows NT is installed, it asks the installer if they wish to create an Emergency Repair Disk. This disk is used to repair missing or corrupt Windows NT files, and restore the registry, which includes the Security Accounts Manager Database, security information, disk configuration and other important information.

To restore this information, it is necessary to boot the computer using Disk1 of the Windows NT setup disks. When prompted at the installation screen, select the option **Press R to repair a Windows NT Installation**, and you will be asked to insert the emergency repair diskette.

This allows you to perform a number of tasks, which include

- Inspecting the registry files
- Inspecting the startup environment
- Verifying the Windows NT System Files
- Inspecting the Boot Sector

- **WINDOWS NT BOOT DISKETTE**

Creating a boot diskette allows an administrator to quickly repair a damaged Windows NT computer which has had the boot sector corrupted. It can be used to replace the files NTLDR, NTDETECT.COM, NTBOOTDD.SYS and BOOT.INI
Any other files cannot be replaced, so in that case, use the emergency repair diskette to restore the missing files.

To create a Windows NT boot diskette [for Intel based computers], perform the following steps

- Format a disk
- Copy the following files to the disk
  NTLDR
  NTDETECT.COM
  BOOT.INI
- Shutdown the computer and restart it with the diskette in Drive A

- **LAST KNOWN GOOD CONFIGURATION**

Often, a user or administrator makes changes to a computers configuration then realizes a mistake has been made, and often, does more damage trying to remove the changes.
When a user logs on to a Windows NT computer, the current configuration information is copied from the registry into a special control set known as *LastKnownGood*. As its name implies, it is the last control set, which was used to successfully boot the Windows NT computer.

When the computer boots up, it is possible to select the *Last Known Good configuration* by pressing the space bar during the boot process

(When the message *Press SPACEBAR for Last Known Good Configuration* is displayed). If changes are made to the computer, which prevent it from restarting [such the removal of a critical driver], this process can be used to restore the system state to that which it was in before the change occurred.

- **AUTOMATIC SYSTEM RECOVERY**

When a fatal error occurs, and Windows NT is forced to shutdown, it is possible to specify additional events, which occur. This information is useful for debugging purposes, as well as restarting the system automatically in the event of a shutdown.

The options are accessed using Start->Settings->Control Panel->System

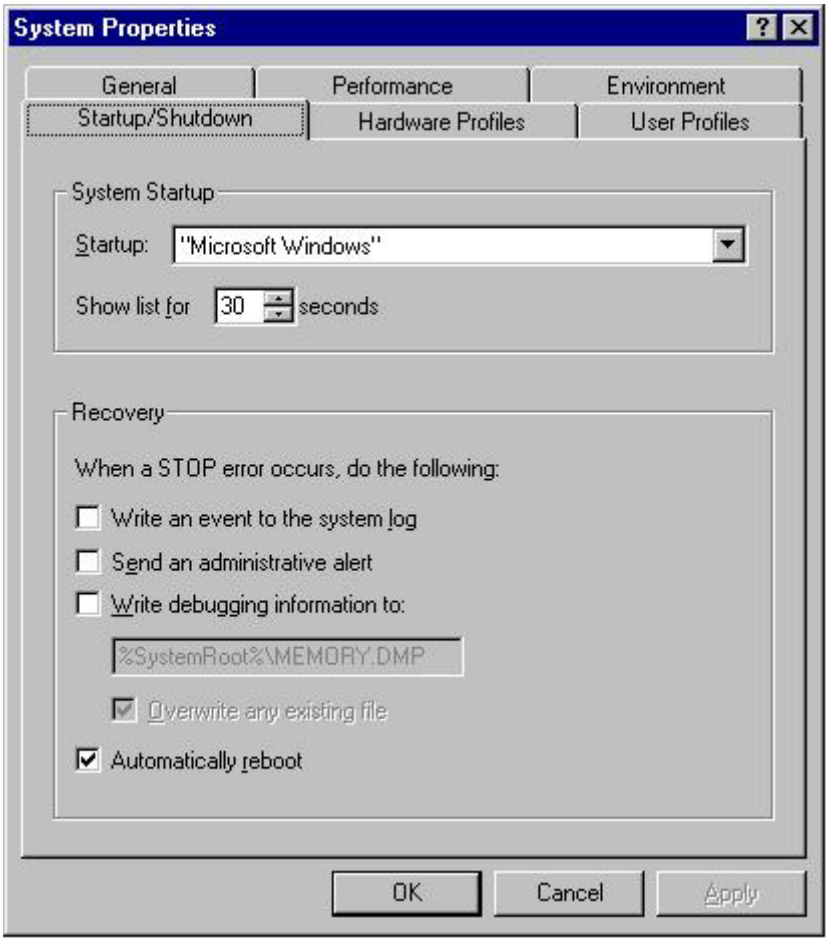


Fig.5.10.7 System properties

Summary:

The core of a network is the network operating system. Just as a computer cannot operate without an operating system, a network of computers cannot operate without a network operating system.

The UNIX operating system was designed to let a number of programmers access the computer at the same time and share its resources.
The operating system coordinates the use of the computer's resources, allowing one person, for example, to run a spell check program while another creates a document, lets another edit a document while another creates graphics, and lets another user format a document -- all at the same time, with each user oblivious to the activities of the others. UNIX systems are usually interconnected using TCP/IP (Transmission Control Protocol, Internet Protocol). This is a protocol mechanism that is widely used by large networks worldwide to interconnect computers of different types

All versions of Windows were designed to participate in a network but Windows NT was specifically designed as a network operating system

Short questions:

1). NOS stands for……
2). State the three basic services of NOS
3). What is ping command?
4). rwx stands for …
5). What is the output for netstat command?
6). What is the main protocol adopted by unix for communication?
7). GUI is acronym for ……
8). In WindowsNTFS FS stands for ……
9). State the purpose of having boot disk
10). List any three salient features of WindowsNT server

Long questions:

1). Discuss in detail about Network Operating System.
2). Render the features of Unix operating System
3). Narrate the networking capabilities of Unix
4). What are the functions of Unix administrator?
5). Describe in detail about arp command

6). Discuss in detail about network security features of Unix.
7). Write short notes on file security features of Unix
8). List the general features of WindowsNT server
9). Discuss about WindowsNT network security
10). Describe the diagnostic tools of WindowsNT

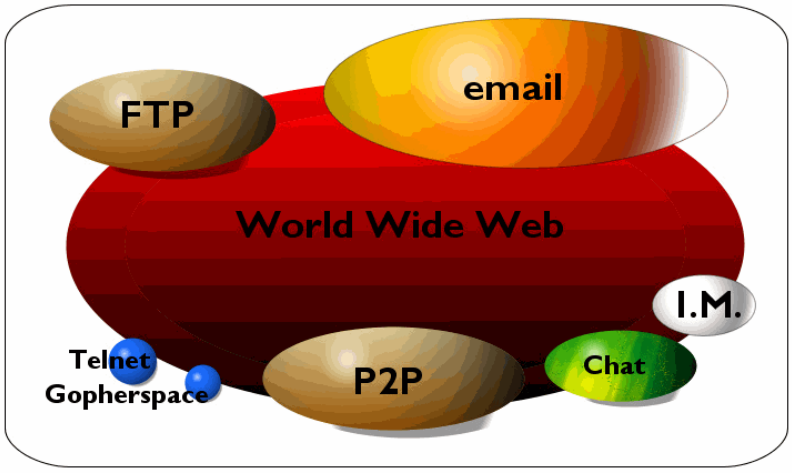


Fig.6.1 Internet services

6.1 E-Mail

Electronic mail was originally designed to allow a pair of individuals to communicative via computer. The first electronic mail software provided only a basic facility: it allowed a person using one computer to type a message and send it across the Internet to a person using another computer.

Current Electronic mail systems provide services that permit complex communication and interaction. For example Electronic mail can be used to:

- Send a single message to many recipients
- Send a message that includes text, audio, video or graphics.
- Send a message to a user on a network outside the Internet.
- Send a message to which a computer program responds.

To appreciate the capabilities and significance of electronic mail, one must understand a few basic facts .The next sections consider how electronic mail appears to a user. Later sections describe how electronic systems work and discuss the impact of electronic mail.

Researchers working on early computer networks realized that networks can provide a form of communication among individuals that combines the speed of telephone communication with permanence of postal mail.

A computer can transfer small notes or large documents across a network almost instantaneously. The Designers called the new form of communication ***electronic mail*** often abbreviated as ***email***. The concept of Email has become extremely popular in the Internet as well as on most other computer networks.

To receive electronic mail, a user must have a mailbox, a storage area, usually on disk, that holds incoming email messages until the user has time to read them. In addition, the computer on which a mailbox resides must also run email software. When a message arrives, email software automatically stores it in the user's mailbox. An email mailbox is private in the same way that postal mailboxes are private: anyone can send a message to a mailbox, only the owner can examine mailbox contents or remove messages.

Like a post office mailbox each email mailbox has a mailbox address. To send email to another user, one must know the recipients mail box address. Thus

- Each individual who participates in electronic mail exchange has a mail box identified by a unique address.
- Any User can send mail across the Internet to another user's mailbox if they know the mailbox address.
- Only the owner can examine the contents of a mail box and extract messages.

To send electronic mail across the Internet, an individual runs an email application program on their local computer. The local application operates similar to a word processor-- It allows a user to compose and edit a message and to specify a recipient by giving a mailbox address. Once the user finishes entering the message and adds attachments, email software sends it across the Internet to the recipient's mailbox.

When an incoming email message arrives, system software can be configured to inform the recipient. Some computers print a text message or highlight a small graphic on the users display (e.g., a small picture of letters in a postal mail box). Other computers sound a tone or play a recorded message. Still other computers wait for the user to finish viewing the current application before making an announcement. Most systems allows a user to suppress notification altogether, in which case the user must periodically check to see if email has arrived.

Once email has arrived, a user can extract messages from his or her mailbox using an application program. The application allows a user to view each message, and optionally, to send a reply. Usually, when an email application begins, it tells the user about the messages waiting in the mailbox. The initial summary contains one line for each email message that has arrived; the line gives the sender's name, the time that message arrived, and the length of the message. After examining the summary, a user can select and view messages on the list. Each time a user selects a message from the summary, the email system displays the message contents. After viewing a message, a user must choose an action. The user can send a reply to whoever sent the message, leave the message in the mail box so it can be viewed again, save a copy of the message in the file, or discard the message.

- A computer connected to the Internet needs application software before users can send or receive electronic mail.
- Email software allows a user to compose and send message or to read messages that have arrived.
- A user can send a reply to any message.

Usually, the sender only needs to supply information for the TO and SUBJECT lines in a message header because email software fills in the date and the senders mailbox address automatically. In a reply, the mail interface program automatically constructs the entire header. It uses the contents of the FROM field in the original message as the contents of the TO field in the reply. It also copies the subject field from the original message to a reply. Having software fill in the header lines is convenient, and also makes it difficult to forge email.

In practice, most email systems supply additional header lines that help identify the sending computer, give the full name of the person who sent the message, provide a unique message identifier that can be used for auditing or accounting, and identify the type of message (e.g., text or graphics). Thus, email messages can arrive with dozens of lines in the header. A lengthy header can be annoying to a recipient who must skip past it to find the body of a message. Software used to read email can make it easier for the recipient by skipping most header lines. To summarize:

- Although most email messages contain many lines of header, software generates most of the header automatically.

- User-Friendly software hides unnecessary header lines when displaying an email message.

6.1.1 E-Mail Operation:

A computer communication always involves interaction between two programs called a client and a server. E-mail systems follow the client-server approach: Two programs co operate to transfer an email message from the sender's computer to the recipient's mail box (transfer requires two programs because an application running on one computer cannot store data directly in a mailbox on another computer's disk). When a user sends an email message, a program on the sender's computer become a client. It contacts an email server program on the recipient's computer and transfers a copy of the message. The server stores the message in the recipient's mailbox.

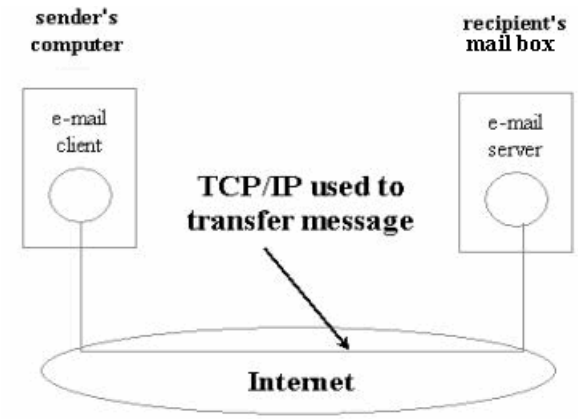


Fig.6.1.1 Email operation

Client software starts automatically as a user finishes composing an email message. The client uses the recipients email address to determine which remote computer to contact. The client uses TCP to send a copy of the email message across the Internet to the server. When the server receives a message, it stores the message in the recipient's mailbox and informs the recipient that email has arrived.

The interaction between a client and a server is complex because at any time computers or the Internet connecting them can fail (e.g., someone can accidentally turn off one of the computers). To ensure that email will be delivered reliably, the client keeps a copy of the message during the

transfer. After the server informs the client that the message has been received and stored on the disk, the client erases its copy.

A computer cannot receive e-mail unless it has an e-mail server program running. On large computers, the system administrator arranges to start the server when the system first begins, and leaves the server running at all times. The server waits for an email message to arrive, stores the message in the appropriate mailbox on disk, and then waits for the next message.

A user who has a personal computer that is frequently powered down or disconnected from the Internet cannot receive email while the computer is inactive. Therefore, most personal computers do not receive email directly. Instead, a user arranges to have a mailbox on a large computer with a server that always remains ready to accept an email message and store it in the users mailbox. For example, a user can choose to place their mailbox on their company's main computer, even if they use a personal computer for most work. To read email from a personal computer, a user must contact the main computer system and obtain a copy of their mailbox.

6.2 File Transfer Protocol (FTP)

Although services like email, Internet fax can be utilized for sending files over the net they are not designed for handling large volumes of data. For sending large volumes of data reliably over the net **File Transfer Protocol (FTP)** is preferred instead.

FTP works in interactive environment. Just type ftp at the DOS command prompt to enter into ftp interactive session. FTP responds to each command the user enters. For example, when a session begins, the user enters a command to identify a remote computer. FTP then establishes a connection to the remote computer. In the same way, to terminate a session user tells FTP to relinquish its connection.

6.2.1 FTP commands

There are around 58 separate commands but the average user need to know only three following basic commands

- **open <name of the ftp computer>:** for connecting to a remote computer.

- **get <filename>:** for retrieve a file from the computer.
- **bye:** Terminate the connection and leave the ftp session.

ftp can be used not only to retrieving files but also for uploading/sending file by using **send** command. Once a connection has established just type the command **send** along with the file name to be sent. A copy of the file will be transferred to the remote computer. Of course, the FTP on the remote site must be configured to allow file storage. Many Internet sites that run ftp allow storage.

6.2.2 FTP File Types

FTP understands only two basic file formats. It classifies each file as either a text file or a binary file. Text file supports ASCII encoding. FTP has commands to convert a non ASCII text file to ASCII text file.

FTP uses classification of binary files for all non text files. For example the following type of files should be specified as a binary files.

- A computer program
- Audio data
- A graphic or video image.
- A spread sheet
- A word processor document
- Compressed files

The compressed file refers to a file, which has been processed to reduce its size by running file compress utility. By using file uncompressing utilities like unzip the original file can be reconstructed.

Choosing between binary and ASCII transfer can be sometimes difficult. When you are unsure about the type of the file choose binary option for transferring the file. If a user requests FTP to perform a transfer using incorrect type the resulting transferred copy may be damaged.

6.2.3 FTP login

The user must login into the ftp site as an authentic user before performing any ftp based transactions. Usually the user will be provided with login name and password. This way the site is protected from malicious users and keeps the data secure.

To make files available to the general public, a system administrator can configure FTP to honor **anonymous** FTP. It works like standard FTP, except that it allows anyone to access public files. To use anonymous FTP, a user enters the login as anonymous and the password as guest. Few sites may prompt for the user's email address just in case of any errors like log failures so that those error messages can be emailed.

Most users invoke FTP through a web browser so that the ftp transactions can be made in a graphic user interface (GUI) environment

6.2.4 FTP operation

FTP operation is also based on client server model.

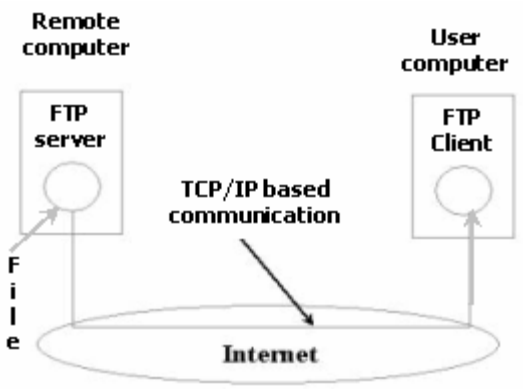


Fig.3.9.1 FTP operation

The user invokes a local FTP program or enters a URL that specifies FTP. The local FTP program or the user's browser becomes an FTP client that uses TCP to contact an FTP server program on the remote computer. Each time the user requests a file transfer, The client and server program interacts to send a copy of the data across the Internet.

The FTP server locates the file that the user requested, and uses TCP to send a copy of the entire contents of the file across the Internet to the client As the client program receives data, it writes the data into a file on the user's local disk. After the file transfer completes, the client and server programs terminate the TCP connection used for the transfer.

Here is an example typical FTP session:

$ ftp plaza.aarnet.edu.au
Connected to plaza.aarnet.edu.au.

```
220 plaza.aarnet.EDU.AU FTP server (Version wu-2.4(2) Fri Apr 15
14:04:20 EST 1994) ready.
Name (plaza.aarnet.edu.au:jphb): ftp
331 Guest login ok, send your complete e-mail address as password.
Password:
230-
230-This is the AARNet Archive Server, Melbourne, Australia.
230-
230-
230-The disk that failed back in September is still not back on-line.
230-As a consequence of this, we are only shadowing files modified in
230-the last 100 days on many of the more popular archives. We
apologise
230-for this inconvenience.
230-
230-Local time is Tue Jun  4 17:46:00 1996
230-
230-Please read the file /info/welcome-ftpuser
230-  it was last modified on Fri Apr 22 14:47:05 1994 - 774 days ago
230 Guest login ok, access restrictions apply.
ftp> pwd
257 "/" is current directory.
226 Transfer complete.
214 bytes received in 0.018 seconds (11 Kbytes/s)
ftp> cd rfc
250 CWD command successful.
ftp> get rfc1048.txt.gz
200 PORT command successful.
150 Opening ASCII mode data connection for rfc1048.txt.gz (5141
bytes).
226 Transfer complete.
local: rfc1048.txt.gz remote: rfc1048.txt.gz
5161 bytes received in 1.6 seconds (3.2 Kbytes/s)
ftp> quit
221 Goodbye.
```

….

6.3 TELNET

The Telnet protocol is often thought of as simply providing a facility for remote logins to the computer via the Internet. This was its original purpose although it can be used for many other purposes.

It is best understood in the context of a user with a simple terminal using the local telnet program (known as the client program) to run a login session on a remote computer where his communications needs are handled by a telnet server program on the remote computer. It should be emphasized that the telnet server can pass on the data it has received from the client to many other types of process including a remote login server.

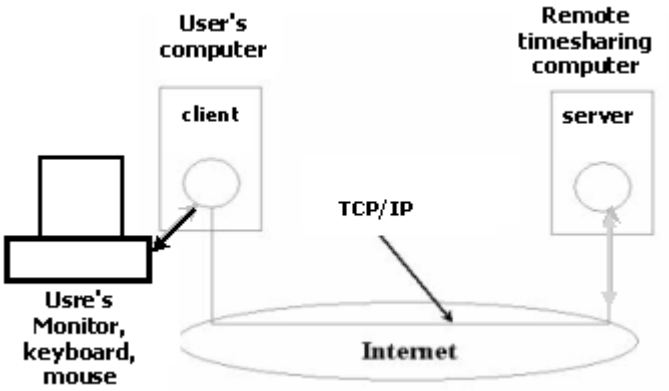


Fig 6.3.1 Telnet session

Once connection has been established between the client and server, the software allows the user to interact directly with the remote computer's operating system. For all user's inputs the server sends output and displays on user's screen.

After a user logs out of the remote computer, the server on the remote computer terminates the Internet connection informs the client that the session has expired and control of the keyboard, mouse and display returns to the local computer

The remote access by telnet has three significant reasons. It makes computation remote from the user. Instead of sending a data file or a message from one computer to another, remote access allows a program to accept input, process it and send back the result to the remote user. Secondly, once user logs in to the remote computer the user can execute any kind of program residing in the remote server. Finally users working in heterogeneous platforms telnetting may become a common interface for different machines.

Here's an example of a telnet session to osmania

$ telnet
telnet> toggle options
Will show option processing.
telnet> open osmania
Trying 202.54.70.200
Connected to linux osmania
Escape character is '^]'.

6.4 Gopher

Gopher is a protocol system, which in advance of the World Wide Web, allowed server based text files to be hierarchically organized and easily viewed by end users who accessed the server using Gopher applications on remote computers. Initially Gopher browsers could only display text-based files before developments such as HyperGopher, which were able to handle simple graphic formats though they were never used on a widespread basis as by this time the World Wide Web and its Hypertext Transfer Protocol (HTTP) were gaining in popularity, and had similar and more extensive functions.

6.4.1 Gopherspace

Gopherspace is a term used to describe the aggregate of all the information on the thousands of Gopher servers in the world. This information consists of individual files (abstracts, full-length documents or papers, lists, and other file types) organized as a hierarchy of subject categories that can be limited to one server or span multiple Gopher servers. Gopher text files are plain files that lack the kinds of formatting control and font variation that HTML files have. One can think of gopherspace as that portion of cyberspace that is accessible through Gopher servers.

Users of most Web browsers will find that their Web browser also includes a Gopher client. This means that you can go directly to any Gopher server from your Web browser providing you know the server's address.

6.5 Messaging / Instant Messaging:

There is no doubt that the Internet has changed the way we communicate. For many of us, e-mail has virtually replaced traditional letters and even telephone calls as the choice for correspondence. Every day, billions of e-mail messages are sent out. E-mail has been the most rapidly adopted form of communication ever known. In less than two decades, it has gone from obscurity to mainstream dominance.

In our fast-paced world, sometimes even the rapid response of e-mail is not fast enough. You have no way of knowing if the person you are sending e-mail to is online at that particular moment or not. Also, if you are sending multiple e-mails back and forth with the same person, you normally have to click through a few steps to read, reply and send the e-mail. This is why instant messaging (IM) has gained popularity.

Instant messaging allows you to maintain a list of people that you wish to interact with. You can send messages to any of the people in your list, often called a buddy list or contact list, as long as that person is online. Sending a message opens up a small window where you and your friend can type in messages that both of you can see. Most of the popular instant-messaging programs provide a variety of features:

- **Instant messages -** Send notes back and forth with a friend who is online
- **Chat -** Create your own custom chat room with friends or co-workers
- **Web links -** Share links to your favorite Web sites
- **Images -** Look at an image stored on your friend's computer
- **Sounds -** Play sounds for your friends
- **Files -** Share files by sending them directly to your friends
- **Talk -** Use the Internet instead of a phone to actually talk with friends

- Streaming content - **Real-time or near-real-time stock quotes and news**

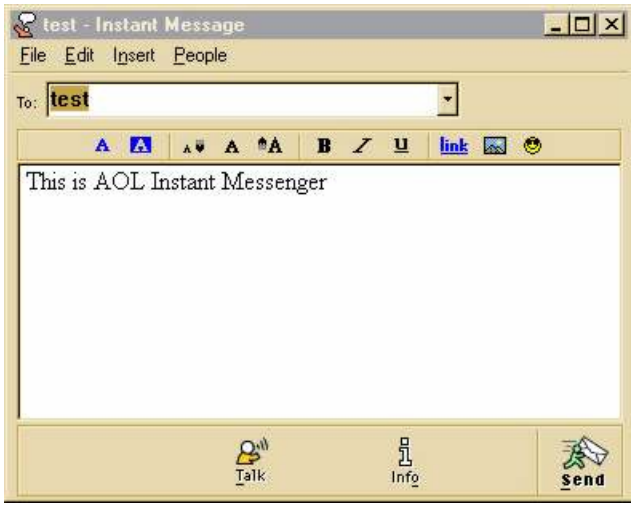


Fig.6.5.1 The most popular AOL Instant Messenger

Before the Internet became popular, a lot of people were already online through the use of bulletin boards and online services. A bulletin board is comparable to a single, isolated Web site that you reach using special communications software and a modem. You create an entry in the software for the bulletin board that contains the board's direct phone number and any special parameters for connecting to the computer hosting the bulletin board. Once connected to the board, you normally use a series of menus to navigate through the board's contents. To reach another board, you have to disconnect from the first board and dial up to the other one.

Major online services, such as America Online (AOL), Prodigy and CompuServe, were the main way that ordinary people could connect and communicate with each other online. Think of an online service as a very sophisticated bulletin board. Whereas most small bulletin boards use standard communications software, online services provide a complete application that includes the communications software necessary to connect to their service. This application also includes the actual interface that you use once you are online and connected to the service. This allows the online service to create a very sophisticated and targeted experience for their users.

Probably one of the biggest attractions of the online service model is the community that it builds. AOL is considered the pioneer of the online community. AOL provides its users with the ability to talk in real-time with each other while they are online through the use of chat rooms and

instant messages. A chat room is software that allows a group of people to type in messages that are seen by everyone in the "room," while instant messages are basically a chat room for just two people.

In the early 1990s, as people began to spend increasing amounts of time on the Internet, creative software developers designed software that could reproduce some of the aspects of an online service. Chat-room software was developed and set up on Web servers, used by sites like TalkCity.

6.6 Web Browsers

Simply putting, a browser is a program that reads HTML (Hyper Text Markup Language, the programming language of the web) and displays it to the viewer.
While there is currently one recognized standard language used to write web pages (HTML 4), there are a myriad of browsers available to view it with. Choosing the right one for your individual needs can help maximize your web experience, which will also cut down on installations and un installations.

Currently the two most popular browsers are **Microsoft Internet Explorer,** and **Netscape Navigator. Microsoft Internet Explorer** is by far more widespread in use and is one of the most powerful browsers available. **NCSA's Mosaic** was one of the first popular browsers to gain wide use and supports most HTML functions but not the newest attributes like frames or animated images.

6.7 Internet Explorer Basics

When Internet Explorer is first opened up on your computer, the main screen of the program will appear. This main window has many parts to it, these parts are described in detail below.

- The "Title Bar" at the very top of the window tells you what the title of the page you are viewing is. The "Title Bar" will also tell you what Internet Explorer application is currently active.

- Directly under the "Title Bar" is the "Main Menu Bar". This bar has many different sub-menus, which control all options, functions, and commands for the entire Internet Explorer

program. Some of the browsing controls can also be found in these sub-menus.

- Beneath this menu is the "Internet Explorer Toolbar". This toolbar contains all of the most frequently used commands and all of the browsing functions. (See the next section for more details)

- Under the toolbar is the "Address Bar". This will tell you the exact HTTP/URL location of the page you are currently viewing. You can also type a Web address directly into this bar and then press enter to go to that site.

- Below the "Address Bar" is the "Link Bar". These buttons will take you to pages at Microsoft's Main home site where they have applications and information specifically designed for your easy use.

- Underneath the "Link Bar" is the "Main Browser Window". This window will display all of the information that is located at the Web site you are currently located at. Any text, images, movies, animation, links, or any other application files will be shown in this window. The scroll bars located on the right side and on the bottom of this window allow you to continue viewing the page you are located at even when the page is too large to fit in your screen.

- The very bottom of the page is the "Status Bar". This bar tells you what the progress of the browser is while it downloads files to the page, where links go to when you move over them, whether or not a document is secure, and any other information that the program feels is necessary for you to know.

The Main Explorer Toolbar

Fig.6.7.1 Explorer tool bar

The main toolbar is composed of eleven different buttons. Each of these buttons has a different function and purpose in Internet Explorer. The individual buttons will each be discussed in the following sections.

1. **The Back Button:** This button will take you back to whatever document you were previously viewing. Pressing it immediately takes you back one document. If you have browsed many pages, or are well into a multi-page document, pressing it repeatedly will continue to back you up one page at a time. Once you reach your starting location, it will be grayed-out and unavailable.

2. **The Forward Button:** This button will take you forward to the next document if you have previously browsed multiple documents and had then backed-up to the page you are currently viewing. (If you have not backed up at all, the forward button will be grayed-out) Pressing it repeatedly will continue to move you forward one page at a time. You can move forward until you reach the last page that you had browsed, at which time the forward button will be grayed-out.

3. **The Stop Button:** The stop button stops ANY current operations by Internet Explorer. It will stop any type of file from loading. It can also be used to stop animations from continuing once a page is loaded. If you press it before a page has finished loading, the page will display everything it had finished loading before the stop button was pressed. If a document is completely loaded and there are no animations, movies, or other files still running, the stop button will have no immediate function.

4. **The Refresh Button:** This button will reload the current document that you are viewing. It is useful if the page updates very frequently so that you can view these changes as soon as they are available. If you are loading a document and the transfer was interrupted, you can reload the full document again by clicking here.

5. **The Home Button:** This button will return you to the page you have selected as the default start-up page for Internet Explorer. It will not take you back to the beginning of your web browsing; it will just return you to your home location from where you are. If you press back after reaching your home page, you will go back to the page you left after you hit the Home button.

6. **The Search Button:** This button will take you to the page you have selected as the default Web search page for Internet Explorer. If you have not selected a page it will take you to Microsoft's default search page.

7. **The Favorites Button:** This button will open up the Favorites menu. You can choose a favorite that you wish to go to from the list, add a favorite to the list, or organize your favorites from this menu.

8. **The Print Button:** The print button will bring up a Print dialog box. In the box you can decide if you would like to print the contents of the page you are viewing, how many pages you will print, and also how many copies you will print. Keep in mind that if you try to print a page that is graphics intensive, you will need a printer that is capable of printing graphics. Also, the more graphics and pages a Web site has, the longer it will take to print.

9. **The Font Button:** Pressing this button causes Internet Explorer to cycle through the available font sizes. This button is useful if the text is too small to read, or too large to fit comfortably in the window.

10. **The Mail Button:** This button will open into a drop down menu from which you can select to read or send E-Mail. You can also open up your newsgroups from this menu.

11. **The Edit Button:** This button will ONLY be on your toolbar if you have a Windows system Web editor (such as Microsoft FrontPage or Microsoft Word) installed on your computer. If you press this button, it will launch that editor and open the document you are currently viewing in it.

Beginning Basic Browsing

Your first time that you browse the web you may have some difficulty. Efficiently browsing the Web is just like any other complex task in life, it takes practice to be good at it. Internet Explorer has some built-in features, which will help to make it easier for you to browse the web. The fastest way to get to a place that you can search from is to click on the "Search" button on the Internet Explorer main toolbar. This button will take you to a document within Microsoft's home site. On this document you will find a choice of categories to look through and a list Search Engines to use. A Search Engine is a application that will attempt to find any documents that contain the subject or phrase that you enter into the search parameters. You can also browse through the categories of Web sites that the search engines have already organized for you.

Another important thing to remember when you first begin browsing the web is that if you know the Web address of a site, you don't need use a search engine to find the page you wish to visit. Go up to the "Address Bar" near the top of the page, and click on it. Now you can type in the Web address of the site you want, and then press enter. Internet Explorer will go to this site directly from whatever document you were currently viewing. This is much faster than going to a search engine and trying to locate the site you want in their directories, or searching for it with a query. (Address Bar shown below

Fig.6.7.2 Explorer address bar

- **Viewing Documents While Not On The Web**

Internet Explorer is capable of displaying HTML documents and images even if you are not connected to the Internet. Go to the file menu from the main menu bar. From this menu select "Open", the open dialog box will appear. (You can also press CTRL-O from the main Explorer window to access this box) In this dialog box, you can type in a Web address to access a page on the Web. Since we are not on the Web, click the "Browse" button to look at files on the hard drive. Select the type of file you want to open from the drop-down menu at the bottom of the box. After you have selected the file type, go to the directory that contains this file. Select the file and then click "Open". The document, image, movie, or sound file you have selected should now be viewable in Internet Explorer.

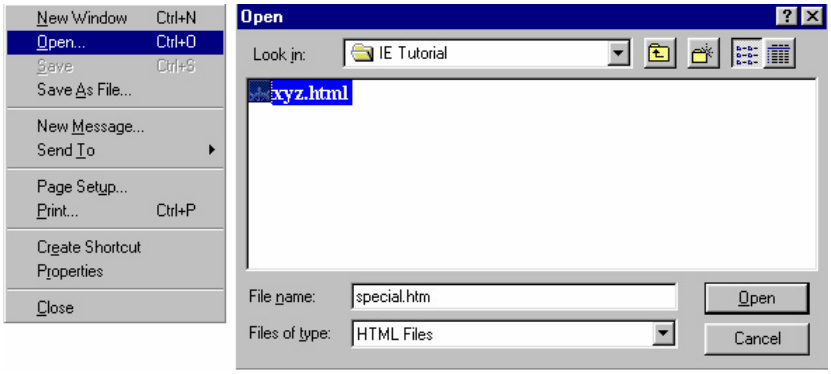


Fig.6.7.3 Opening a html file

- **Printing Web Documents**

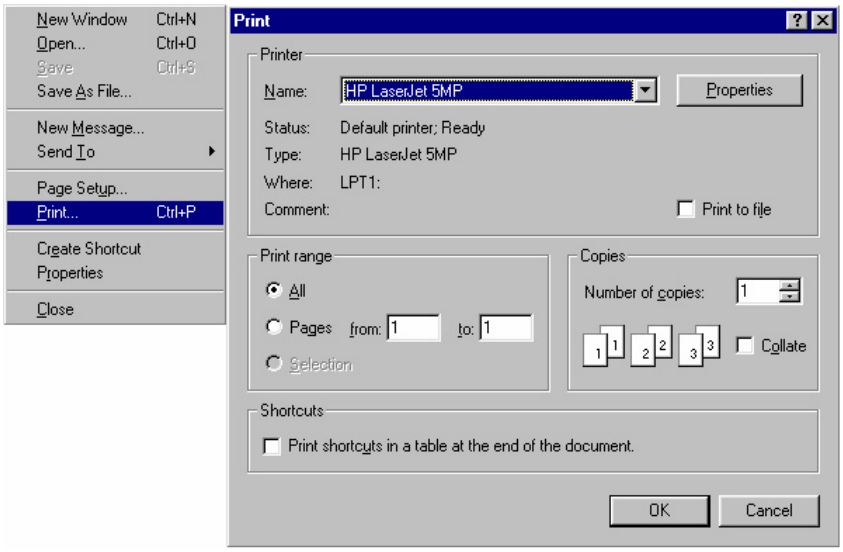


Fig.6.7.4 Printing the contents

If your computer is connected to a printer, you can print out any Web document that you wish whether you are viewing it on the Web, or if you are just viewing it from your hard disk. Go to the file menu from the main menu bar. From this menu select "Print", the Print dialog box will appear. (An easier way to open this box is to simply click the "Print" button on the main toolbar or to press CTRL-P) In this dialog box you can decide how you would like to print the contents of the page you are viewing, how many pages you will print, and how many copies you will print. Keep in mind that if you try to print a page that is graphics intensive, you will need a printer that is capable of printing graphics. Also, the more graphics and pages a Web document has, the longer it will take to print.

- **Tips For Doing Web Searches**

When you are using a search engine to find something on the Web, it helps to find ways to narrow your search so it is faster and more efficient. Most of the search engines use the same set of operators and commands in their search vocabulary. The following are the most commonly used operators and a brief description of each. These would be used when typing in a keyword or phrase into a search engine.

- **Quotes (" ") :** Putting quotes around a set of words will only find results that match the words in that exact sequence.

- **Wildcard Use (*) :** Attaching an * to the right-hand side of a word will return partial matches to that word.
- **Using Plus (+) :** Attaching a + in front of a word requires that the word be found in every one of the search results.
- **Using Minus (-) :** Attaching a - in front of a word requires that the word not be found in any of the search results.

○ Speeding Up Browsing

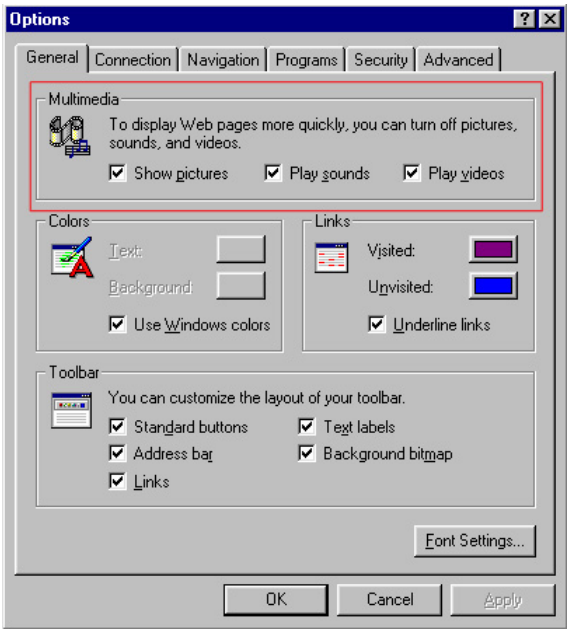


Fig.6.7.5 Enhancing browser speed option

There are many ways to make the browsing process much quicker and easier. One of the main ways that you can improve the speed of the computer when loading a document is to disable the automatic loading of images. Go to the main menu of Internet Explorer, and from the View sub-menu, select "Options". From the Options dialog box, select the "General" folder tab at the top of the box. In the multimedia section you can select whether or not Internet Explorer loads an image, sound file, or movie. If you want a type of file to be automatically loaded, place a check mark in the appropriate box. If you want the images disabled, click to remove the check. Now whenever Internet Explorer loads a document that has images, a small icon will appear where each image is located on the page. If you wish to view the image at that location, right-click on the image area and then select "View Image" from the menu. (The

multimedia section is outlined in the first image for your convenience, and the upper-right image shows what images look like when they do not load).

- **Saving Files After Viewing Them**

Frequently on a Web Page, you will find links that you can click on which will activate a selected file. Other times, the appropriate plug-in will be engaged when you click an application file. Once you have heard the sound, watched the video, or read the text, you may want to save the file on your computer.

- Most files available for viewing allow you to "Right-Click" on them which displays a menu box.
- From this box select "Save As", "Save Picture As", or whatever happens to fit the type of file you have just seen or heard.
- Choose where on your computer the file will be saved and give it a name.
- Click "Save" to begin saving the file. In the example below, the Eastern Illinois University logo was viewed. A "Right-Click" on it brought up a menu box. Finally, it will be saved to the hard drive.

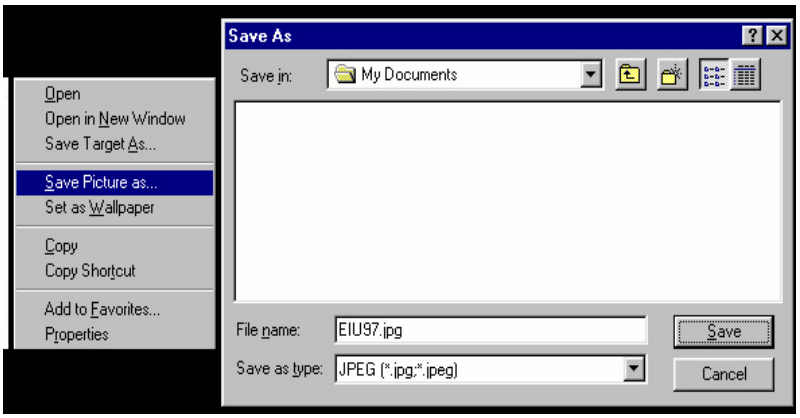


Fig.6.7.6 Saving pictures with Save As option

- **Downloading Files From Links**

Many Web Pages have links to files that you can view such things as Images, Sounds, or Movies. Suppose that you don't want to look at them now. You can always download them directly from the links and view them at a later time.

- "Right-Click" on the file that you want to download.
- In the menu box that pops up, select "Save Target As".
- A Save As dialog box will appear. You can select what name the file will have, and the location to where it will be downloaded. A shortcut to get to the Save As box is to hold "Shift" and "Left-Click" on the link you want to download. After you have selected the name and destination, click "Save". In the example below, suppose you would like to download the wave file called "Door.wav". First, a "Right-Click" on the filename will bring up the menu box. Next, choose "Save Target As" a select you desired location from the Save As dialog box. Finally click "Save" and download the wave file.

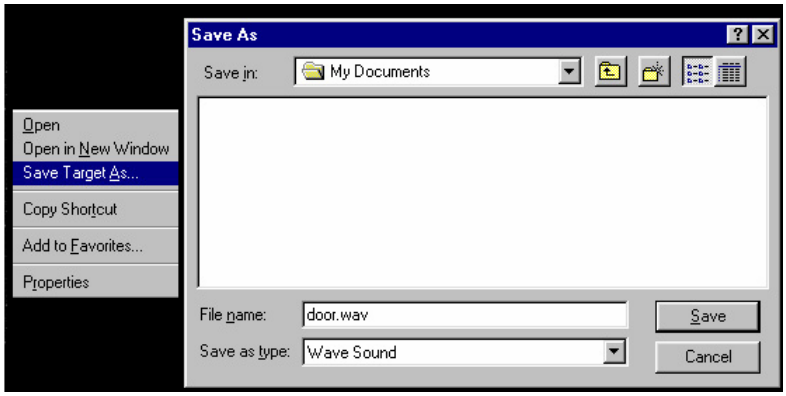


Fig.6.7.7 Saving a target

6.8 Netscape Navigator

Netscape Navigator is currently one of the popular commercial browsers used to surf the Internet. It's been written that nearly 75% of

those who currently surf are using at least some version of this company's browsers. Netscape Communications, founded by former students from the University of Illinois NCSA group, which puts out the Mosaic Browser, has been a leading innovator in web technology. Netscape Navigator, which actually started it's life as Mosaic, has brought many versatile features to web browsing such as frames, plug-ins, and JavaScript, some of which are now HTML standards. Netscape adds more reliable JavaScript support, a wider variety of plug-ins, more functionality to frames and tables, and improved security. Internet mail and news is standard and Netscape also supports real-time telephone functions through the available Cool Talk® plug-in. Netscape is available for Windows, Mac, and Unix systems.

Fig.6.8.1 Net-Scape Navigat-or

6.9 Netscape Communicator 4.0

Netscape Communicator 4.0 is an integrated "suite" of Netscape Internet components all brought together in one convenient package. All can function separately or together to form a highly versatile Internet browsing and composition tool. Like Netscape 3.0, Communicator features the latest version of the very popular Netscape Navigator and includes an Internet composition and publishing program called Composer, internet news and mail functions, and several business add on components as well. Netscape has recently released version 4.01, which features security and other bug fixes.

Communicator 4.0 is available in two versions:

Standard and **Professional**. The standard edition includes:

Fig 6.8.2 Standard Communicator 4.0 Components

Netscape Navigator 4.0 - Communicator 4.0 features the latest browser release from Netscape. Riding the wave of their leadership in browser functionality, Navigator 4.0 adds on to the features of version 3.0 as well as adds better security and an improved user interface.

Composer - Communicator comes with a web-authoring tool much like Microsoft's Front Page program. Composer is a visual web authoring tool and works much like standard word processor programs allowing you to visually compose a web page as opposed to the standard coding, checking and frequently updating as you would with an HTML editor (the way this page was created for example). For those looking to put up a home page with little to no HTML experience, this is a practical and very helpful tool, as no knowledge of HTML is required.

This editor allows users to add links, images, background images, format pages using colors for text, links, background, etc. Users can also create tables, and publish directly to the web (or upload to a web site directly from Composer). The drawbacks are that it does not support Frames, scripting languages, or dynamic HTML, but these are features are still pretty much for advanced page authors anyway.

- **Collabra** - Netscape Communicator includes an improved messaging center called Collabra. This component acts as an Internet mail center gathering news group messages as well as users Internet mail. Users can use Collabra to subscribe to numerous Internet news groups, keep track of postings, as well as compose their own postings.

- **Messenger** - Like Navigator 3.0, Communicator features an integrated mail component known as Messenger. This component basically allows the user to send and receive E-mail through the users service provider.

Netscape Communicator is available for Windows, Mac, and Unix systems

6.10 NCSA Mosaic

NCSA's Mosaic was one of the first browsers put out for commercial use. Developed at the University of Illinois by the National Center for Super computer Applications, or NCSA, Mosaic 3.0, though not fully supportive of newer HTML standards, is a good web browser. What it lacks in support for frames, animated images, plug-ins, and scripting languages, it makes up for in its friendly user interface. Version 3.0 includes powerful tools like "Manager Mode" as well as an extensive web and browser toolbar. Though it does not support plug-ins, Mosaic does work with MIME programs, or external programs that play multimedia, such as Microsoft's AVI player. Mosaic does not participate in the so-called "browser wars", so it doesn't have any non-standard functions, just great user features. An interesting tidbit is some of the people who developed Netscape Navigator actually have their roots in the University of Illinois.

- **Mosaic 3.0** has a friendly user interface and loads of features to help navigate the web with. Even though this browser doesn't support many of the newer HTML standards, I do enjoy using it from time to time myself.

- **"Manager Mode"** is a great feature that lets you view you current History List, Hot lists, Cache files, and even document sources without having to open an external window. It does this by dividing the browser window into two frames, one being the web page, the other you Manager window. A very cool feature I wouldn't mind seeing on one of the bigger browsers.

This browser does not support independent text commands which are tags that do not appear in the document head. For non web authors, that means that any text attributes not specified in the very start of the web page are ignored. This is a problem on a page like Zenheffville's home page. No Frames site where there are many different font color types and sizes. Newer browsers do recognize text tags throughout the document.

Mosaic is freely available on the net.

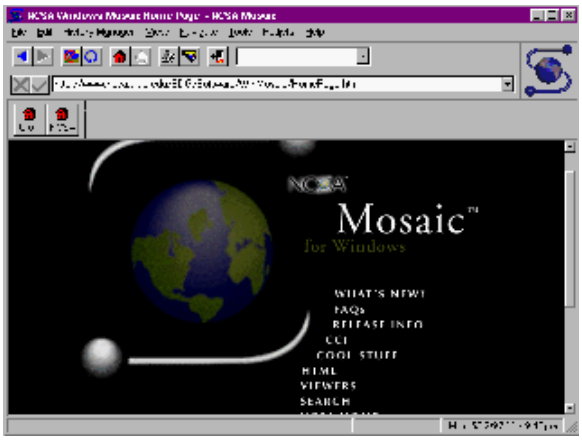


Fig.6.9.1 Browser page

Summary:

Apart from World Wide Web Internet applications include email, ftp, telnet, messaging etc which are equally popular.

E-mail Electronic mail was originally designed to allow a pair of individuals to communicative via computer. The first electronic mail software provided only a basic facility: it allowed a person using one computer to type a message and send it across the Internet to a person using another computer.

Although services like email, Internet fax can be utilized for sending files over the net they are not designed for handling large volumes of data. For sending large volumes of data reliably over the net **File Transfer Protocol (FTP)** is preferred instead.
The **Telnet** protocol is often thought of as simply providing a facility for remote logins to the computer via the Internet. This was its original purpose.

A browser is a program that reads HTML (Hyper Text Markup Language, the programming language of the web) and displays it to the viewer. Currently the two most popular browsers are **Microsoft Internet Explorer,** and **Netscape Navigator. Microsoft Internet Explorer** is by far more widespread in use and is one of the most powerful browsers available. **NCSA's Mosaic** was one of the first popular browsers to gain wide use initially.

Short questions:

1). State the various services available on the Internet.
2). What is E-mail?
3). State one advantage of FTP?
4). How to end a FTP session?
5). What is remote login?
6). What is the common protocol associated with all Internet services.
7). What is a browser?
8). Explain the function of refresh button
9). State the purpose of back button.
10). What is instant messaging?

Long questions:

1). Enumerate various services offered by Internet and discuss briefly about each of them.
2). When FTP is needed?-Explain in detail
3). Narrate the FTP operation
4). How telnet session initiated? -Describe its operation.
5). Discuss in detail about messaging.
6). Depict various features of a typical browser.
7). List the various browsers that are available today. Describe any one them in detail
8). With the help of suitable illustrations , show how to increase the browser speed
9). Which is your favorite browser? Why?
10). Describe the Netscape browser.

INTERNET AND E-MAIL
PRACTICALS
DOCUMENTATION

Written by
Dr.P.Premchand
Dept. of CSE, College of Engineering,
Osmania University, Hyd 500007
Edited by
K.Goverdhan Naidu
Jr.Lecturer, PCR Govt. Junior College,
Chittor

Internet & e-mail Lab

Aim:

To become familiar with the network settings required to connect a PC to a local area network and to gain access to the Internet or intranets. In this lab, you will find a workstation's/server's network settings, network interface card (NIC) configuration and drivers and TCP/IP protocol settings for a typical Windows client workstation.

Tasks:

1. Connect and power up a workstation, including monitor, mouse, and keyboard.
    - If the Windows password dialog box comes up, press **ENTER**. Do NOT cancel.
    - Ask the teacher if you need a bootable disk.
2. Use Control Panel to determine the workstation computer name, network client, the internet protocols in use, and information about the NIC:

    - Click on **Start**
    - Select Settings and then **Control Panel**.
    - Double click the **Network icon**.
    - Click the Identification Tab at the top of the window to find the computer name and workgroup name.

Kindly make the following observations:

Workstation Name	
Workgroup Name	
User Login	
Password protected? (YES/NO)	

- Click the **Configuration** Tab and note what networking components are installed and take down the descriptions that appear when each is selected.

General Component	Specific Component	Description
Network Client Type (Computer icon)		
NIC installed (Network card icon)		
1st Protocol installed (Twisted cable icon)		
2nd Protocol installed		
Other network components		
Other network components		

- Use Control Panel to check the IP address:
    - From the **Control Panel**, double click the **Network icon**.
    - Click on the **TCP/IP** protocol while on the **Network Configuration** tab.
    - Click the **Properties** button.
    - Make sure the IP Address tab is selected.
    - What two choices are available here? Write down their descriptions.

- Use winipcfg.exe utility to check network settings:
    - Click on Start and Run.
    - Type in WINIPCFG in the dialog box and press ENTER.
    - Click on More Info >>.
    - Record the Adapter Address:
    - Record the IP Address:
- Switch off the computer.
- Write down the following data pertaining to your system
    - IP Address
    - TCP/IP
    - MAC address (Adapter Address)
    - Protocol

- **Installing the Network interface card:**

Aim:

To remove and to install a Network Interface Card (NIC) in a PC.

Tasks:

1. Prepare to remove the NIC:

    1. Ground yourself by touching something metal, other than the computer.
    2. Turn off your computer and unplug the power cable.
    3. Remove the cover and call the teacher over to show her the NIC.
    4. Ground yourself by touching something metal; the case is OK, if it's not touching the rest of the computer.

2. Remove the network card:
    1. Remove the screw holding the card to the case.
    2. Handle the top corners of the network card with both hands and gently rock the card front to rear to remove it from the expansion slot.
    3. Trade network cards with your neighbor.
    4. Record the type of card here:

3. Install the network card

    1. Again, handle the top corners of the network card with both hands.
    2. Align the tabs of the network card with the slot and gently rock the card front to rear to insert it into the expansion slot.
    3. Finally, secure the card to the case with a screw.
    4. Replace the cover of the computer case and then restart the computer. The Windows 98 setup hardware detection will automatically determine the adapter driver for your network card. Windows 98 may ask you to supply your computer name and workgroup name. Select a computer name for your PC and use a specific workgroup name provided by your lab instructor.

4. See if the installation worked:

    1. Double-click on the Network Neighborhood icon on the desktop. If you find your computer's name displayed in the window, the network card is working properly. If you do not, then Windows 98 may have installed an incorrect driver for your network card. If so, you will need to do the following steps to add an adapter driver:
    2. Click the Start button, select Settings, then select Control Panel.
    3. Double-click the Network icon. A network dialog box will appear.
    4. Click on the Add button. Select adapter and click on the Add button once again.
    5. Choose to find the drivers in C:\win98.
    6. Windows 98 may ask you to reboot your system. After you restart the computer, follow the instructions in the beginning of this exercise to check whether your network card is working properly.

5. Check the installation a second way:

    1. Go to the Control Panel
    2. Double-click on System and then Device Manager
    3. Double click on Network Adapters and then right click the NIC adapter in use.
    4. Click Properties to see if the device is working properly.

NOTE: If there is a problem with the NIC or driver, the icon will show a yellow circle with an exclamation mark in it with (possible resource conflict) or a red X indicating a serious problem (device could cause Windows to lock up).

6. Try to gather the following pertaining to your system.

    1. NIC: Make and its specifications
    2. PCI: How many PCI slots are there?
    3. Device driver: Details. Try to upgrade

- **Simple Local area networking (LAN):**

Aim:
Create a simple LAN with two PCs using an Ethernet hub/switch and two straight-through cables to connect the workstations

Tasks

1. Obtain a CAT 5 straight-through cable from the teacher.
    1. Verify that the pins are wired straight through by holding the two RJ-45 connectors for the cable side by side with the clip down. All pins should have the same color wire on the same pin at both ends of the cable. (pin 1 should match pin 1 and pin 8 should match pin 8 etc.)
    2. Record the order of the colours here:
2. Connect the workstation to a hub/switch.
    1. Plug the hub or its AC adapter into a power outlet. Plug the straight through cable from workstation the workstation into any port of the hub, except the first.
    2. After the workstations have booted, check the green link light on the back of each NIC and the green lights on the used ports of the hub to verify that there is a good physical connection between the hub and the NIC in the workstations . If the link light is not on it usually indicates a bad cable connection, an incorrectly wired cable or the NIC or hub may not be functioning correctly.
3. Check the TCP/IP Protocol Settings.
    1. Use the Control Panel and double-click on Network
    2. Select the TCP/IP protocol, which matches your NIC, from the Configuration tab
    3. Click on Properties. Check the IP Address and Subnet mask for your workstation on the IP Address tab.
    4. Since we are only making an internal network, an intranet, the IP addresses can be set to just about anything. For this lab, we will use the Class C network address 200.150.100.0 and each workstation will use a different last value for its host ID number. For example host 1 will be set to static IP address 200.150.100.1
    5. Set the default subnet mask on each workstation to 255.255.255.0.

4. Check the network connection with the Ping Utility.
    1. Click on Start, Programs and then the MS-DOS Prompt.
    2. Enter the Ping command followed by the IP address of your own PC (Example - ping 200.150.100.1) and record the result:
    3. Repeat for the IP address of your neighbour. How was the result different?

5. Set up Windows Networking Options.
    1. Use the Control Panel, Network utility, Configuration tab and check to be sure that you have the following networking components installed:

        a) Client for Microsoft Networks (small computer icon).
        b) The NIC adapter (small NIC icon).
        c) The TCP/IP protocol (small network cable connection icon).
        d) File and printer sharing for Microsoft Networks (small computer with a hand underneath icon).
    2. The last one is probably missing, so add it.
    3. Click on Add.
    4. Click on each of the four choices and record their purposes:
    5. Click on Service and then Add.
    6. Choose the appropriate service and click OK. It should load automatically.
    7. If asked, do not reboot yet.
    8. Again on the Configuration tab, click the File and Print Sharing button. Check the box that says "I want to be able to give others access to my files" to allow each workstation to share its Folders.
    9. Click on the Access Control tab and verify that that the "Share Level Access Control" button is selected.
    10. Click on the Identification tab and enter a name for your computer. The Workgroup should be ICE and the Computer Description is optional.
    11. Click OK until all windows are closed and then reboot.

6. Check out your LAN.
    1. Double-click on **Network Neighborhood**.
    2. Record what you see:
    3. Double-click on each icon to see what is there.
7. Share some files.
    1. Use Windows Explorer to create a folder to be shared called "Testfolder".
    2. Double-click on My Computer or Network Neighborhood, select the folder and right click to share it. Enter the name of the share and click OK.
    3. After your neighbors have done the same, create a new document and save it to their folder. Record the name of your file and the name of the workstation with which you shared the file: _____
    4. Open the file which your neighbor saved to your folder. Record its name: _____

8. Find the meanings for the following terms:
    1. LAN
    2. Ethernet
    3. CAT 5 or category 5 cable
    4. RJ45 connector
    5. Hub
    6. Class C IP address
    7. Ping

- **Internet Connection**

AIM:

Use an Ethernet hub to connect to the Internet and to investigate HTTP and FTP.

Tasks

1. Connect your workstation to the hub

    1. Obtain a CAT 5 straight-through cable from the teacher.
    2. Plug the hub or its AC adapter into a power outlet.
    3. Plug the straight through cable from workstation the workstation into any port of the hub, except the first.

2. Try to reach the Internet.

    1. Open Internet Explorer.
    2. If it asks you to set up the connection, choose the last option which says that you are already set up.
    3. What happens?

3. Check IP address settings.

    1. Use the Control Panel and double-click on Network
    2. Select the TCP/IP protocol, which matches your NIC, from the Configuration tab
    3. Click on Properties. Check the IP Address and Subnet mask for your workstation on the IP Address tab.
    4. Since you are connecting to the Internet, you can not just make up your own address. Let the TVDSB's server assign you a valid address by setting the IP address to **Obtain an IP address automatically**.
    5. Click OK until you are asked to reboot.
    6. Reboot.

4. Try to reach the Internet.

    1. Open Internet Explorer.
    2. What happens?

5. Investigate FTP and HTTP.

    1. Go to www.boiap.ac.in
    2. What are vocational courses?
    3. Go to google.co.in
    4. What is FTP and what is an FTP **site?**
    5. Go to ftp://ftp.archive.org/pub/etext/.
    6. Open the folder called **etext00.**
    7. Open the file called **00ws110.txt**
    8. Time how long it takes to load the full text.
    9. How big is the .txt file of the text? _____
    10. What have you opened? _____

6. Use the built-in FTP utility.
    1. Click on the Windows Start button and then Run.
    2. Type in **ftp** and enter.
    3. Type in **open ftp.archive.org**. What happens?
    4. Type in **none.**
    5. Type in **dir** . What does this do?
    6. Type in **cd pub**.
    7. Type in **cd etext.**
    8. Type in **cd etext00** . What does **cd** do?
    9. Type in **get 00ws110.txt** . What does this do?
    10. How long does this download take? _____
    11. Where does the file, **00ws110.txt** end up?

7. Find definitions for:

    1. DHCP
    2. FTP
    3. HTTP

- **Working with Hyper terminal**

Aim:

Work with HyperTerminal, using Telnet and Kermit protocols.

Tasks

1. Connect your workstation to the hub

    1. Obtain a CAT 5 straight-through cable from the teacher.
    2. Plug the hub or its AC adapter into a power outlet.
    3. Plug the straight through cable from workstation the workstation into any port of the hub, except the first.

2. Set your IP address back

3. Install HyperTerminal

    1. Click on the Windows Start button and then Help.
    2. Click on the Index tab.
    3. Type in hyper.
    4. Record the purpose of HyperTerminal
    5. Click on Click here to start HyperTerminal and follow the Help instructions to install HyperTerminal.
    6. You may have to direct the install to c:/win98, if it asks for the Windows 98 CD.

4. Run Hyper Terminal.

    1. Click the Start button.
    2. Point to Programs, Accessories, Communications and then click HyperTerminal.

5. Create a connection using the connection description dialog box.

    1. Enter a name for the connection.
    2. Choose an icon or allow the default to be used.
    3. Click the **OK** button. The Phone Number dialog is displayed.
    4. Choose Connect using: TCP/IP (Winsock)
    5. Record the default port nmber: _____
    6. For the Host address, fill in your neighbour's IP address.
    7. Click OK.

6. Have your neighbour prepare to receive your call.

    1. Click on Call in the menu bar.
    2. Wait for a call.

7. Reconnect if your attempt to connect times out.

    1. Click on Call in the menu bar.
    2. Click on Call.
    3. Watch the bottom left corner to see when the connection is made.
    4. Type a message to your neighbour.
    5. Have your neighbour type one too.

8. Figure out how to transfer files between your two machines
    1. Use Kermit

9. Clean up your machine

    1. Remove WS-FTP.
    2. Remove Hyperterminal
    3. RemoveFile and printer sharing for Microsof Networks.
    4. Remove any files you created.
    5. Remove any files you downloaded (e.g., Shakespeare's First Foli)
    6. Set the IP addres to 192.168.0.1
    7. Set the mask to 255.255.255.0
    8. Set the computer's name to computer.

10. Show the teacher your machine.

11. Switch off the system

12. Find the following definitions:

    1. Telnet
    2. Kermit
    3. port number
    4. port (for software, not hardware)

Supplementary notes

Networking Hardware

Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data processing and communications within the network.

Networking hardware and devices

The following components are the basic constituents of any network

- File Servers
- Workstations
- Network Interface Cards
- Switches
- Repeaters
- Bridges
- Routers
- Modems

File Server: The file server controls the communication of information between the nodes on a network. For example, it may be asked to send a word processor program to one workstation, receive a database file from another workstation, and store an e-mail message during the same time period. This requires a computer that can store a lot of information and share it very quickly. File servers should have at least the following characteristics

Workstations:

It is a very fast computer with a large amount of RAM and storage space, along with a fast network interface card, with excellent graphic capabilities.

Network interface card:

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, with the card fitting into an expansion slot inside the computer. Some computers, such as Mac Classics, use external boxes, which are attached to a serial port or a SCSI port. Laptop computers can now be purchased with a network interface card built-in or with network cards that slip into a PCMCIA slot.

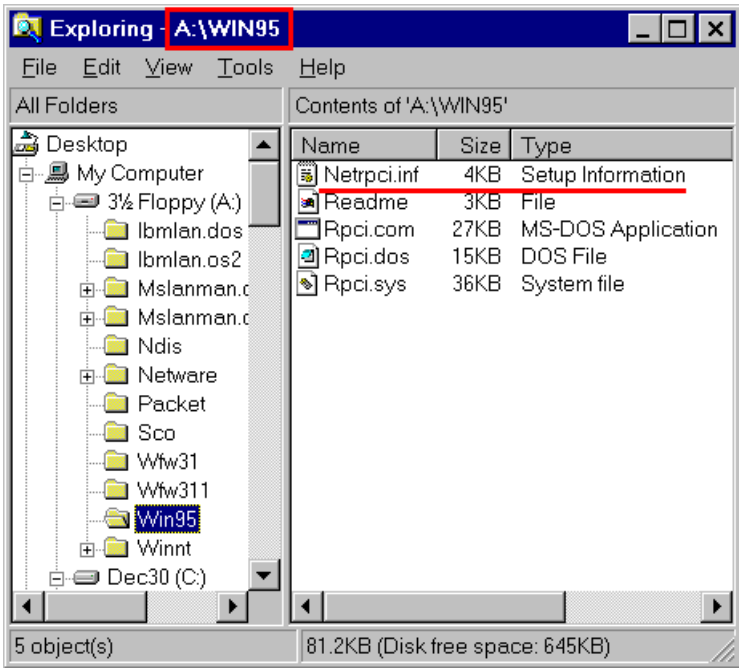
Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using. The three most common network interface connections are Ethernet cards, LocalTalk connectors, and Token Ring cards.

Ethernet Cards:

Ethernet cards are usually purchased separately from a computer, although many computers now include in the motherboard itself. Ethernet cards contain connections for either coaxial or twisted pair cables (or both). If it is designed for coaxial cable, the connection will be BNC. If it is designed for twisted pair, it will have a RJ-45 connection. Some Ethernet cards also contain an AUI connector. AUI Connector (Attachment Unit Interface) - A 15 pin connector found on Ethernet cards that can be used for attaching coaxial, fiber optic, or twisted pair cable.

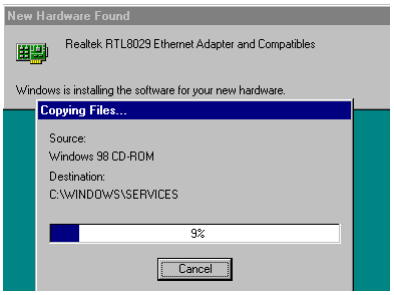
Fig NIC Ethernet card

When buying a network card, make sure, that you can get updates of the Network drivers!

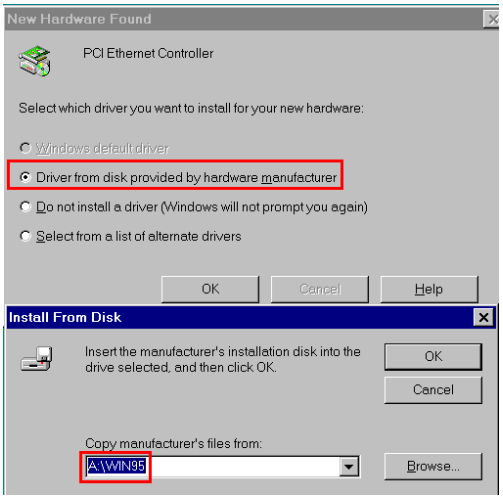


Normally drivers for nic cards are provided on a floppy disk. Search for a directory "Windows" or similar, and locate the INF-file, containing the Setup-Information. If no floppy disk is provided, then the driver for this NIC should be included already with Windows.

Since it is a PCI-card, Windows will detect it on startup and either will use its own driver (if the card is known)

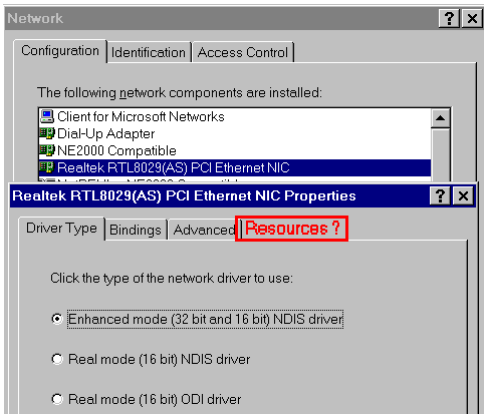


Or will prompt you for the "Manufactures Disk":



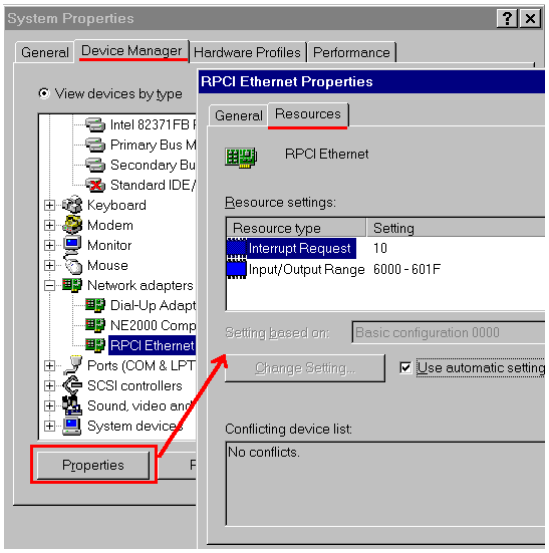
Where you now need to define the location (directory) for the INF-file.

To verify, which resources (I/O-address and Interrupt/IRQ) has been assigned, you can try in the Control-Panel, *Network*-Applet, the *Properties* of the PCI Network card:

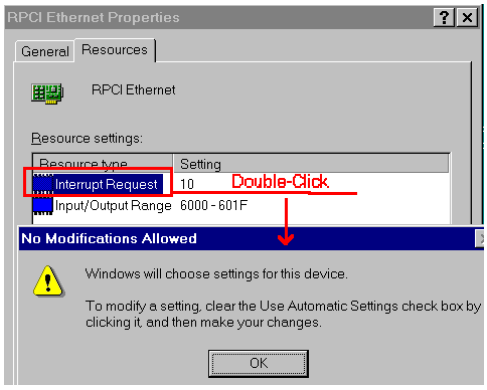


but for a PCI-card, the tab: "***Resources***" *(listing the I/O-address and Interrupt/IRQ)* is usually missing.

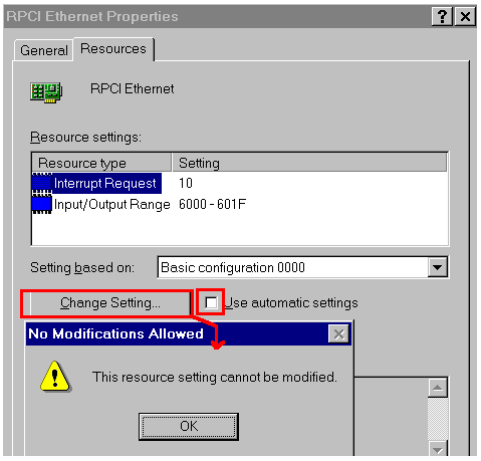
For that, use in the "*Control-Panel*" the ***System***-Applet, tab: "*Device Manager*" *(which is also used to check conflicts in resource usage)*



Locate under "*Network adapters*" your PCI-network card and check its "*Properties*" You can try to ***Double-Click*** on a resource in an attempt to change the values:

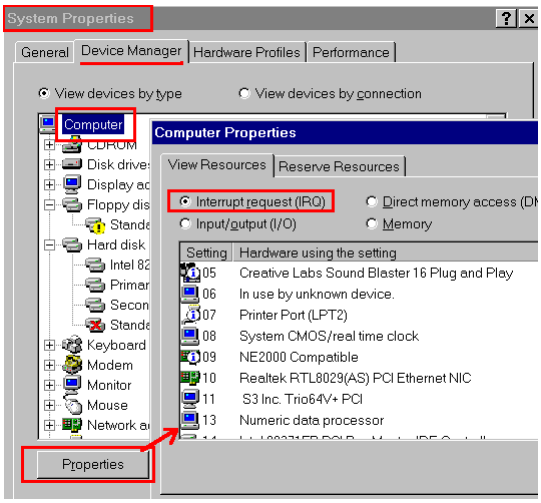


But also "*un-checking*" the "***Use of automatic settings***":



Will NOT allow you to manually define a configuration value.

Check in the "*Control-Panel*" "***System***-Applet under tab: "*Device Manager*" in the Properties of the "*Computer*", that the Interrupt is not used by multiple devices:



If another device is using already the Interrupt, try to move the other device to a different Interrupt or check in your BIOS: most BIOS version allow either to assign an IRQ to a specific PCI-slot or allow to reserve specific IRQs NOT to be used by a PCI-device.

Switch:

A concentrator is a device that provides a central connection point for cables from workstations, servers, and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central switch/hub. Most switches are active, which is they electrically amplify the signal as it moves from one device to another. Switches no longer broadcast network packets as hubs did in the past. They memorize addressing of computers and send the information to the correct location directly.

Switches are:

- Usually configured with 8, 12, or 24 RJ-45 ports
- Often used in a star or star-wired ring topology
- Sold with specialized software for port management
- Also called hubs
- Usually installed in a standardized metal rack that also may store netmodems, bridges, or routers

Repeaters:

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.
A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted-pair cable to a multi-port active concentrator. The concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.

Bridges:

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. You might say that the bridge is like a traffic cop at a busy intersection during rush hour. It keeps information flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be used to connect different types of cabling, or physical topologies. They must, however, be used between networks with the same protocol.

Routers:

A router translates information from one network to another; it is similar to a super intelligent bridge. Routers select the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts.

While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges, and other routers on the network. Routers can even "listen" to the entire network to determine which sections are busiest -- they can then redirect data around those sections until they clear up.
If you have a school LAN that you want to connect to the Internet, you will need to purchase a router. In this case, the router serves as the translator between the information on your LAN and the Internet. It also determines the best route to send the data over the Internet.

Routers can:

- Direct signal traffic efficiently
- Route messages between any two protocols
- Route messages between linear bus, star, and star-wired ring topologies
- Route messages across fiber optic, coaxial, and twisted-pair cabling

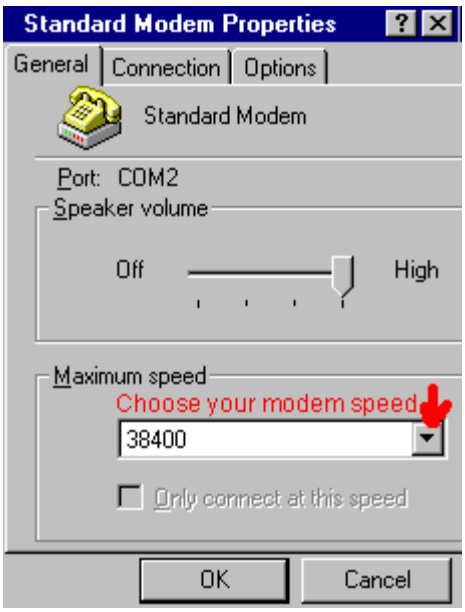
Modems:

Some tips for installing an External Modem

- Turn computer off.
- Plug modem into a free serial port.
- Plug modem power in and hook up phone line.
- Restart system, you should go into a plug and play routine with windows.
- Your system will recognize your new hardware especially if is is PnP (Plug and play) device. In most cases you will be brought to a hardware wizard under windows and it will ask for a driver for your device.
- Make sure you have the installation CD or floppy in the drive.
- Browse location for what is called a INF. File, this provides information on your device and will help load device.
- Simply choose location of INF. file and hit ok or next. This should load the driver for device and your in the computer.

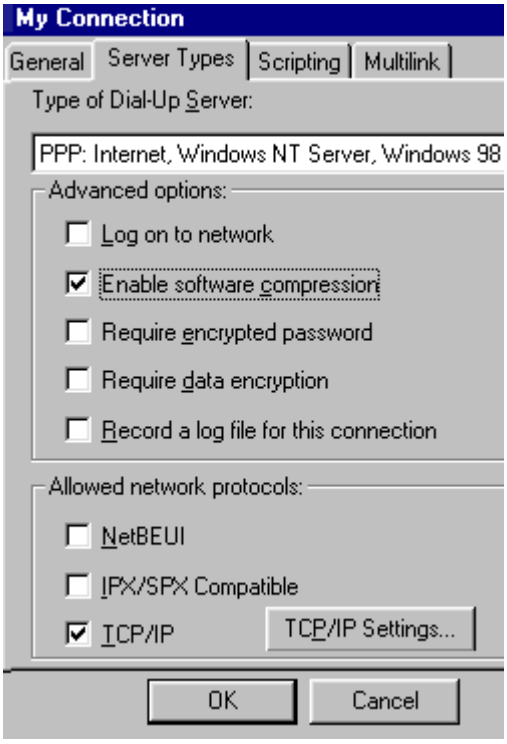
- **Installing dial-up network:**
    - Double-click **My Computer** on your desktop
    - Double-click the **Control Panel** icon
    - Double-click the **Add/Remove Programs** icon
    - Click **Windows Setup**
    - Click **Communications**
    - Click **Details**
    - **Check** the **box** beside **Dial-Up Networking**
    - OK
    - OK Again
    - Windows 95 will ask for installation diskettes or CD
    - **Put** your **diskettes** or CD **in the appropriate drive**
    - Once Dial-Up Networking installs, click the OK button to restart
    - Click the **Start** button and choose **Shut Down**
    - Choose **Restart**
    - Yes

1. Click the **CONFIGURATION** button
2. Select your modem speed: Select 19200 if you have a 14.4 modem
   38400 if you have a 33.6 modem and select 57600 if you have a 56K modem
3. Click **OK** button

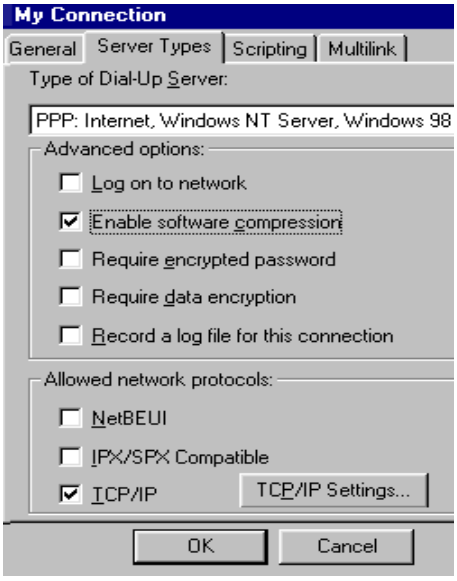


Server types

1. Look at the top of the dialogue box. Select the **SERVER TYPES** TAB
2. Type of Dial-Up Server is PPP: Windows NT, Windows 98
3. Uncheck Log on to network.
4. Check Enable software compression.
5. Uncheck require encrypted password.
6. Uncheck NetBEUI.
7. Uncheck IPX/SPX Compatible.
8. Check **TCP/IP**



TCP/IP Settings



Some ISP's require that the server assigns the IP address. You'll have to check with your ISP to see if that's the case. If so, just select "Server Assigned IP address" and "Server assigned name server addresses" and

you'll be all set. Otherwise, get the DNS numbers from your ISP and follow these directions.

1. Click the TCP/IP Settings button in the lower right corner.
2. Select the Server assigned IP address radio button
3. Select the Specify name server addresses button
4. Primary DNS box, type your Internet Service Providers DNS numbers. They will look something like this: 111.111.111.111
5. Secondary DNS box, type the DNS numbers of your ISP: 111.111.111.111
6. Check both Use IP header compression and Use default gateway on
   remote network.
7. Click OK

Adding a dial-up adaptor

1. Click the Start button point to Settings and choose Control Panel.
2. Click the Network icon.
3. Select the Configuration tab.
4. Click the Add button.
5. Select Adapter.
6. Click the Add button.
7. From the Manufactures: list, choose Microsoft.
8. From the Network Adapters: list, choose Dial-up Adapter.
9. Click the OK button.

Adding TCP/IP

1. Click the Start button point to Settings and choose Control Panel.
2. Click the Network icon.
3. Select the Configuration tab.
4. Click the Add button.
5. Select Protocol.
6. Click the Add button.
7. From the Manufactures: list, choose Microsoft.
8. From the Network Protocol: list, choose TCP/IP.
9. Click the OK button

Adding network client

1. Click the Add button.
2. Select Client.
3. Click the Add button.
4. From the Manufacturers: list, select Microsoft.
5. From the Network Clients: list, select Client for Microsoft Networks.
6. Click the OK button.

Installing Integrated services Digital Network (ISDN)

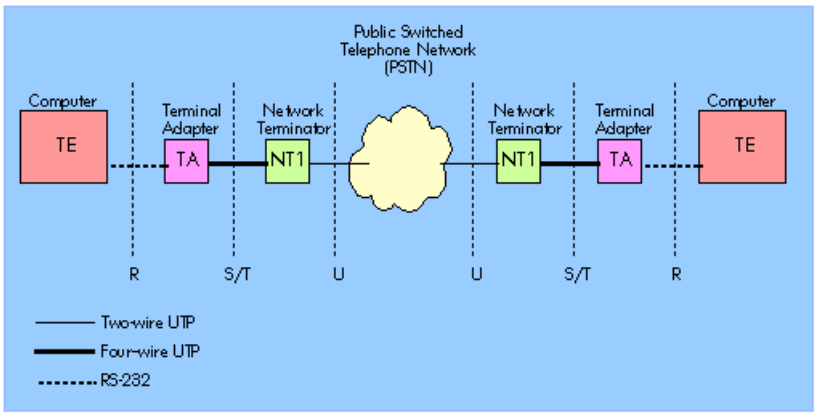


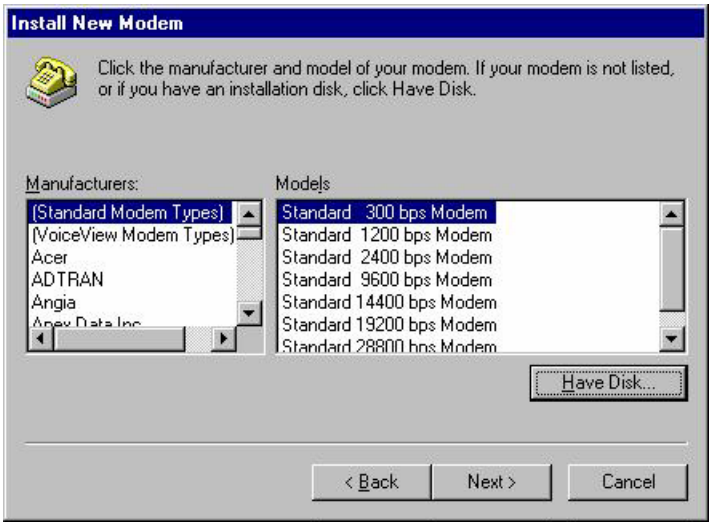
Fig A typical ISDN connection

Step no.1:

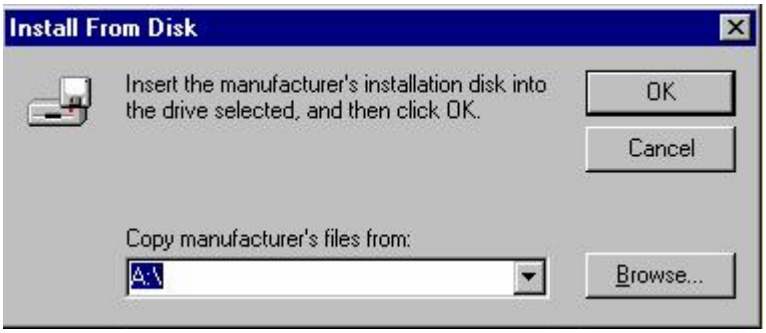
- An existing Integrated Services Digital Network (ISDN) line installed by your Telephone Company or ISDN Provider.
- The information sheets supplied with your installation. You will need to know your Service Profile Identifiers (SPIDS), Switch Type, etc.
- An ISDN internal or external Terminal Adapter properly installed in your computer and connected to your ISDN wall jack.
- The ISDN Setup Software supplied with your Terminal Adapter, on either floppy disk or CD. Make sure you have. Make sure you have the following provider's Web Account information available: your username, password, and your local access number.

Step no.2: Installing a commercial Terminal adaptor:

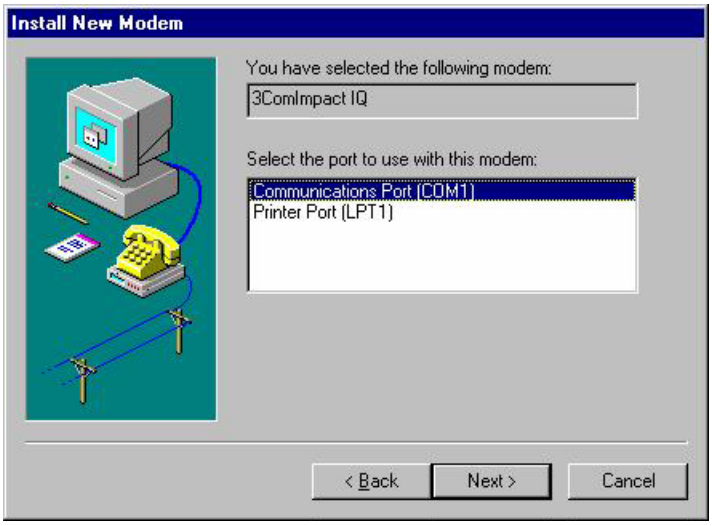
- Connect the device to your computer according the manual.
- To install the device into Windows, click on start, settings, then control panel.
- In the Control Panel, double-click on Modems. Click Add, and then check the box that says "Do not detect my modem, I will select it from a list", which will bring up the following window.



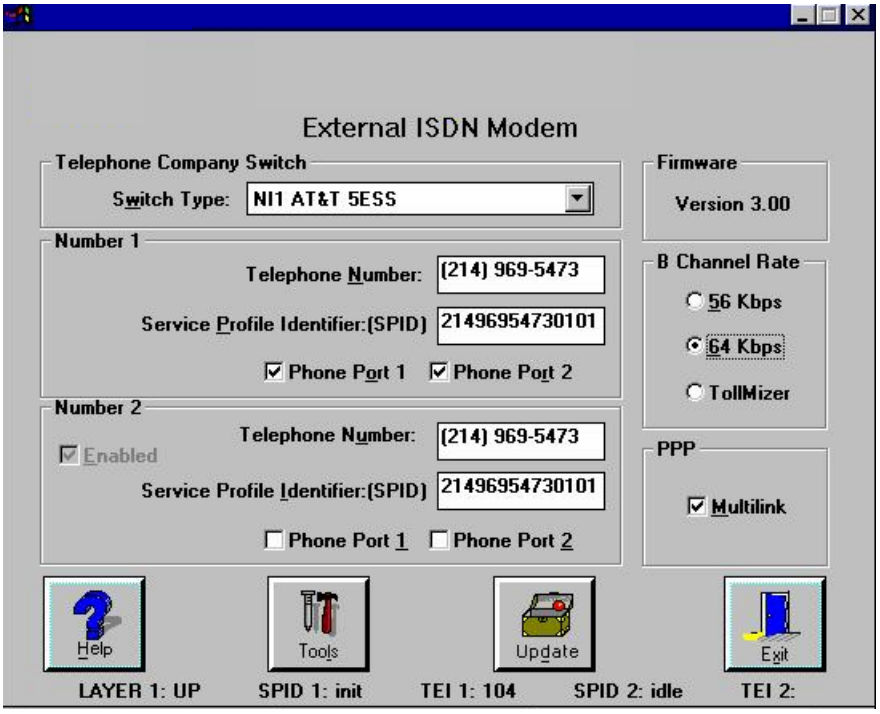
Select **Have Disk**



- Place the driver disk into your floppy drive, and then press OK
- Select the appropriate device from the list, and then press Next.



- You will be prompted to select your communications port. Highlight the correct one, then press Next
- Click **Finish** and you should return to the modem properties window with your new device appearing in the window.
- Click OK and close the control panel.
- Now click the **start** button and select **run**
- Type a:\setup.exe in the window. This should start the setup wizard.
- Click **Continue** at the first screen.
- On the next screen, the wizard defaults to the 3comiq directory for storing its files. You can change it at this point, if you like, then press Continue.
- The Wizard will then test your connection.
- You will be prompted from your first ISDN telephone number. This is *your* telephone number, not the number that you will be dialing.
- If all tests correctly, and the IQ can determine your spids, it will bring up a configuration window.



- It should be configured as shown, excepting that phone number and corresponding SPID should appear in the "Number 1" and "Number 2" areas. Also, (the values shown here are dummy) the box for MultiLink should only be checked if you have a 128K dialup ISDN account with Internet America. If you have a 64k ISDN account then make sure this is NOT checked.
- Click Exit to close. ISDN is ready to surf!

- **Web hosting**

Before you decide to host your website its important to get your domain name registered. Once you've figured out what your Domain Name is going to be, the next step is to figure out how to make it available on the Internet. All sites on the Internet are hosted on Web servers of one sort or another.

What is Web Hosting?
The term hosting is generically used to describe a variety of services necessary to support a web site. If you connect a couple of computers together at home, or at work, then share printers and even disk drives - you've got a little network set up. Now connect millions of computers around the world together and you've got the Internet.

To make that connection you usually dial into an Internet Service Provider or ISP who gives you the ability to connect to the web, email, and use other parts of the internet as well.
These ISP's not only give their customers a way to connect their home computers to the internet, they also allow websites on their computers which are called servers. By creating a website and putting it on a server connected to the rest of the net, anyone in the world who is also connected to the net can see your site.

Fundamental Web Hosting Needs
In the most general sense, a web site requires (1) hardware, (2)software, (3) a connection to the Internet and (4) an administrator.

1. **Administrator**
   The Administrator performs the following duties:
   - Configure Server / Install Software
   - Monitor Server
   - Run Traffic Reports
   - Run Backups
   - Monitor site responsiveness
   - Manage disk storage space
   - Security monitoring and management
   - Administer Databases
2. **Software**
   Software could consist of an:
   - Operating System
     (i.e., Windows NT, Linux)

   Required:
   - Web Server (i.e., Apache or IIS)
   - Traffic Reporting (i.e., Web Trends)
   - Credit Card Software
   - Databases
   - Digital Encryption (i.e., VeriSign)

   3. Hardware
   - Server
   - Network devices
     (switches, routers, wiring)
   - Tape backup
   - Secure physical racks or lockers
   - Storage Area Network (SAN) - Optional
   - Premise security - Optional

- Network Firewall - Optional
- Load balancing - Optional
- Fire control systems - Optional
- Uninterruptible Power Supply -Optional

Connectivity
Connectivity is the manner in which the ISP or MSP provides Internet access to the website. At a minimum this should be a Frame Relay or T1 connection. Better providers will provide redundant connections to diverse upstream Internet providers.

Levels of Service
Hosting services can be divided into four different categories, with each providing a different set of administrative, hardware, software, and connectivity services. Your choice will depend upon your business requirements and your technical capability. Generally, as the level of service increases, the costs increase. The four categories are:

- Shared
- Co-location
- Dedicated
- In house

Hosting Arrangement	Best suited for companies with...	Price Range*
Shared Shared Hosting environment put multiple web sites on one server. All of the web sites on the shared server use the same network connection, the same hardware resources, and the same software. You are only responsible for managing the design and content of the Web site.	Company brochure or profile. Basic e-com. Bulletin board or small chat room. Small and medium sized businesses	Rs.2,500 - Rs.10,000 per year ($15 - $300 per month)

Dedicated You rent your own dedicated server from a hosting provider. The hosting provider is responsible for buying hardware, installing software and maintaining the server. You may customize the server with remote server access and would be responsible for managing any applications.	Mission critical e-Commerce or interactive site Multiple Web sites High speed and significant data transfer requirements Unique software needs Limited technical staff resources	Rs.16,000-Rs.5 Lakh per month ($300-$10,000 per month)
Collocated With collocated Web hosting, the Web host provides your company with space to store your own server hardware and a high-speed connection to the Internet for that server. Server collocation is generally best for companies that have the in-house capability to manage a Web server.	Mission critical e-Commerce or interactive site High speed/significant data transfer requirements Unique software needs Strong technical staff capable of server maintenance	Rs. 8,000-Rs.5 Lakh ($200-$10,000 per month)
In House You set up a server on your own premises. You buy the connectivity, hardware and software, and configure and maintain the system. You need to hire a system administrator or an information technology team.	Multiple Web sites Internet Service Provider Eg: Big Corporate companies like IBM	Expensive; need staff, connectivity and real estate.

*Pricing ranges reflect a wide variation in available features and services. The quotes you receive will vary according to the options you choose.

How to Choose a Web Hosting Service

It is good to make a right choice the first time, because if you have to move to another hosting service, it will cost you time and you will lose some of your valued customers due to the downtime setting up with another host.

You will also have to pay set up and hosting fees for a new account.

Some basic things to consider when choosing a Web Hosting Service:

Speed and reliability of the servers and hardware

Make sure they have a high-speed connection (preferably T3 or higher) to the Internet.

- Effective Bandwidth Management – opt for unlimited bandwidth for your site.
- Backup Systems – good hosts will have back up systems in place to guard against power failures, which will cause you to lose data and customers.

There are so many free tools are available that allows you to evaluate server performance before making a decision! Net Mechanic will measure the speed of access for all facets of access (network speed, DNS lookup, connect time, download time, and absence of timeouts). The "download time" statistic is the most important single item to compare. Collect your list of candidate hosting services and run side-by-side tests of all the candidates. Collect samples during peak and non-peak times for optimal comparison.

Space

How much space do you expect to eventually want for your web site? Planning ahead can save you lots of money later. If you expect to grow, look for a place that offers sites of 100 MB or more. Some services offer 500 MB sites for less money than others that offer only 30 MB.

Compatibility with existing Software and Skills

Are your host's server, software and support services compatible with the skills and software you are using? For example if you are using FrontPage to create your site, make sure they have FrontPage extensions installed on their server.

Some of the basic features of a hosting service should include:

- Domain name registration
- At least 20MB of allocated space
- Unmetered bandwidth
- Free Technical Support
- POP3 E-Mail Accounts
- Email Forwarding
- Email Auto-responders
- Email Aliases
- FTP Access
- FrontPage Support
- Own CGI-Bin Access
- Free Perl, CGI
- Server Side Includes (SSI)
- Password Protection
- Reseller/referral program

Flexibility and room for growth – Keep in mind the future needs of your web site. If the traffic to your site explodes, or in the future you may need a database solution then your host must be able to accommodate the changes.

Quality of their support services Quality of existing customers – ask for any BIG current customers that are hosting with that service. Opinions of existing customers – ask for any testimonies of existing customers to get feedback from them concerning reliability and support.

Stability – you do not want your hosting service to go out of business (like what happened to many of the free hosts) and leave you stranded. Check how many years they have been in business.

Support and Responsiveness – Make sure you can contact them 24/7 by phone or email. Test the quality and efficiency of response by sending them an email pertaining to some question you may have before you sign

up. Is there really anybody there? We think that this is the single most important consideration. Also, check out the quality of their online documentation.

Types of Hosting Services

- **Free Hosting:** Free sites are for people whose sites are small and do not expect much traffic.
  Pros It's Free For small non business sites
  Cons No usage of domain names Limited technical support Unreliability of servers, software Limited web space, technical support Host may shut down due without notice
- **Virtual Hosting:** (also known as domain or shared hosting). This is the most popular and cost effective form of hosting.
  Pros Low cost Great for the average business sites Good technical support
  Cons Multiple sites on server Sometimes slow updates Limited security and control due to the large number of sites on 1 server.
  Use your own domain name (www.yoursite.com)

If you follow these basic guidelines, you will have a reliable, efficient and satisfying hosting service that will contribute to the success of your business for many years to come.

Choosing an excellent service to host your web site doesn't have to require luck. Knowing what to look for makes selection simple.

Selecting a Server Operating system:
Usually, Web hosts use either Linux or Microsoft Windows NT Server. Web servers generally fall into one of two categories:

Linux-based and
Microsoft Windows NT.

Linux a clone of Unix, the older and more popular of the two systems, has a strong reputation for reliability and power. On the other hand, many new to the Web find it difficult to understand and navigate. NT is regarded as easier to use than Linux for data-driven Web sites; it also supports the user-friendly Web page design tools in Microsoft's FrontPage software.

Visitors using any of a host of computer and browser combinations will be able to access your site, regardless of whether you choose a Linux or an NT Server.

Choose the server system with which you feel most comfortable; if you wish to use software on your Web site that can only run on a specific server (e.g. Apache for Linux, IIS for NT) you should choose to locate your Web site using that server.

Web server software

Web server software is the application that runs on your computer and makes Web pages stored on your computer available to Internet users. It also co-ordinates such things as secure e-commerce transactions and streaming audio and video.

Web server software can also be integrated with databases to make information stored in your database available to Internet users.

Some popular Web server programs

Unlike operating systems, of which there are fairly few, there are quite a variety of different Web server software packages that are available. We'll look at some pros and cons of each.

Apache

Apache lends itself particularly well to projects that are heavily Java based. It offers superior handling of the Java Database Connectivity (JDBC) application program interface (a program which allows Java-based services to access information stored in SQL-compliant databases).

Apache, like Linux, is a piece of open-source software. It's maintained by a group of programmers who create the software for the thrill of it - not for any expected financial gain. Apache was born in early 1995, as free Web server software based around NCSA httpd 1.3, which was the most popular Web server of the day, and a bunch of software patches. From that it earned it's moniker, which stands for "A PAtCHY server." Since then, it has been completely re-written, and has become the most popular WWW server on the Internet.

Apache pros:

- Open source updates. it's constantly being updated and you can add functionality as it becomes available.
- Free. The software is free. It's hard to beat that price.
- Multi-platform support. Apache can be used on systems that have 80x86-series (i.e. Intel) processors running either Linux or NT as an OS, or on other computers running a Unix-type OS on a different processor.
- Popular. Apache is the most-used Web server software package in the world. As such, it's unlikely that further development of the software will ever cease.

Apache cons:

- No Support. Apache's developers do not provide any type of support for their product. There are third-party companies that provide Apache support, but you have to pay for it.

- Runs best on Linux. Given two machines with the same hardware and different operating systems (Linux and NT,) Apache runs faster on the Linux machine. This means that if you decide to go with Apache, you should also use Linux to get maximum performance. If you've decided to use NT, it makes more sense to use the Web server Microsoft includes with that operating system.

Microsoft Internet Information Server (IIS)

Essentially, IIS is the server software of choice if it is an ASP-based site. IIS is Microsoft's main business offering in the Web server software market. It offers the same ease of use as many other Windows applications, including "Wizards" that assist with setup and maintenance of the software. It should be easy for anyone familiar with the NT OS to set up.

IIS really shines when it comes to the handling of Active Server Pages (ASPs), pages that are generated by the Web server software using Active X scripting - usually Visual Basic Script or JavaScript code. IIS offers superior ASP-based interface to ODBC sources like Access and SQL-Server.

IIS Pros:

- Microsoft product. Since IIS is a Microsoft product, it not only has the same heavy backing as other Microsoft products, but is integrated seamlessly into the OS itself. This means you can do things like drag and drop files into the software for instant availability on the Web with a minimum of hassle.

- Comes free with NT. If you do decide that NT is the best OS to use, IIS is free.

- Limits bandwidth. Unlike other server software, IIS has the ability to limit how much bandwidth your web pages have available. Thus, if your ISP charges extra if you use more than a given amount of bandwidth in a month, you can set your Web server to limit itself to using that much bandwidth, saving you from having to pay an extra monthly fee.

- Crash protection. If one application running on the server crashes, the Web server and other applications continue to run, and the failed application restarts the next time a user requests it.

IIS Cons:

- Limited to NT-based systems. IIS is not available for use on non-NT systems. This means that if you think a UNIX-based OS is what you're looking for, you can't use IIS.

- Closed source. As with NT, the source code to IIS is Microsoft's proprietary information - you can't get access to it to make changes. This also means that there aren't many third-party developers working on improving the core software.

Web hosting lab

The student may be advised to go through the process of creating web using his creative ideas
Hosting web sites is a costly affair, however there are so many sites, which offer free web hosting service
One such site is geocities.com. The student should have an e-mail account in his name. The following steps explain the procedure for hosting an web.

Your 10-Step Guide to the Basics of Yahoo! Web Hosting

Welcome to Yahoo! Web Hosting. This guide provides a step-by-step overview of how easy it is to set up, manage, and market your professional business web site

Step 1: Sign up for Yahoo! Web Hosting

Just pick a Yahoo! Web Hosting package and speed through our sign up process to get started fast. You'll choose your web site domain name (like www.widget-designs.com).

Step 2: Welcome to Manage My Services -- please explore!

The Manage My Services page is your central headquarters for managing every aspect of your web operation. Please take some time to explore the resources available from this page.

Step 3: Set up your email accounts.

Take advantage of Yahoo! Web Hosting's full-featured email solutions to improve your company communications. It's easy to set up accounts and preferences.

Step 4: Plan and organize your web site content

Before you begin building, we recommend that you outline your site content and consider structural issues like navigation. This simple process paves the way for easier site construction, effective site management, and a more engaging experience for your visitors.

Step 5: Choose a web site design tool and start building

Rely on easy, powerful Yahoo! Web Hosting tools or fire-up an application you already own. Work online or offline. Use advanced code or simple wizards. With Yahoo! Web Hosting, it's all up to you.

Step 6: Enhance your site

You can make your site more dynamicith our communications tools, add-ons, and advanced scripting language support.

Step 7: Set up password-protected areas

If your business requires it, you can easily set up special password-protected areas of your site using the Password

Manager.

Step 8: Attract visitors to your new web site
Now that you've invested time and effort to build a great web site, it's time to develop and execute a marketing strategy to ensure that people can find it.

Step 9: Learn from your success and grow
Yahoo! Web Hosting makes it easy to keep tabs on your web site performance, so you can refine your strategy and continue to improve

Step 10: Add e-commerce capabilities to your site
Yahoo! Merchant Solutions offers everything you need to sell online from your professional web site