MSc. (CS)-05/PDCA-05/CCNI

VARDHAMAN MAHAVEER OPEN UNIVERSITY, KOTA

Computer Networking and Internet

Course Development Committee

Chaiman

Prof. (Dr.) Naresh Dadhich
Vice-Chancellor
Vardhaman Mahaveer Open University Kota

Convener / Coordinator

Prof. (Dr.) D.S. Chauhan
Department of Mathematics
University of Rajasthan Jaipur

Member Secretary / Coordinator

Sh. Rakesh Sharma
Assistant Professor (Computer Application)
V.M. Open University Kota

Members

1. Prof. (Dr.) S.C. Jain
Engineering College Ajmer
2. Prof. (Dr.) M.C. Govil
M.N.I.T. Jaipur
3. Dr. (Mrs.) Madhavi Sinha
A.I.M. & A.C.T. Jaipur

Editing and Course Writing

Editor

Sh. Rajeev Srivastava
HOD (Computer Science)
LBS PG College Jaipur

Writers

1. Dr. S.B. Sharma
Director, Dau Dayal Vocational Institute

Dr. B.R. Ambedkar University Agra
2. Dr. D.K. Paliwal

Lecturer (Institute of Basic Sciences)

Dr. B.R. Ambedkar University Agra
3. Sh. Manoj Kumar
Asstt. Professor (Computer Engineering)
Rajasthan Technical University Kota
4. Ms. Poonam Kshatriya
Sr. Lecturer (Computer Science)
A.I.M. & A.C.T. Jaipur
5. Ms. Shweta Sharma

Lecturer (Computer Engineering)
Modi Institute of Technology Kota

Academic and Administrative Arrangement

Prof. (Dr.) Naresh Dadhich
Vice-Chancellor
Vardhaman Mahaveer Open University, Kota

Prof. M.K.Ghadoliya
Director
Academic

Yogendra Goyal
Incharge
Material Production and Distribution

Course Production

Yogendra Goyal
Assistant Production Officer
Vardhaman Mahaveer Open University, Kota

Re-Production: May, 2010 ISBN - 13/978-81-8496-215-4

Printed and published on behalf of V.M.Open University, Kota by Registrar

Printers : The Pooja, Kota /May2010/1000

Index

Unit Number	Unit Name	Page Number
UNIT - I	COMPUTER NETWORK FUNDAMENTALS	1 - 22
UNIT II	COMPUTER NETWORK CONTD.	23-40
UNIT- III	COMPUTER NETWORK CONTD.	41 - 65
UNIT - IV	INTERNET	66 - 75
UNIT - V	INTERNET FEATURES	76 - 101
UNIT - VI	INTERNET CONNECTIVITY	102 - 137
UNIT - VII	WORLD WIDE WEB	138 - 156
Unit-VIII	Application of Internet	157-164
Unit-XI	E-Commerce	165-179
Unit-X	Creating and Maintaining Web Sites	180-194
Unit-XI	Formatting Features	195-204
Unit-XII	Website Features	205-216
Unit-XIII	JAVA Script	217-234
Unit-XIV	Active Server Pages (ASP)	235-249
Unit-XV	Active Server Pages (ASP) Contd.	250-268

UNIT - I

COMPUTER NETWORK FUNDAMENTALS

STRUCTURE OF THE UNIT

1.0 Objective
1.1 Introduction
1.2 Definitions
1.3 Applications
1.4 Transmission media
    1.4.1 Magnetic Media
    1.4.2 Twisted pair
    1.4.3 Co-axial cable
    1.4.4 Fiber Optics
1.5 Networking essentials
    1.5.1 Repeaters
    1.5.2 Hubs
    1.5.3 Switches
    1.5.4 Routers
    1.5.5 Gateways
    1.5.6 NIC
1.6 Summary
1.7 Glossary
1.8 Further Readings
1.9 Answers to the self learning exercises
1.10 Unit end questions

1.0 OBJECTIVE:

Students who complete this unit should be able to understand the following tasks:

- Evolution of Networking
- Various types of transmission media
- Various types of inter-network connecting devices

1.1 INTRODUCTION

Data networks developed as a result of business applications that were written for microcomputers. The microcomputers were not connected so there was no efficient way to share data among them. It was not efficient or cost-effective for businesses to use floppy disks to share data known as Sneaker net. Sneaker net created multiple copies of the data. Each time a file was modified it would have to be shared again with all other people who needed that file. If two people modified the file and then tried to share it, one of the sets of changes would be lost. Businesses needed a solution that would successfully address the following three problems:

- How to avoid duplication of equipment and resources
- How to communicate efficiently
- How to set up and manage a network

Businesses realized that computer networking could increase productivity and save money. Networks were added and expanded almost as rapidly as new network technologies and products were introduced. The early development of networking was disorganized. However, a tremendous expansion occurred in the early 1980s.

1.2 DEFINITIONS

LAN (Local Area Network)

A high-speed, low-error data network covering a relatively small geographic area, up to a few thousand meters. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LANs allow businesses to locally share computer files and printers efficiently and make internal communications possible. LANs manage data, local communications, and computing equipment. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

LANs consist of the following components:

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

MAN (Metropolitan Area Network)

A MAN usually consists of two or more LANs in a common geographic area. A network that spans a metropolitan area. Generally, a MAN spans a larger geographic area than a LAN, but a smaller geographic area than a WAN. For example, a bank with multiple branches may utilize a MAN. Typically, a service provider is used to connect two or more LAN sites using private communication lines or optical services. A MAN can also be created using wireless bridge technology by beaming signals across public areas. Wireless bridge technologies that send signals across public areas can also be used to create a MAN.

WAN (Wide Area Network)

A WAN is a data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs. WANs interconnect LANs, which then provide access to computers or file servers in other locations. Because WANs connect user networks over a large geographical area, they make it possible for businesses to communicate across great distances. WANs allow computers, printers, and other devices on a LAN to be shared with distant locations. WANs provide instant communications across large geographic areas.

Collaboration software provides access to real-time information and resources and allows meetings to be held remotely. WANs have created a new class of workers called telecommuters. These people never have to leave their homes to go to work.

WANs are designed to do the following:

- Operate over a large and geographically separated area

- Allow users to have real-time communication capabilities with other users
- Provide full-time remote resources connected to local services
- Provide e-mail, Internet, file transfer, and e-commerce services

Some common WAN technologies include the following:

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

The Internet and Beyond

More than just a technology, the Internet has become a way of life for many people, and it has spurred a revolution of sorts for both public and private sharing of information. The most popular source of information about almost anything, the Internet is used daily by technical and non-technical users alike.

The Internet: The Largest Network of All

With the meteoric rise in demand for connectivity, the Internet has become a major communications highway for millions of users. It is a decentralized system of linked networks that are worldwide in scope. It facilitates data communication services such as remote log-in, file transfer, electronic mail, the World Wide Web and newsgroups. It consists of independent hosts of computers that can designate which Internet services to use and which of their local services to make available to the global community.

Initially restricted to military and academic institutions, the Internet now operates on a three-level hierarchy composed of backbone networks, mid-level networks and stub networks. It is a full-fledged conduit for any and all forms of information and commerce. Internet websites now provide personal, educational, political and economic resources to virtually any point on the planet.

Intranet: A Secure Internet-like Network for Organizations

With advancements in browser-based software for the Internet, many private organizations have implemented *intra*nets. An intranet is a private network utilizing Internet-type tools, but available only within that organization. For large organizations, an intranet provides easy access to corporate information for designated employees.

Extranet: A Secure Means for Sharing Information with Partners

While an intranet is used to disseminate confidential information *within* a corporation, an *extra*net is commonly used by companies to share data in a secure fashion with their business partners. Internet-type tools are used by content providers to update the extranet. Encryption and user authentication means are provided to protect the information, and to ensure that designated people with the proper access privileges are allowed to view it.

Self learning Exercises :

1. The performance of a data communication network depends on:

   (a) the number of users (b) the transmission media

   (c) the hardware and software (d) all of the above

2. The information to be communicated in a data communication system is the:

(a) medium (b) protocol

(c) message (d) transmission

3. The world's largest network that provides communication to people around the world:

(a) LAN (b) Intranet

(c) Internet (d) WAN

1.3 APPLICATIONS

Computer Networking has become more and more a part of our daily lives. The exchange of information and sharing of devices in this digital world can only be accomplished by networking. It has evolved from being something only useful to businesses, to being a necessity to home users. Computer networking has expanded it uses in many positive ways and continues to do so.

Interactive Multimedia Networking

Applications that require real-time interaction among their users are gaining importance and diffusion as computer networks become more powerful and ubiquitous. Many such applications impose very stringent requirements on the network; among the applications today widely deployed, video-conferencing is the most demanding. In order for the participants in a videoconference call to interact naturally, the end-to-end delay should be below human perception; even though an objective and unique figure cannot be set, 100 ms is widely recognized as the desired one way delay requirement for interaction. Since the global propagation delay can be about 100 ms, the actual end-to-end delay budget available to the system designer (excluding propagation delay) can be no more than 10 ms.

E-Com (Electronic Commerce)

This covers the electronic business transactions over network Electronic Commerce (EC) conducted on the Internet and World Wide Web.(WWW). After an introduction to the Internet and WWW, during which the benefits of using these infrastructures for EC are highlighted, the importance of authentication, confidentiality, integrity and non-repudiability in any business transaction will be handled and extrapolated to EC on the Internet/WWW. The importance of digital signatures and digital identities are major issues, as well as the public key infrastructure on which such signatures and identities are based. The role of Certification Authorities in certifying digital identities is an important issue. Several Internet security protocols like Secure Sockets Layer (SSL) and Secure Hyper Text Transport protocol (SHTTP) as well as the secure payment protocol SET participates, showing how the discussed security technologies are used in these protocols. Different implementations for electronic cash as well as some legal and policy aspects concludes the EC.

Today, E-mail and Internet access are as important to your business as your phone, or any other revenue-producing asset. Innovative network peripherals, powerful administrative tools and thorough management of these growing networks are a requirement to keep your networks available, reliable and secure. Many companies offer for industry-leading solutions from building the backbone of your workgroup or enterprise WAN to connectivity from your home offices or between your satellite sites.

Enterprise Management

Enterprise management solutions generally do more than optimize infrastructure, availability and performance. Companies provide solutions that put you in control and allow you to focus on improving your business' efficiency and increasing customer satisfaction. This allows you a greater (ROI) return on investment.

Network Systems

In today's challenging economic environment, IT managers increasingly have to do more with constrained resources. For the enterprise network manager, this means looking for smarter ways to use the network while managing the demands of users, applications and limited budgets. Companies offer a unique blend of practical and innovative technologies and way of combining them that provides you with high-value, leading-edge solutions designed for the realities of business and the Internet.

1.4 TRANSMISSION MEDIA

Whatever type of network is used, some type of network media is needed to carry signals between computers. Two types of media are used in networks: cable-based media, such as twisted pair, and the media types associated with wireless networking, such as radio waves, microwaves and Infrared waves.

In networks using cable-based media, there are three basic choices:

- Twisted pair
- Coaxial
- Fiber-optic

Twisted-pair and coaxial cables both use copper wire to conduct the signals electronically; fiber-optic cable uses a glass or plastic conductor and transmits the signals as light.

For many years, coaxial was the cable of choice for most LANs. Today, however (and for the past 10 years), twisted pair has proved to be far and away the cable media of choice, thus retiring coax to the confines of storage closets. Fiber-optic cable has also seen its popularity rise but because of cost has been primarily restricted to use as a network backbone where segment length and higher speeds are needed. That said, fiber is now increasingly common in server room environments as a server to switch connection method, and in building to building connections in what are termed as metropolitan area networks (MANs).

Copper cable is used in almost every LAN. Many different types of copper cable are available. Each type has advantages and disadvantages. Proper selection of cabling is key to efficient network operation. Since copper uses electrical currents to transmit information, it is important to understand some basics of electricity.

1.4.1 Magnetic Media

All matter is composed of atoms. The Periodic Table of Elements lists all known types of atoms and their properties. The atom is comprised of three basic particles:

- **Electrons** – Particles with a negative charge that orbit the nucleus
- **Protons** – Particles with a positive charge
- **Neutrons** – Neutral particles with no charge

The protons and neutrons are combined together in a small group called a nucleus. Atoms, are groups of atoms called molecules, can be referred to as materials. Materials are classified into three groups based on how easily free electrons flow through them.

The basis for all electronic devices is the knowledge of how insulators, conductors, and semiconductors control the flow of electrons and work together. The materials through which current flows vary in their resistance to the movement of the electrons. The materials that offer very little or no resistance are called conductors. Those materials that do not allow the current to flow, or severely restrict its flow, are called insulators. The amount of resistance depends on the chemical composition of the materials.

All materials that conduct electricity have a measure of resistance to the flow of electrons through them. These materials also have other effects called capacitance and inductance that relate to the flow of electrons. Impedance includes resistance, capacitance, and inductance and is similar to the concept of resistance.

Attenuation is important in relation to networks. Attenuation refers to the resistance to the flow of electrons and explains why a signal becomes degraded as it travels along the conduit.

Electrical insulators are materials that are most resistant to the flow of electrons through them. Examples of electrical insulators include plastic, glass, air, dry wood, paper, rubber, and helium gas. These materials have very stable chemical structures and the electrons are tightly bound within the atoms.

Electrical conductors are materials that allow electrons to flow through them easily. The outermost electrons are bound very loosely to the nucleus and are easily freed. At room temperature, these materials have a large number of free electrons that can provide conduction. The introduction of voltage causes the free electrons to move, which results in a current flow.

Semiconductors are materials that allow the amount of electricity they conduct to be precisely controlled. Examples include carbon (C), germanium (Ge), and the alloy gallium arsenide (GaAs). Silicon (Si) is the most important semiconductor because it makes the best microscopic-sized electronic circuits. Silicon is very common and can be found in sand, glass, and many types of rocks.

Voltage is sometimes referred to as electromotive force (EMF). EMF is related to an electrical force, or pressure, that occurs when electrons and protons are separated. The force that is created pushes toward the opposite charge and away from the like charge. This process occurs in a battery, where chemical action causes electrons to be freed from the negative terminal of the battery. The electrons then travel to the opposite, or positive, terminal through an external circuit. The electrons do not travel through the battery. Remember that the flow of electricity is really the flow of electrons. Voltage can also be created in three other ways. The first is by friction, or static electricity. The second way is by magnetism, or an electric generator. The last way that voltage can be created is by light, or a solar cell.

The purpose of the physical layer is to transport a raw bit stream from one machine to another. Various physical media can be used for the actual transmission. Each one has its own niche in terms of bandwidth, delay, cost, and ease of installation and maintenance. Media are roughly grouped into guided media, such as copper wire and fiber optics, and unguided media, such as radio and lasers through the air.

Magnetic media, commonly called as copper wire media, is term referring to the transmission of audio/video, analog/digital data on a magnetised medium, in form of voltage pulses.

Cables have different specifications and expectations. Important considerations related to performance are as follows:

- What speeds for data transmission can be achieved? The speed of bit transmission through the cable is extremely important. The speed of transmission is affected by the kind of conduit used.
- Will the transmissions be digital or analog? Digital or baseband transmission and analog or broadband transmission require different types of cable.
- How far can a signal travel before attenuation becomes a concern? If the signal is degraded, network devices might not be able to receive and interpret the signal. The distance the signal travels through the cable affects attenuation of the signal. Degradation is directly related to the distance the signal travels and the type of cable used.

The following Ethernet specifications relate to cable type:

- 10BASE-T
- 10BASE5
- 10BASE2

10BASE-T refers to the speed of transmission at 10 Mbps. The type of transmission is baseband, or digitally interpreted. The T stands for twisted pair.

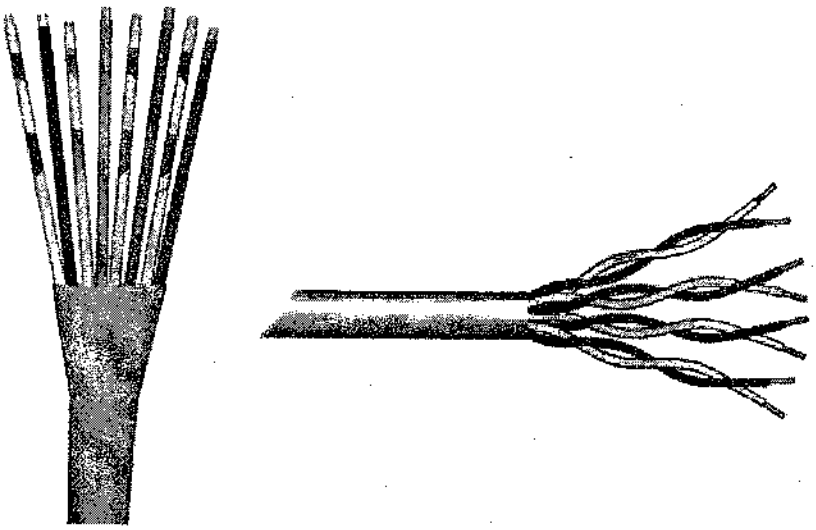
10BASE5 refers to the speed of transmission at 10 Mbps. The type of transmission is baseband, or digitally interpreted. The 5 indicates that a signal can travel for approximately 500 meters before attenuation could disrupt the ability of the receiver to interpret the signal. 10BASE5 is often referred to as Thicknet. Thicknet is a type of network and 10BASE5 is the cable used in that network.

10BASE2 refers to the speed of transmission at 10 Mbps. The type of transmission is baseband, or digitally interpreted. The 2, in 10BASE2, refers to the approximate maximum segment length being 200 meters before attenuation could disrupt the ability of the receiver to appropriately interpret the signal being received. The maximum segment length is actually 185 meters. 10BASE2 is often referred to as Thinnet. Thinnet is a type of network and 10BASE2 is the cable used in that network.

1.4.2 Twisted Pair

Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each connection on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable. For some business locations, twisted pair is enclosed in a shield that functions as a ground. This is known as shielded twisted pair (STP). Ordinary wire to the home is unshielded twisted pair (UTP).

UTP :



UTP cables are made up of pairs of copper wires twisted together. The twisting serves an important purpose – it helps to eliminate electromagnetic interference (EMI). EMI is a common problem on networks using copper wire. Signals from one wire pair might interfere with another (referred to as crosstalk), while powerful external electrical devices may also impact transmission capabilities. When using UTP cables, a common mistake is to unravel the twisting too far – this will certainly degrade signal strength and make the wires more prone to interference.

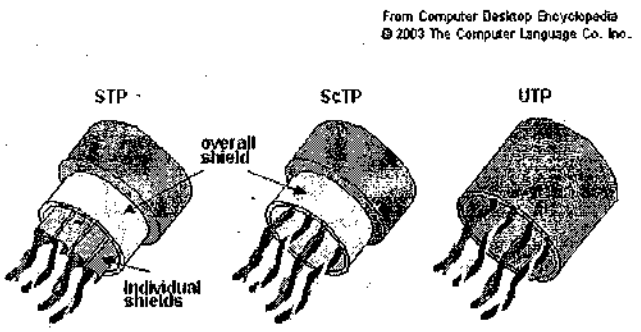
UTP cable has many advantages. It is easy to install and is less expensive than other types of networking media. In fact, UTP costs less per meter than any other type of LAN cabling. However, the real advantage is the size. Since it has such a small external diameter, UTP does not fill up wiring ducts as rapidly as other types of cable. This can be an extremely important factor to consider, particularly when a network is installed in an older building. When UTP cable is installed with an RJ-45 connector, potential sources of network noise are greatly reduced and a good solid connection is almost guaranteed.

There are some disadvantages of twisted-pair cabling. UTP cable is more prone to electrical noise and interference than other types of networking media, and the distance between signal boosts is shorter for UTP than it is for coaxial and fiber optic cables. Twisted pair cabling was once considered slower at transmitting data than other types of cable. This is no longer true. In fact, today, twisted pair is considered the fastest copper-based media..

The category of the cabling defines how many wire pairs you'll find in a given cable. Voice grade cable, also known as Category (or simply 'Cat') 3, uses only two pairs and is used for telephone service and 10Mb Ethernet. Cat 5 wiring, on the other hand, uses 4 wire pairs and is the minimum required for 100Mb Fast Ethernet. For the most part, buildings today are usually pre-wired for Cat 5, although Cat 3 may still be found in older environments. You may also come across what is known as Cat 5E – this version of Cat 5 simply has more twists per inch of wiring, providing better resistance to EMI and higher transmission capabilities.

STP :

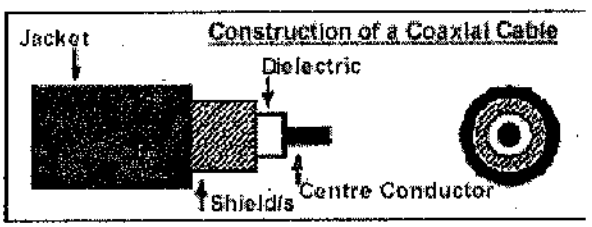
Twisted pair cables are often shielded in attempt to prevent electromagnetic interference (EMI). Because the shielding is made of metal, it may also serve as a ground. However, usually a shielded or a screened twisted pair(ScTP) cable has a special grounding wire added called a drain wire. This shielding can be applied to individual pairs, or to the collection of pairs. When shielding is applied to the collection of pairs, this is referred to as screening. The shielding must be grounded for the shielding to work.



STP cable combines the techniques of cancellation, shielded, and twisted wires. Each pair of wires is wrapped in metallic foil. The two pairs of wires are wrapped in an overall metallic braid or foil. It is usually 150-ohm cable. As specified for use in Token Ring network installations, STP reduces electrical noise within the cable such as pair to pair coupling and crosstalk. STP also reduces electronic noise from outside the cable such as electromagnetic interference (EMI) and radio frequency interference (RFI). STP cable shares many of the advantages and disadvantages of UTP cable. STP provides more protection from all types of external interference. However, STP is more expensive and difficult to install than UTP. A variation of STP, known as ScTP for "screened twisted pair" or FTP for "foil twisted pair," uses only the overall shield and provides more protection than UTP, but not as much as STP.

1.4.3 Coaxial Cable

Coaxial cable (or "coax) is the most common cable used for transmitting video signals. The name "coaxial" refers to the common axis of the two conductors.



The dielectric is surrounded by foil shield/s and/or copper braid/s which form the outer conductor and also shield against The outer conductor/shield is encased in a PVC jacket. Most coaxial cables for video applications have a nominal impedance of 75 ohms. Their differing electrical and physical characteristics make it important to select the correct type of cable to suit the application.

A coaxial cable has a solid copper or copper-clad-steel centre conductor surrounded by a non-conductive dielectric insulating material. The center conductor can also be made of tin plated aluminium cable allowing for the cable to be manufactured inexpensively. Over this insulating material is a woven copper braid or metallic foil that acts as the second wire in the circuit and as a shield against for the inner conductor. This second layer, or shield also reduces the amount of outside electromagnetic interference. Covering this shield is the cable jacket.

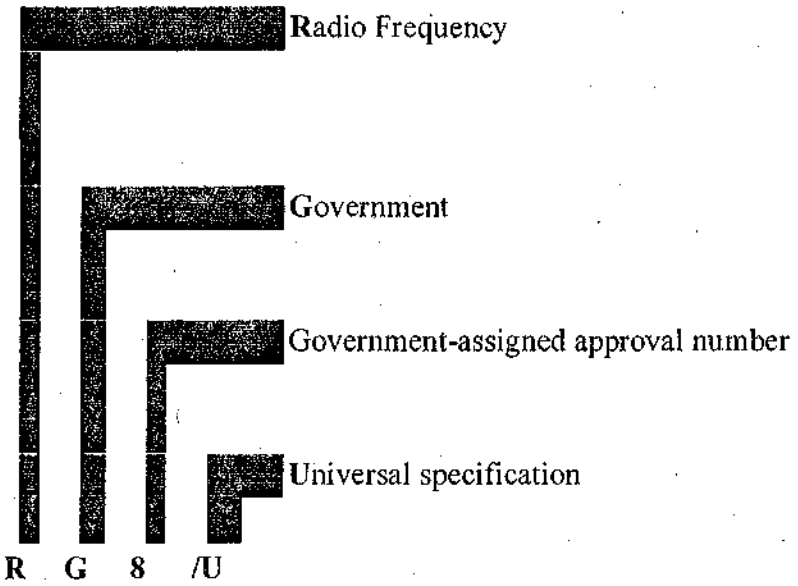
For LANs, coaxial cable offers several advantages. It can be run longer distances than shielded twisted pair, STP, unshielded twisted pair, UTP, and screened twisted pair, ScTP, cable without the need for repeaters. Repeaters regenerate the signals in a network so that they can cover greater distances. Coaxial cable is less expensive than fiber-optic cable and the technology is well known. It has been used for many years for many types of data communication such as cable television.

It is important to consider the size of a cable. As the thickness increases, it becomes more difficult to work with a cable. Remember that cable must be pulled through conduits and troughs that are limited in size. Coaxial cable comes in a variety of sizes. The largest diameter was specified for use as Ethernet backbone cable since it has greater transmission lengths and noise rejection characteristics. This type of coaxial cable is frequently referred to as Thicknet. This type of cable can be too rigid to install easily in some situations. Generally, the more difficult the network media is to install, the more expensive it is to install. Coaxial cable is more expensive to install than twisted-pair cable.

In the past, Thinnet coaxial cable with an outside diameter of only 0.35 cm was used in Ethernet networks. It was especially useful for cable installations that required the cable to make many twists and turns. Since Thinnet was easier to install, it was also cheaper to install. This led some people to refer to it as Cheapernet. The outer copper or metallic braid in coaxial cable comprises half the electric circuit. A solid electrical connection at both ends is important to properly ground the cable. Poor shield connection is one of the biggest sources of connection problems in the installation of coaxial cable. Connection problems result in electrical noise that interferes with signal transmission. For this reason Thinnet is no longer commonly used nor supported by latest standards, 100 Mbps and higher, for Ethernet networks.

Types of Coax :

Coaxial cables that conform to U.S. Government specifications are identified with an RG designation. The meaning of the individual components of the designation are:



If the letters **A**, **B** or **C** appear before the slash (/) it indicates a specification-modification or revision. As an example, RG 8/U is superseded by RG 8A/U.

The three most commonly used coaxial cable types for video applications are RG59/U, RG6/U and RG11/U.

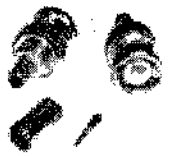
- **RG59/U** is available with either solid copper or copper-clad-steel centre conductor. It's suitable for basic analog TV antenna feeds in residential applications and for basic CCTV systems over short cable runs. The copper-clad-steel type has high tensile strength and should be used when terminating the cable with F-Type connectors.
- **RG6/U Quad-shield** is the minimum requirement under the latest Australian Standard for digital TV antenna cabling and for all TV antenna cabling for apartments/units (MATV). It is also used for the distribution of Cable TV (CATV) and Satellite TV (SATV) in residential or commercial premises. It features a copper-clad-steel inner conductor. Single-shield, dual-shield and tri-shield versions of RG6/U are available but do not provide adequate EMI shielding.
- **RG11/U Quad-shield** is used for the same applications as RG6/U for either backbone cabling or for long distribution runs. It features a copper-clad-steel inner conductor.

Choosing the correct cable :

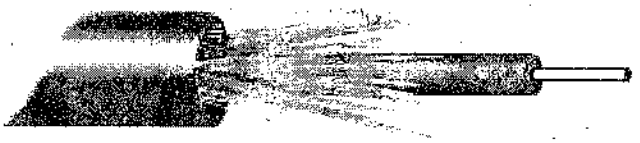
Use the table below to determine which cable should be used for your application.

Analog TV	**RG59/U**	Acceptable performance on cable runs <225 metres
	RG6/U	Gives superior performance on cable runs <225 metres.Used for cable runs >225 metres but <545 metres.
	RG11/U	For cable runs greater than 545 metres.
CCTV	**RG59/U**	Acceptable performance on cable runs <225 metres
	RG6/U	Gives for superior performance on cable runs <225 metres.Used for cable runs >225 metres but <545 metres.
	RG11/U	For cable runs greater than 545 metres.
DTV, CATV, SATV, MATV	**RG6/U** **RG11/U**	Standard cable for these applications Recommended for long cable runs and for backbone cabling.

Coaxial Connectors

	**BNC connector** are bayonet type connectors, commonly used in CCTV systems. They are the most suitable connector for use with RG59/U cable. BNC connectors are specified by IEC standard IEC60169-8. The argument, over what the "BNC" in "BNC connector" means, will go on forever. It has been variously defined as: British Navy Connector, Bayonet Node Connector, Bayonet Nut Coupling, Baby Neil Connector, etc. The two Amphenol engineers who invented the BNC connector were named Paul Neil and Carl Concelman. It therefore seems logical that the "true" meaning of the "BNC" acronym is perhaps "Bayonet Neil-Concelman".
	**F-Type connectors** are used for CATV, SATV and Digital TV in conjunction with either RG6 or RG11 cables. The copper-clad-steel inner conductor of the cable forms the inner "pin" of the connector. Although "twist-on" type connectors are available, they do not produce a reliable connection in comparison to a crimp-type connector that has been terminated with a good-quality ratchet crimping tool. F-type connectors are also known as F-81 connectors and are specified by IEC standard IEC60169-24. F-type connectors are named according to the type of cable or the application that they have been designed for as shown in the table below.

that light can take through the fiber, the fiber is called "multimode" fiber. Single-mode fiber has a much smaller core that only allows light rays to travel along one mode inside the fiber.



Properties of light rays:

When electromagnetic waves travel out from a source, they travel in straight lines. These straight lines pointing out from the source are called rays. Think of light rays as narrow beams of light like those produced by lasers. In the vacuum of empty space, light travels continuously in a straight line at 300,000 kilometers per second. However, light travels at different, slower speeds through other materials like air, water, and glass. When a light ray called the incident ray, crosses the boundary from one material to another, some of the light energy in the ray will be reflected back. That is why you can see yourself in window glass. The light that is reflected back is called the reflected ray.

The light energy in the incident ray that is not reflected will enter the glass. The entering ray will be bent at an angle from its original path. This ray is called the refracted ray. How much the incident light ray is bent depends on the angle at which the incident ray strikes the surface of the glass and the different rates of speed at which light travels through the two substances.

The bending of light rays at the boundary of two substances is the reason why light rays are able to travel through an optical fiber even if the fiber curves in a circle.

The optical density of the glass determines how much the rays of light in the glass bends. Optical density refers to how much a light ray slows down when it passes through a substance. The greater the optical density of a material, the more it slows light down from its speed in a vacuum. The index of refraction is defined as the speed of light in vacuum divided by the speed of light in the medium. Therefore, the measure of the optical density of a material is the index of refraction of that material. A material with a large index of refraction is more optically dense and slows down more light than a material with a smaller index of refraction.

For a substance like glass, the Index of Refraction, or the optical density, can be made larger by adding chemicals to the glass. Making the glass very pure can make the index of refraction smaller. The next lessons will provide further information about reflection and refraction, and their relation to the design and function of optical fiber

An overview of reflection:

When a ray of light (the incident ray) strikes the shiny surface of a flat piece of glass, some of the light energy in the ray is reflected. The angle between the incident ray and a line perpendicular to the surface of the glass at the point where the incident ray strikes the glass is called the angle of incidence. The perpendicular line is called the normal. It is not a light ray but a tool to allow the measurement of angles. The angle between the reflected ray and the normal is called the angle of reflection. The Law of Reflection states that the angle of reflection of a light ray is equal to the angle of incidence. In other words, the angle at which

Connector Name	Application / Description
F-59A male F-6 (F-56) F-11	F-connector that seizes the outer braid and jacket of an RG-59, RG-6 (RG-56) or RG-11 coaxial cable. The cable's centre conductor extends through the connector to form the centre contact.
F-61	An equipment or panel-mounted F-connector (usually female) with soldered cable connections. A 3/8" (32 pitch) thread is provided to accept the connector nut of the male connector.
F-71	A male/male F-connector.
F-81A	female/female F-connector used to couple two male-ended cables together for in-line or wall-plate applications.

PAL (Belling Lee) connectors are a push-on connector that have been traditionally used for TV antenna wall plates and connections. With the exception of TV/VCR hook-ups, PAL connectors are being replaced by F-Type connectors as required for CATV, SATV and DTV. PAL connectors are specified by IEC standard IEC60169-2.

Adaptors. Where BNC connectors are required with RG6/U coaxial cable, it is recommended that an F-Type plug be crimped to the RG6/U and an F-Type to BNC adaptor used.

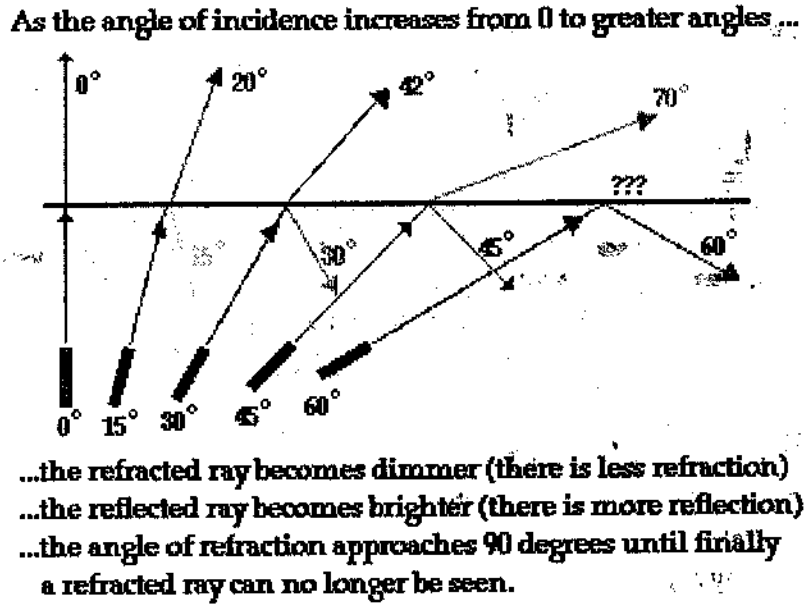
1.4.4 Fiber Optics

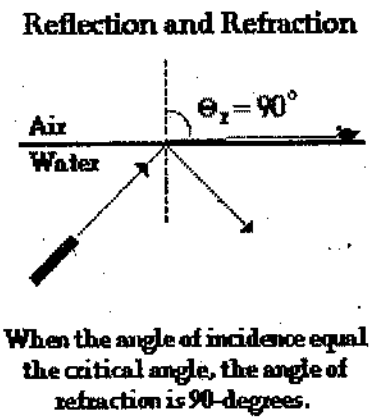
Optical fiber is the most frequently used medium for the longer, high bandwidth, point-to-point transmissions required on LAN backbones and on WANs. Optical media uses light to transmit data through thin glass or plastic fiber. Electrical signals cause a fiber-optic transmitter to generate the light signals sent down the fiber. The receiving host receives the light signals and converts them to electrical signals at the far end of the fiber. However, there is no electricity in the fiber-optic cable. In fact, the glass used in fiber-optic cable is a very good electrical insulator.

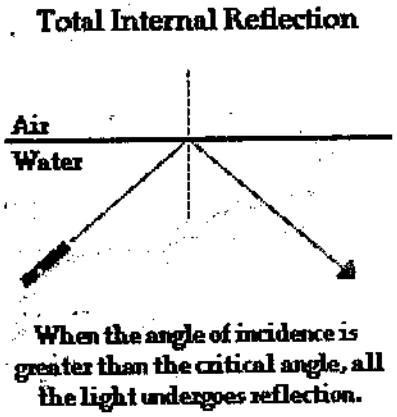
The part of an optical fiber through which light rays travel is called the core of the fiber. Light rays can only enter the core if their angle is inside the numerical aperture of the fiber. Likewise, once the rays have entered the core of the fiber, there are a limited number of optical paths that a light ray can follow through the fiber. These optical paths are called modes. If the diameter of the core of the fiber is large enough so that there are many paths

a light ray strikes a reflective surface determines the angle that the ray will reflect off the surface.

These principles are depicted in the diagram below.







An overview of refraction:

When a light strikes the interface between two transparent materials, the light divides into two parts. Part of the light ray is reflected back into the first substance, with the angle of reflection equaling the angle of incidence. The remaining energy in the light ray crosses the interface and enters into the second substance.

If the incident ray strikes the glass surface at an exact 90-degree angle, the ray goes straight into the glass. The ray is not bent. However, if the incident ray is not at an exact 90-degree angle to the surface, then the transmitted ray that enters the glass is bent. The bending of the entering ray is called refraction. How much the ray is refracted depends on the index of refraction of the two transparent materials. If the light ray travels from a substance whose index of refraction is smaller, into a substance where the index of refraction is larger, the refracted ray is bent towards the normal. If the light ray travels from a substance where the index of refraction is larger into a substance where the index of refraction is smaller, the refracted ray is bent away from the normal.

Consider a light ray moving at an angle other than 90 degrees through the boundary between glass and a diamond. The glass has an index of refraction of about 1.523. The diamond has an index of refraction of about 2.419. Therefore, the ray that continues into the diamond will be bent towards the normal. When that light ray crosses the boundary between the diamond and the air at some angle other than 90 degrees, it will be bent away from the normal. The reason for this is that air has a lower index of refraction, about 1.000 than the index of refraction of the diamond.

Total internal reflection as it relates to optical media

A light ray that is being turned on and off to send data (1s and 0s) into an optical fiber must stay inside the fiber until it reaches the far end. The ray must not refract into the material wrapped around the outside of the fiber. The refraction would cause the loss of part of the light energy of the ray. A design must be achieved for the fiber that will make the outside surface of the fiber act like a mirror to the light ray moving through the fiber. If any light ray that tries to move out through the side of the fiber were reflected back into the fiber at an angle that sends it towards the far end of the fiber, this would be a good "pipe" or "wave guide" for the light waves.

The laws of reflection and refraction illustrate how to design a fiber that guides the light waves through the fiber with a minimum energy loss. The following two conditions must be met for the light rays in a fiber to be reflected back into the fiber without any loss due to refraction:

- The core of the optical fiber has to have a larger index of refraction (n) than the material that surrounds it. The material that surrounds the core of the fiber is called the cladding.
- The angle of incidence of the light ray is greater than the critical angle for the core and its cladding.

When both of these conditions are met, the entire incident light in the fiber is reflected back inside the fiber. This is called total internal reflection, which is the foundation upon which optical fiber is constructed. Total internal reflection causes the light rays in the fiber to bounce off the core-cladding boundary and continue its journey towards the far end of the fiber. The light will follow a zigzag path through the core of the fiber.

A fiber that meets the first condition can be easily created. In addition, the angle of incidence of the light rays that enter the core can be controlled. Restricting the following two factors controls the angle of incidence:

- **The numerical aperture of the fiber** – The numerical aperture of a core is the range of angles of incident light rays entering the fiber that will be completely reflected.

- **Modes** – The paths which a light ray can follow when traveling down a fiber.

By controlling both conditions, the fiber run will have total internal reflection. This gives a light wave guide that can be used for data communications.

Self Learning Exercises :

4 Why are pairs of wires twisted together in UTP cable :

(a) twisting of wires makes it less expensive

(b) twisting of wires makes it thinner

(c) twisting of reduces noise problems

(d) makes six pairs fit in space of four pairs

5 Which material is considered electrical semiconductor :

(a) Air (b) Silicon

(c) Glass (d) Gold

6 Which of the following are the parts of fiber optic cable :

(a) Clad (b) Braid

(c) Core (d) All of the above

1.5 NETWORKING ESSENTIALS

1.5.1 Repeaters

A repeater connects two segments of your network cable. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. When talking about, ethernet topology, you are probably talking about using a hub as a repeater. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work only at the physical layer of the OSI network model.

1.5.2 Hubs

Hubs are actually multiport repeaters. The difference between hubs and repeaters is usually the number of ports that each device provides. A typical repeater usually has two ports. A hub generally has from 4 to 24 ports. Hubs are most commonly used in Ethernet 10BASE-T or 100BASE-T networks.

Hubs come in three basic types:

- **Passive** – A passive hub serves as a physical connection point only. It does not manipulate or view the traffic that crosses it. It does not boost or clean the signal. A passive hub is used only to share the physical media. A passive hub does not need electrical power.
- **Active** – An active hub must be plugged into an electrical outlet because it needs power to amplify a signal before it is sent to the other ports.
- **Intelligent** – Intelligent hubs are sometimes called smart hubs. They function like active hubs with microprocessor chips and diagnostic capabilities. Intelligent hubs are more expensive than active hubs. They are also more useful in troubleshooting situations.

Devices attached to a hub receive all traffic that travels through the hub. If many devices are attached to the hub, collisions are more likely to occur. A collision occurs when two or more workstations send data over the network wire at the same time. All data is corrupted when this occurs. All devices that are connected to the same network segment are members of the same collision domain.

Sometimes hubs are called concentrators since they are central connection points for Ethernet LANs.

1.5.3 Switches

Switches occupy the same place in the network as hubs. Unlike hubs, switches examine each packet and process it accordingly rather than simply repeating the signal to all ports. Switches map the Ethernet addresses of the nodes residing on each network segment and then allow only the necessary traffic to pass through the switch. When a packet is received by the switch, the switch examines the destination and source hardware addresses and compares them to a table of network segments and addresses. If the segments are the same, the packet is dropped ("filtered"); if the segments are different, then the packet is "forwarded" to the proper segment. Additionally, switches prevent bad or misaligned packets from spreading by not forwarding them.

Filtering of packets, and the regeneration of forwarded packets enables switching technology to split a network into separate collision domains. Regeneration of packets allows for greater distances and more nodes to be used in the total network design, and dramatically lowers the overall collision rates. In switched networks, each segment is an independent collision domain. In shared networks all nodes reside in one, big shared collision domain.

Easy to install, most switches are self learning. They determine the Ethernet addresses in use on each segment, building a table as packets are passed through the switch. This "plug and play" element makes switches an attractive alternative to hubs.

Switches can connect different networks types (such as Ethernet and Fast Ethernet) or networks of the same type. Many switches today offer high-speed links, like Fast Ethernet or FDDI, that can be used to link the switches together or to give added bandwidth to important servers that get a lot of traffic. A network composed of a number of switches linked together via these fast uplinks is called a "collapsed backbone" network.

Dedicating ports on switches to individual nodes is another way to speed access for critical computers. Servers and power users can take advantage of a full segment for one node, so some networks connect high traffic nodes to a dedicated switch port.

Full duplex is another method to increase bandwidth to dedicated workstations or servers. To use full duplex, both network interface cards used in the server or workstation, and the switch must support full duplex operation. Full duplex doubles the potential bandwidth on that link, providing 20 Mbps for Ethernet and 200 Mbps for Fast Ethernet.

Bridge

A bridge reads the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets. Bridges can be programmed to reject packets from particular networks. Bridging occurs at the data link layer of the OSI model, which means the bridge cannot read IP addresses, but only the outermost hardware address of the packet. In our case the bridge can read the ethernet data which gives the hardware address of the destination address, not the IP ad-

dress. Bridges forward all broadcast messages. Only a special bridge called a translation bridge will allow two networks of different architectures to be connected. Bridges do not normally allow connection of networks with different architectures. The hardware address is also called the MAC (media access control) address. To determine the network segment a MAC address belongs to, bridges use one of:

- **Transparent Bridging** - They build a table of addresses (bridging table) as they receive packets. If the address is not in the bridging table, the packet is forwarded to all segments other than the one it came from. This type of bridge is used on Ethernet networks.
- **Source route bridging** - The source computer provides path information inside the packet. This is used on Token Ring networks.

1.5.4 Router

A router is used to route data packets between two networks. It reads the information in each packet to tell where it is going. If it is destined for an immediate network it has access to, it will strip the outer packet, readdress the packet to the proper Ethernet address, and transmit it on that network. If it is destined for another network and must be sent to another router, it will re-package the outer packet to be received by the next router and send it to the next router. The section on routing explains the theory behind this and how routing tables are used to help determine packet destinations. Routing occurs at the network layer of the OSI model. They can connect networks with different architectures such as Token Ring and Ethernet. Although they can transform information at the data link level, routers cannot transform information from one data format such as TCP/IP to another such as IPX/SPX. Routers do not send broadcast packets or corrupted packets. If the routing table does not indicate the proper address of a packet, the packet is discarded.

There is a device called a brouter which will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols. It functions at the network and data link layers of the OSI network model.

1.5.5 Gateways

A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model. Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model. To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. This does not mean the routing machine is a gateway as defined here, although it could be.

1.5.6 NIC (Network interface Card)

Each network card, called a network interface card **(NIC)** has a built in hardware address programmed by its manufacturer. This is a 48 bit address and should be unique for each card. This address is called a media access control **(MAC)** address.

Network Interface Cards, commonly referred to as NICs, are used to connect a PC to a network. The NIC provides a physical connection between the networking cable and the computer's internal bus. Different computers have different bus architectures. PCI bus

slots are most commonly found on 486/Pentium PCs and ISA expansion slots are commonly found on 386 and older PCs. NICs come in three basic varieties: 8-bit, 16-bit, and 32-bit. The larger the number of bits that can be transferred to the NIC, the faster the NIC can transfer data to the network cable. Most NICs are designed for a particular type of network, protocol, and medium, though some can serve multiple networks.

Many NIC adapters comply with plug-and-play specifications. On these systems, NICs are automatically configured without user intervention, while on non-plug-and-play systems, configuration is done manually through a set-up program and/or DIP switches.

Cards are available to support almost all networking standards. Fast Ethernet NICs are often 10/100 capable, and will automatically set to the appropriate speed. Gigabit Ethernet NICs are 10/100/1000 capable with auto negotiation depending on the user's Ethernet speed. Full duplex networking is another option where a dedicated connection to a switch allows a NIC to operate at twice the speed.

Self learning exercises:

7 What is the function of router?

(a) It routes traffic from one LAN segment to another

(b) It regenerates the data

(c) It transforms the data from one format to another

(d) None of the above

8 What is multiport repeater called as?

(a) Hub (b) Switch

(c) Router (d) Gateway

9 What is the Gateway?

(a) It is used to connect two totally dissimilar networks

(b) It regenerates and retransmits signals from one network to another

(c) It acts as a bridge between two networks

(d) It is used to change the format of the message

1.6 SUMMARY

Computer networks developed in response to business and government computing needs. Applying standards to network functions provided a set of guidelines for creating network hardware and software and provided compatibility among equipment from different companies. Information could move within a company and from one business to another.

Network devices, such as repeaters, hubs, bridges, switches and routers connect host devices together to allow them to communicate. Protocols provide a set of rules for communication.

The amount of information that can flow through a network connection in a given period of time is referred to as bandwidth. Network bandwidth is typically measured in thousands of bits per second (kbps), millions of bits per second (Mbps), billions of bits per second (Gbps) and trillions of bits per second (Tbps). The theoretical bandwidth of a network is an important consideration in network design. If the theoretical bandwidth of a network connection is known, the formula T=S/BW (transfer time = size of file / bandwidth) can be

used to calculate potential data transfer time. However the actual bandwidth, referred to as throughput, is affected by multiple factors such as network devices and topology being used, type of data, number of users, hardware and power conditions.

Intranets are only available to users who have access privileges to the internal network of an organization. Extranets are designed to deliver applications and services that are Intranet based to external users or enterprises.

1.7 GLOSSARY

- **Attenuation** - signal loss due to impedance
- **Backbone** - Main cable used to connect computers on a network.
- **Bandwidth** - Indicates the amount of data that can be sent in a time period. Measured in Mbps which is one million bits per second.
- **Baseband** - Data bits are defined by discrete signal changes.
- **Bridge** - Read the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets but only sends packets intended for that segment they are attached to.
- **Broadband** - Uses analog signals to divide the cable into several channels with each channel at its own frequency. Each channel can only transmit one direction.
- **Broadcast** - A transmission to all interface cards on the network.
- **Brouter** - Will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols.
- **EMI interference)** - Interference by electromagnetic signals that can cause reduced data integrity **(electromagnetic** and increased error rates on transmission channels.
- **Media** - The hardware method used to connect computers over a network. The three main types are copper cable, fiber optic cable, and wireless.
- **Protocol** - A set of standards sets of standards that define all operations within a network. There are various protocols that operate at various levels of the OSI network model such as transport protocols include TCP, SPX.
- **Repeater** - Used on a network to regenerate signals to be sent over long distances or tie computers together on a network.
- **Router** - Routes data packets between two networks. It reads the information in each packet to tell where it is going.
- **Thicknet** - Half inch rigid cable. Maximum cable length is 500 meters. Transmission speed is 10Mbps. Expensive and is not commonly used. (RG-11 or RG-8).

- **Thinnet** - Thinnet uses a British Naval Connector (BNC) on each end. Thinnet is part of the RG-58 family of cable*. Maximum cable length is 185 meters. Transmission speed is 10Mbps.
- **Token Ring** - A network architecture developed by IBM which sends tokens around a ring of computers to allow media access. Standardized to IEEE 802.5
- **Topology** - The shape of the physical connection of a network with regard to repeaters and networked computers. The three main types are ring, bus, and star.
- **VPN** - Virtual Private Networking. The function of VPN is to allow two computers or networks to talk to each other over a transport media that is not secure, but the network is made secure by VPN security protocols.

1.8 FURTHER READINGS

1. Data Communication & Networking - Behrouz Forouzan
2. CCNA (Cisco Certified Network Associate) First year Companion Guide - Cisco Press
3. Computer Networks – Andrew Tanenbaum; Prentice Hall India(PHI)

1.9 ANSWERS TO THE SELF LEARNING EXERCISES

1. d
2. c
3. c
4. c
5. b
6. d
7. a
8. a
9. a

1.10 UNIT END QUESTIONS

1. How do guided media differ from unguided media.
2. Name the advantages of optical fiber over twisted-pair and coaxial cable.
3. Why is coaxial cable superior to twisted pair cable?
4. What is reflection? How is total internal reflection used in fiber optics for communication?
5. What is major advantage of shielded twisted pair over un-shielded twisted Pair?
6. What is the device Router used for?
7. What is the function of Repeater?
8. Differentiate between Switch and Bridge?
9. What is the significance of NIC?
10. List out various Internet applications.

UNIT II

COMPUTER NETWORK CONTD

STRUCTURE OF THE UNIT

2.0 Objective
2.1 Introduction
2.2 Type of Networks
2.2.1 LAN
2.2.2 MAN
2.2.3 WAN
2.2.4 Wireless Networks
2.3 Network Topologies
2.3.1 Bus
2.3.2 Ring
2.3.3 Star
2.3.4 Tree
2.3.5 Mesh
2.4 Reference Models
2.4.1 OSI
2.4.2 TCP/IP
2.5 Summary
2.6 Glossary
2.7 Further Readings
2.8 Answers to the self learning exercises
2.9 Unit end questions

2.0 OBJECTIVE

Students who complete this unit should be able to understand the following tasks:

- Types of Networks
- Introduction to Wireless networks
- Architecture of Networks
- Reference models - OSI
- Architecture of TCP/IP

2.1 INTRODUCTION

In the mid-1980s, the network technologies that emerged were created with a variety of hardware and software implementations. Each company that created network hardware and software used its own company standards. These individual standards were developed because of competition with other companies. As a result, many of the network technologies were incompatible with each other. It became increasingly difficult for networks that used different specifications to communicate with each other. Network equipment often

had to be replaced to implement new technologies.

One early solution was the creation of local-area network (LAN) standards. LAN standards provided an open set of guidelines that companies used to create network hardware and software. As a result, the equipment from different companies became compatible. This allowed for stability in LAN implementations.

In a LAN system, each department of the company is a kind of electronic island. As the use of computers in businesses grew, LANs became insufficient. A new technology was necessary to share information efficiently and quickly within a company and between businesses. The solution was the creation of metropolitan-area networks (MANs) and wide-area networks (WANs). Because WANs could connect user networks over large geographic areas, it was possible for businesses to communicate with each other across great distances.

In the mid-1980s PC users began to use modems to share files with other computers. This was referred to as point-to-point, or dial-up communication. This concept was expanded by the use of computers that were the central point of communication in a dial-up connection. These computers were called bulletin boards. Users would connect to the bulletin boards, leave and pick up messages, as well as upload and download files. The drawback to this type of system was that there was very little direct communication and then only with those who knew about the bulletin board. Another limitation was that the bulletin board computer required one modem per connection. If five people connected simultaneously it would require five modems connected to five separate phone lines. As the number of people who wanted to use the system grew, the system was not able to handle the demand. For example, imagine if 500 people wanted to connect at the same time.

From the 1960s to the 1990s the U.S. Department of Defense (DoD) developed large, reliable, wide-area networks (WANs) for military and scientific reasons. This technology was different from the point-to-point communication used in bulletin boards. It allowed multiple computers to be connected together through many different paths. The network itself would determine how to move data from one computer to another. One connection could be used to reach many computers at the same time. The WAN developed by the DoD eventually became the Internet.

2.2 TYPES OF NETWORKS

A **network** is two or more computers that have been connected for the purposes of exchanging data and sharing resources. Networked shared resources range from printers, CD-ROMs, and modems to files and hard drives. Networks vary in size and scope.

There are two main types of network categories which are:

- Server based
- Peer-to-peer

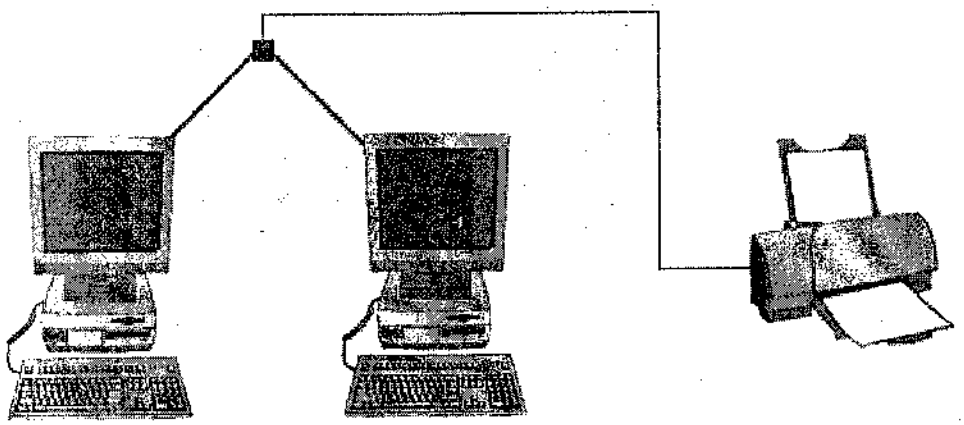
In a server based network, there are computers set up to be primary providers of services such as file service or mail service. The computers providing the service are called servers and the computers that request and use the service are called client computers.

In a peer-to-peer network, various computers on the network can act both as clients and servers. For instance, many Microsoft Windows based computers will allow file and print sharing. These computers can act both as a client and a server and are also referred to as peers. Many networks are combination peer-to-peer and server based networks. The net-

work operating system uses a network data protocol to communicate on the network to other computers. The network operating system supports the applications on that computer. A Network Operating System (NOS) includes Windows NT, Novell Netware, Linux, Unix and others.

Many types of computer networks exist, but you need only be concerned with the following:

Peer-to-peer network: This type of network includes two or more PCs that are connected to share data files, a printer, or other resources.



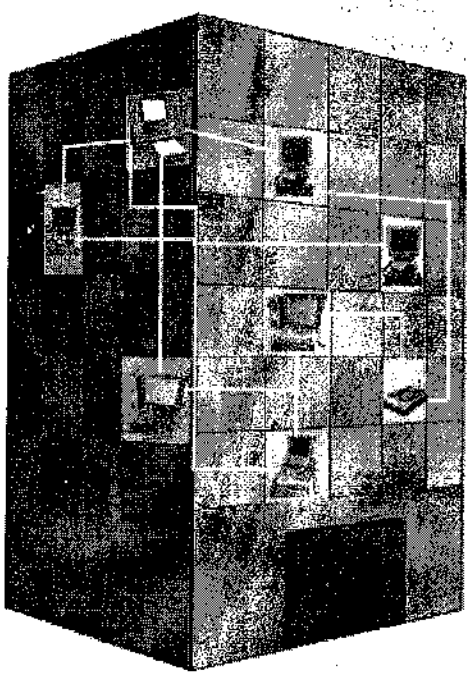
A physical connection is made by connecting an adapter card, such as a modem or a NIC, from a PC to a network. The physical connection is used to transfer signals between PCs within the local-area network (LAN) and to remote devices on the Internet.

The logical connection uses standards called protocols. A protocol is a formal description of a set of rules and conventions that govern how devices on a network communicate. Connections to the Internet may use multiple protocols. The Transmission Control Protocol/Internet Protocol (TCP/IP) suite is the primary set of protocols used on the Internet. The TCP/IP suite works together to transmit and receive data, or information.

In describing the basics of networking technology, it will be helpful to explain the different types of networks in use.

2.2.1 Local Area Networks (LANs)

A network is any collection of independent computers that exchange information with each other over a shared communication medium. Local Area Networks or LANs are usually confined to a limited geographic area, such as a single building or a college campus. LANs can be small, linking as few as three computers, but can often link hundreds of computers used by thousands of people. The development of standard networking protocols and media has resulted in worldwide proliferation of LANs throughout business and educational organizations. A small business or corporate department may install a LAN that interconnects from two to hundreds of PCs, using permanently installed cabling or perhaps a wireless technology.



Types of LAN Technology

Ethernet

Ethernet is the most popular physical layer LAN technology in use today. It defines the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and LocalTalk.

Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

Fast Ethernet

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

Network managers who want to incorporate Fast Ethernet into an existing configuration are required to make many decisions. The number of users in each site on the network that need the higher throughput must be determined; which segments of the backbone need to be reconfigured specifically for 100BASE-T; plus what hardware is necessary in order to connect the 100BASE-T segments with existing 10BASE-T segments. Gigabit Ethernet is a future technology that promises a migration path beyond Fast Ethernet so the next generation of networks will support even higher data transfer speeds.

Gigabit Ethernet

Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Also known as "gigabit-Ethernet-over-copper" or 1000Base-T, GigE is a version of Ethernet that runs at speeds 10 times faster than 100Base-T. It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.

From the data link layer of the OSI model upward, the look and implementation of Gigabit Ethernet is identical to that of Ethernet. The most important differences between Gigabit Ethernet and Fast Ethernet include the additional support of full duplex operation in the MAC layer and the data rates.

10 Gigabit Ethernet

10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.

Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing. As it is still very new, which of the standards will gain commercial acceptance has yet to be determined.

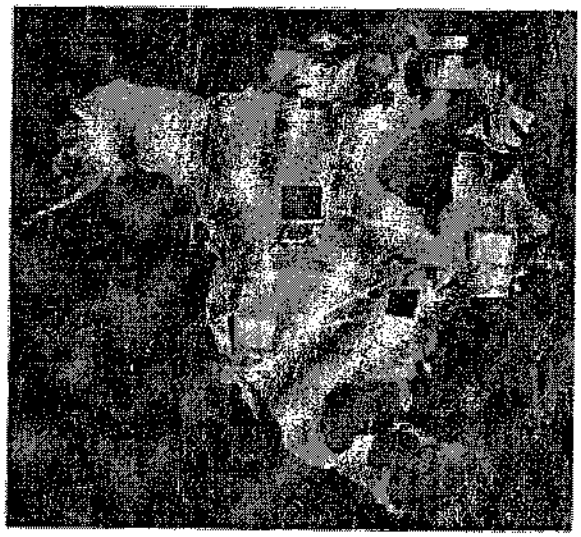
2.2.2 Metropolitan Area Network (MAN)

A network that spans a metropolitan area. Generally, a MAN spans a larger geographic area than a LAN, but a smaller geographic area than a WAN.

2.2.3 Wide Area Networks (WAN)

Often elements of a network are widely separated physically. Wide area networking combines multiple LANs that are geographically separate. This is accomplished by connecting the several LANs with dedicated leased lines such as a T1 or a T3, by dial-up phone lines (both synchronous and asynchronous), by satellite links and by data packet carrier services. WANs can be as simple as a modem and a remote access server for employees to dial into, or it can be as complex as hundreds of branch offices globally linked. Special routing protocols and filters minimize the expense of sending data over vast distances. A

corporation may maintain a WAN using dialup, leased, or other dedicated communication means.



2.2.4 Wireless Local Area Networks (WLANs)

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network.

Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless LANs have several disadvantages. They provide poor security, and are susceptible to interference from lights and electronic devices. They are also slower than LANs using cabling.

Wireless LANs, or WLANs, use radio frequency (RF) technology to transmit and receive data over the air. This minimizes the need for wired connections. WLANs give users mobility as they allow connection to a local area network without having to be physically

connected by a cable. This freedom means users can access shared resources without looking for a place to plug in cables, provided that their terminals are mobile and within the designated network coverage area. With mobility, WLANs give flexibility and increased productivity, appealing to both entrepreneurs and to home users. WLANs may also enable network administrators to connect devices that may be physically difficult to reach with a cable.

The Institute for Electrical and Electronic Engineers (IEEE) developed the 802.11 specification for wireless LAN technology. 802.11 specifies over-the-air interface between a wireless client and a base station, or between two wireless clients. WLAN 802.11 standards also have security protocols that were developed to provide the same level of security as that of a wired LAN.

The first of these protocols is Wired Equivalent Privacy (WEP). WEP provides security by encrypting data sent over radio waves from end point to end point.

The second WLAN security protocol is Wi-Fi Protected Access (WPA). WPA was developed as an upgrade to the security features of WEP. It works with existing products that are WEP-enabled but provides two key improvements: improved data encryption through the temporal key integrity protocol (TKIP) which scrambles the keys using a hashing algorithm. It has means for integrity-checking to ensure that keys have not been tampered with. WPA also provides user authentication with the extensible authentication protocol (EAP).

Wireless Protocols

Specification	Data Rate	Modulation Scheme	Security
802.11	1 or 2 Mbps in the 2.4 GHz band	FHSS, DSSS	WEP and WPA
802.11a	54 Mbps in the 5 GHz band	OFDM	WEP and WPA
802.11b/High Rate/Wi-Fi	11 Mbps (with a fallback to 5.5, 2, and 1 Mbps) in the 2.4 GHz band	DSSS with CCK	WEP and WPA
802.11g/Wi-Fi	54 Mbps in the 2.4 GHz band	OFDM when above 20Mbps, DSSS with CCK when below 20Mbps	WEP and WPA

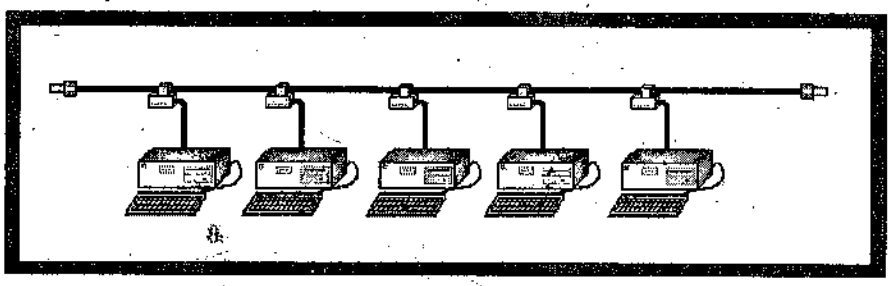
2.3 TOPOLOGIES

The network topology describes the method used to do the physical wiring of the network. It is the geometric arrangement of nodes and cable links in a LAN. A node is an active device connected to the network, such as a computer or a printer. A node can also be a piece of networking equipment such as a hub, switch or a router. The main ones are bus, star, and ring.

There are also hybrid networks including a star-bus hybrid, star-ring network, and mesh networks with connections between various computers on the network. Mesh networks ideally allow each computer to have a direct connection to each of the other computers.

2.3.1 Bus

The simplest topology to understand is the Bus. In a Bus, all the devices on the network are connected to a common cable. Normally, this cable is terminated at either end, and can never be allowed to form a closed loop. The following figure shows an example of a Bus network.

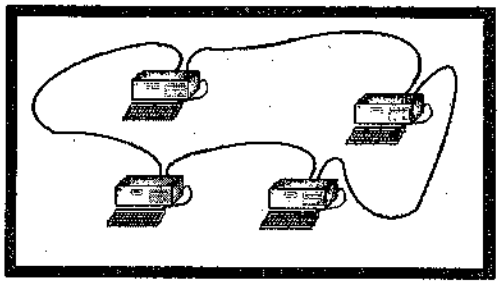


Bus Topology

2.3.2 Ring

A Ring topology is very similar to the Bus. In a Ring, all the devices on the network are connected to a common cable which loops from machine to machine. After the last machine on the network, the cable then returns to the first device to form a closed loop. The following figure shows an example of a Ring network.

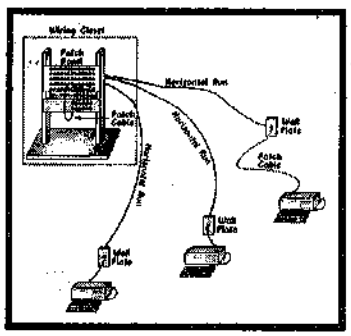
Ring Topology



2.3.3 Star

A star topology is completely different from either a Bus or a Ring. In a Star. each device has its own cable run connecting the device to a common hub or concentrator. Only one device is permitted to use each port on the hub. The following figure shows an example of a Star network.

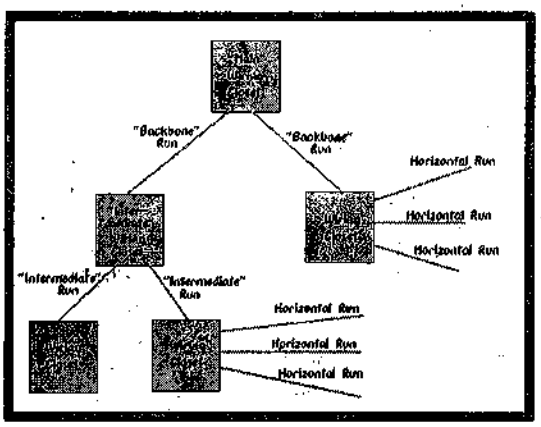
Star Topology



2.3.4 Tree

A tree topology can be thought of as being a "Star of Stars" network. In a Tree network, each device is connected to its own port on a concentrator in the same manner as in a Star. However, concentrators are connected together in a heirarchial manner — i.e. a hub will connect to a port on another hub. The following figure shows a Tree network.

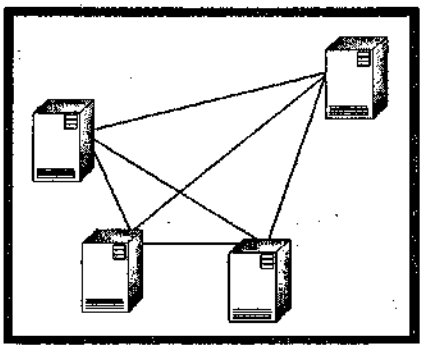
Tree Topology



2.3.5 Mesh

A Mesh topology consists of a network where every device on the network is physically connected to every other device on the network. This provides a great deal of performance and reliability, however the complexity and difficulty of creating one increases geometrically as the number of nodes on the network increases. For example, a three or four node mesh network is relatively easy to create, whereas it is impractical to set up a mesh network of 100 nodes — the number of interconnections would be so ungainly and expensive that it would not be worth the effort. Mesh networks are not used much in local area networks (LANs) but are used in Wide Area Networks (WANs) where reliability is important and the number of sites being connected together is fairly small. The following figure shows an example of a four-node Mesh network.

Mesh Topology



There are two types of mesh topologies: full mesh and partial mesh.

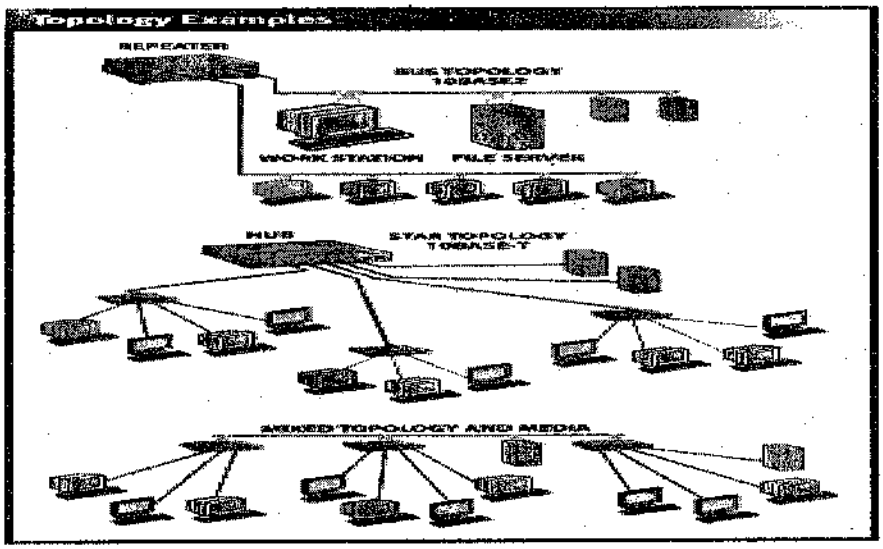
Full mesh topology occurs when every node has a circuit connecting it to every other node in a network. Full mesh is very expensive to implement but yields the greatest amount of redundancy, so in the event that one of those nodes fails, network traffic can be directed to any of the other nodes. Full mesh is usually reserved for backbone networks.

Partial mesh topology is less expensive to implement and yields less redundancy than full mesh topology. With partial mesh, some nodes are organized in a full mesh scheme but others are only connected to one or two in the network. Partial mesh topology is commonly found in peripheral networks connected to a full meshed backbone.

The topology this documentation deals with most is star topology since that is what ethernet networks use.

General Topology Configurations

10BASE-T Ethernet and Fast Ethernet use a star topology where access is controlled by a central computer. Generally a computer is located at one end of the segment, and the other end is terminated in central location with a hub or a switch. Because UTP is often run in conjunction with telephone cabling, this central location can be a telephone closet or other area where it is convenient to connect the UTP segment to a backbone. The primary advantage of this type of network is reliability, for if one of these 'point-to-point' segments has a break; it will only affect the two nodes on that link. Other computer users on the network continue to operate as if that segment were non-existent.



Collisions

Ethernet is a shared medium, so there are rules for sending packets of data to avoid conflicts and to protect data integrity. Nodes determine when the network is available for sending packets. It is possible that two or more nodes at different locations will attempt to send data at the same time. When this happens, a packet collision occurs.

Minimizing collisions is a crucial element in the design and operation of networks. Increased collisions are often the result of too many users on the network. This leads to competition for network bandwidth and can slow the performance of the network from the user's point of view. Segmenting the network is one way of reducing an overcrowded network, i.e., by dividing it into different pieces logically joined together with a bridge or switch.

CSMA/CD

In order to manage collisions Ethernet uses a protocol called Carrier Sense Multiple Access/ Collision Detection (CSMA/CD). CSMA/CD is a type of contention protocol that defines how to respond when a collision is detected, or when two devices attempt to transmit packages simultaneously. Ethernet allows each device to send messages at any time without having to wait for network permission; thus, there is a high possibility that devices may try to send messages at the same time.

After detecting a collision, each device that was transmitting a packet delays a random amount of time before re-transmitting the packet. If another collision occurs, the device waits twice as long before trying to re-transmit.

Self Learning Exercises:

1. Which of the following will cause collision in an Ethernet network?
   (a) two nodes having the same MAC addresses
   (b) two or more nodes transmitting at the same time
   (c) non-OSI compliant protocols running on the network
   (d) multiple protocols running on the same network
2. Which of the following physical topologies are used with 10Base-T Ethernet network?
   (a) Mesh (b) Star
   (c) Bus (d) Hybrid
3. Which layer of OSI model deals with bit time and timing for Standard Ethernet, Fast Ethernet and Gigabit Ethernet?
   (a) Session (b) Presentation
   (c) Physical (d) Application
4. Which topology is considered to be the most reliable?
   (a) Tree (b) Mesh
   (c) Star (d) Bus

2.4 REFERENCE MODELS

The Internet was developed based on the standards of the TCP/IP protocols. The TCP/IP model gains credibility because of its protocols. The OSI model is not generally used to build networks. The OSI model is used as a guide to help students understand the communication process.

Open System Interconnection reference model is a network architectural model developed by International Organization for Standardization (ISO) and International Telecommunication Union Telecommunication Standardization Sector (ITU-T). The model consists of seven layers, each of which specifies particular network functions such as addressing, flow control, error control, encapsulation, and reliable message transfer. The highest layer (the application layer) is closest to the user. The lowest layer (the physical layer) is closest to the media technology. The next to lowest layers are implemented in hardware and software, while the upper five layers are implemented only in software. The OSI reference

model is used universally as a method for teaching and understanding network functionality.

2.4.1 OSI - The Open System Interconnection Model

Another standard architectural model that is often used to describe a network protocol stack is the OSI reference model. This model consists of a seven layer protocol stack (see Figure A-2). The Open System Interconnection (OSI) model specifies how dissimilar computing devices such as Network Interface Cards (NICs), bridges and routers exchange data over a network by offering a networking framework for implementing protocols in seven layers. Beginning at the application layer, control is passed from one layer to the next. The following describes the seven layers as defined by the OSI model, shown in the order they occur whenever a user transmits information.

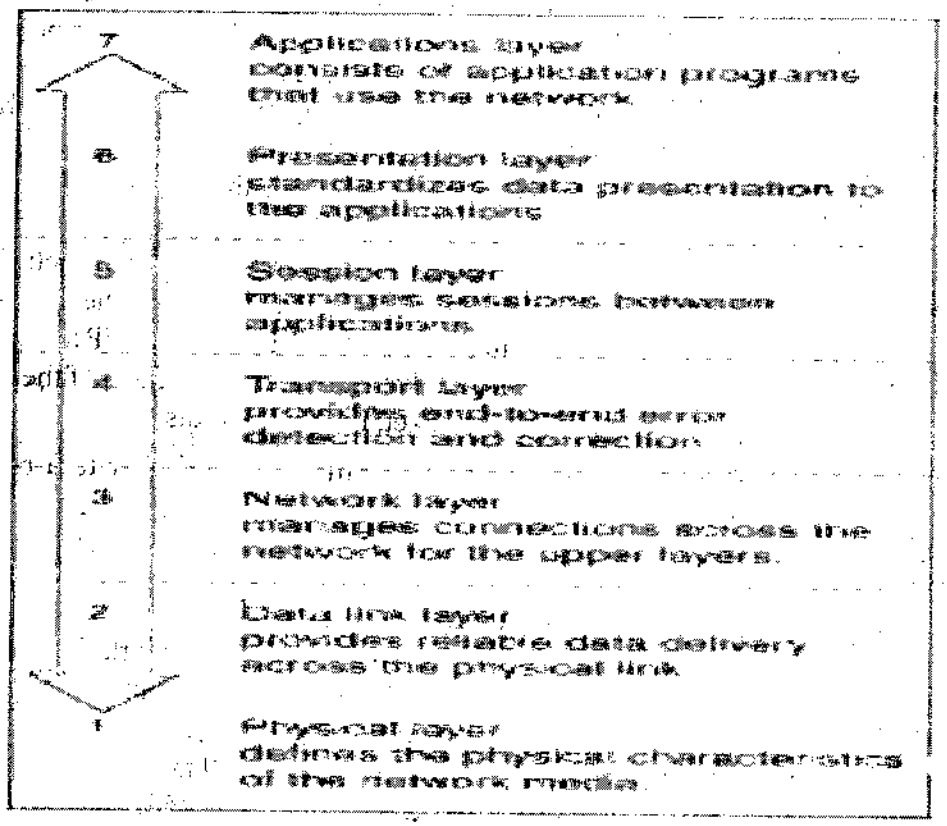


Figure A-2: The OSI Protocol Reference Model

Understanding Architectural Models and Protocols

In an architectural model, a layer does not define a single protocol—it defines a data communication function that may be performed by any number of protocols. Because each layer defines a function, it can contain multiple protocols, each of which provides a service suitable to the function of that layer.

Every protocol communicates with its peer. A *peer* is an implementation of the same protocol in the equivalent layer on a remote computer. Peer-level communications are standardized to ensure that successful communications take place. Theoretically, each protocol is only concerned with communicating to its peer—it does not care about the layers above or below it.

A dependency, however, exists between the layers. Because every layer is involved in sending data from a local application to an equivalent remote application, the layers must agree on how to pass data between themselves on a single computer. The upper layers rely on the lower layers to transfer the data across the underlying network.

How a Protocol Stack Works

As the reference model indicates, protocols (which compose the various layers) are like a pile of building blocks stacked one upon another. Because of this structure, groups of related protocols are often called *stacks* or *protocol stacks*.

Data is passed down the stack from one layer to the next, until it is transmitted over the network by the network access layer protocols. The four layers in this reference model are crafted to distinguish between the different ways that the data is handled as it passes down the protocol stack from the application layer to the underlying physical network.

At the remote end, the data is passed up the stack to the receiving application. The individual layers do not need to know how the layers above or below them function; they only need to know how to pass data to them.

Each layer in the stack adds control information (such as destination address, routing controls, and checksum) to ensure proper delivery. This control information is called a *header* and/or a *trailer* because it is placed in front of or behind the data to be transmitted. Each layer treats all of the information that it receives from the layer above it as data, and it places its own header and/or trailer around that information.

These wrapped messages are then passed into the layer below along with additional control information, some of which may be forwarded or derived from the higher layer. By the time a message exits the system on a physical link (such as a wire), the original message is enveloped in multiple, nested wrappers—one for each layer of protocol through which the data passed. When a protocol uses headers or trailers to package the data from another protocol, the process is called *encapsulation*. This process is illustrated in Figure A-3.

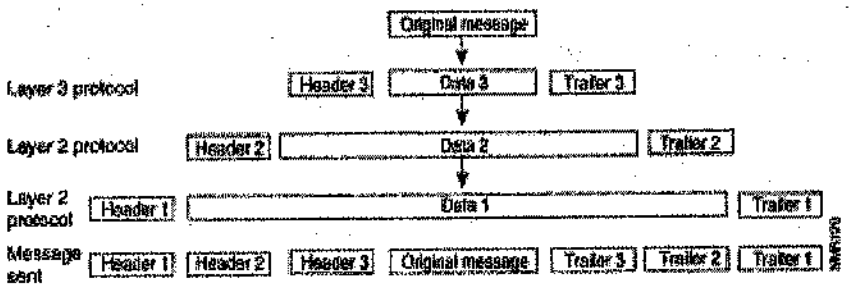


Figure A-3: Encapsulation of Data for Network Delivery

When data is received, the opposite happens. Each layer strips off its header and/or trailer before passing the data up to the layer above. As information flows back up the stack, information received from a lower layer is interpreted as both a header/trailer and data. The process of removing headers and trailers from data is called *decapsulation*. This mechanism enables each layer in the transmitting computer to communicate with its corresponding layer in the receiving computer. Each layer in the transmitting computer communicates with its *peer* layer in the receiving computer via a process called *peer-to-peer communication*.

Each layer has specific responsibilities and specific rules for carrying out those responsibilities, and it knows nothing about the procedures that the other layers follow. A layer carries out its tasks and delivers the message to the next layer in the protocol stack. An *address mechanism* is the common element that allows data to be routed through the various layers until it reaches its destination.

Each layer also has its own independent data structures. Conceptually, a layer is unaware of the data structures used by the layers above and below it. In reality, the data structures of a layer are designed to be compatible with the structures used by the surrounding layers for the sake of more efficient data transmission. Still, each layer has its own data structures and its own terminology to describe those structures.

Layer 7: Application

This layer supports the application and end-user processes. Within this layer, user privacy is considered and communication partners, service and constraints are all identified. File transfers, email, Telnet and FTP applications are all provided within this layer.

Layer 6: Presentation (Syntax)

Within this layer, information is translated back and forth between application and network formats. This translation transforms the information into data the application layer and network recognize regardless of encryption and formatting.

Layer 5: Session

Within this layer, connections between applications are made, managed and terminated as needed to allow for data exchanges between applications at each end of a dialogue.

Layer 4: Transport

Complete data transfer is ensured as information is transferred transparently between systems in this layer. The transport layer also assures appropriate flow control and end-to-end error recovery.

Layer 3: Network

Using switching and routing technologies, this layer is responsible for creating virtual circuits to transmit information from node to node. Other functions include routing, forwarding, addressing, internetworking, error and congestion control, and packet sequencing.

Layer 2: Data Link

Information in data packets are encoded and decoded into bits within this layer. Errors from the physical layer flow control and frame synchronization are corrected here utilizing transmission protocol knowledge and management. This layer consists of two sub layers: the Media Access Control (MAC) layer, which controls the way networked computers gain access to data and transmit it, and the Logical Link Control (LLC) layer, which controls frame synchronization, flow control and error checking.

Layer 1: Physical

This layer enables hardware to send and receive data over a carrier such as cabling, a card or other physical means. It conveys the bitstream through the network at the electrical and mechanical level. Fast Ethernet, RS232, and ATM are all protocols with physical layer components.

This order is then reversed as information is received, so that the physical layer is the first and application layer is the final layer that information passes through.

2.4.2 TCP/IP - The Internet protocol

The Internet was developed to provide a communication network that could function in wartime. Although the Internet has evolved from the original plan, it is still based on the TCP/IP protocol suite. The design of TCP/IP is ideal for the decentralized and robust Internet. Many common protocols were designed based on the four-layer TCP/IP model.

It is useful to know both the TCP/IP and OSI network models. Each model uses its own structure to explain how a network works. However, there is much overlap between the two models. A system administrator should be familiar with both models to understand how a network functions.

Any device on the Internet that wants to communicate with other Internet devices must have a unique identifier. The identifier is known as the IP address because routers use a Layer 3 protocol called the IP protocol to find the best route to that device. The current version of IP is IPv4. This was designed before there was a large demand for addresses. Explosive growth of the Internet has threatened to deplete the supply of IP addresses. Subnets, Network Address Translation (NAT), and private addresses are used to extend the supply of IP addresses. IPv6 improves on IPv4 and provides a much larger address space. Administrators can use IPv6 to integrate or eliminate the methods used to work with IPv4.

In addition to the physical MAC address, each computer needs a unique IP address to be part of the Internet. This is also called the logical address. There are several ways to assign an IP address to a device. Some devices always have a static address. Others have a temporary address assigned to them each time they connect to the network. When a dynamically assigned IP address is needed, a device can obtain it several ways.

For efficient routing to occur between devices, issues such as duplicate IP addresses must be resolved.

This page provides a comparison of the OSI model and the TCP/IP model.

The OSI and TCP/IP models have many similarities:

- Both have layers.
- Both have application layers, though they include different services.
- Both have comparable transport and network layers.
- Both use packet-switched instead of circuit-switched technology.
- Networking professionals need to know both models.

Here are some differences of the OSI and TCP/IP models:

- TCP/IP combines the OSI application, presentation, and session layers into its application layer.
- TCP/IP combines the OSI data link and physical layers into its network access layer.
- TCP/IP appears simpler because it has fewer layers.
- When the TCP/IP transport layer uses UDP it does not provide reliable delivery of packets. Thetransport layer in the OSI model always does.

IP Addressing

A computer may be connected to more than one network. In this situation, the system must be given more than one address. Each address will identify the connection of the computer to a different network. Each connection point, or interface, on a device has an address to a network. This will allow other computers to locate the device on that particular network. The combination of the network address and the host address creates a unique address for each device on a network. Each computer in a TCP/IP network must be given a unique identifier, or IP address. This address, which operates at Layer 3, allows one computer to locate another computer on a network. All computers also have a unique physical address, which is known as a MAC address. These are assigned by the manufacturer of the NIC. MAC addresses operate at Layer 2 of the OSI model.

An IP address is a 32-bit sequence of ones and zeros. Here is a sample of 32-bit number 11000000.10101000.00000001.00001000. To make the IP address easier to work with, it is usually written as four decimal numbers separated by periods. For example, an IP address of one computer is 192.168.1.2. Another computer might have the address 128.10.2.1. This is called the dotted decimal format. Each part of the address is called an octet because it is made up of eight binary digits. For example, the IP address 192.168.1.8 would be 11000000.10101000.00000001.00001000 in binary notation. The dotted decimal notation is an easier method to understand than the binary ones and zeros method. This dotted decimal notation also prevents a large number of transposition errors that would result if only the binary numbers were used.

It is easy to see the relationship between the numbers 192.168.1.8 and 192.168.1.9. The binary values 11000000.10101000.00000001.00001000 and 11000000.10101000.00000001.00001001 are not as easy to recognize. It is more difficult to determine that the binary values are consecutive numbers.

Self Learning Exercises :

5. Why was OSI model created?
   (a) to ensure secrecy of proprietary networking technologies
   (b) to ensure that networks are compatible with each other
   (c) to slow down the expansion of new technologies
   (d) to ensure that network administrators receive a high salary to decipher Networks
6. Which OSI layer is responsible for email and file transfer?
   (a) Application (b) Presentation
   (c) Transport (d) Session
7. Which OSI layer provides reliable connection and error control?
   (a) Application (b) Presentation
   (c) Transport (d) Session
8. Which OSI layer is responsible for end-to-end reliable delivery of the message?
   (a) Application (b) Presentation
   (c) Transport (d) Session

2.5 SUMMARY

A local-area network (LAN) is designed to operate within a limited geographical area. LANs allow multi-access to high-bandwidth media, control the network privately under local administration, provide full-time connectivity to local services and connect physically adjacent devices.

A wide-area network (WAN) is designed to operate over a large geographical area. WANs allow access over serial interfaces operating at lower speeds, provide full-time and part-time connectivity and connect devices separated over wide areas.

A metropolitan-area network (MAN) is a network that spans a metropolitan area such as a city or suburban area. A MAN usually consists of two or more LANs in a common geographic area.

2.6 GLOSSARY

- **TCP/IP Transmission Control Protocol/Internet Protocol** - A common name for the suite of protocols developed by the U.S. Department of Defense (DoD) in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite.
- **Topology** - A map of the physical arrangement of network nodes and media within an enterprise networking structure.
- **Tree topology** - A LAN topology similar to a bus topology, except that tree networks can contain branches with multiple nodes. Transmissions from a station propagate the length of the medium and are received by all other stations.
- **OSI Open System Interconnection** - An international standardization program created by International Organization for Standardization (ISO) and International Telecommunication Union Telecommunication Standardization Sector (ITU-T) to develop standards for data networking that facilitate multivendor equipment interoperability.
- **Impedance** - The amount of resistance to the transmission device.
- **Infrared** - Infrared is just below the visible range of light between 100Ghz and 1000Thz.
- **Interference** - Electromagnetic Interference (EMI). Crosstalk - When wires pick up electromagnetic signals from nearby wires also carrying signals.
- **Internetwork** - Several subnets connected together using routers.
- **Intranet** - Refers to using internet technologies such as a web server on an internal network.
- **ISA** - Industry Standard Architecture internal computer bus. Used when the original 8088 8bit microprocessor based personal computers were produced. (16 bit).
- **LAN** - Local Area Network
- **MAN**- Metropolitan area network refers to a network which connects several LANS over various media that is large enough to cover an area the size of a city.
- **W3C** - World Wide Web Consortium sets standards for the web working with the IETF.
- **WAN** - Wide Area Network is larger than a MAN and may be an enterprise network or a global network.
- **X.25** - This is a set of protocols developed by the CCITT/ITU which specifies how to connect computer devices over an internetwork.

2.7 FURTHER READINGS

1. Computer Networks : A.Tanenbaum; Prentice Hall India
2. Data & Computer Communications : William Stallings; Pearson Education

2.8 ANSWERS TO THE SELF LEARNING EXERCISES

1. b
2. b
3. c
4. b
5. b
6. a
7. c
8. c

2.9 UNIT END QUESTIONS

1. What are various types of Networks?
2. What are the advantages of Networks?
3. What do you understand by topology?
4. What is protocol?
5. What are the advantages of layered model protocol?
6. Describe the protocol architecture for TCP/IP?
7. Why is IP addressing used for?
8. What is the significance for Wireless Networks?

UNIT- III

COMPUTER NETWORK CONTD

STRUCTURE OF THE UNIT

3.0 Objective
3.1 Introduction
3.2 Protocols
3.2.1 TCP/IP
3.2.2 UDP
3.2.3 IPv4
3.2.4 IPv6
3.3 Switching
3.3.1 Circuit Switching
3.3.2 Packet Switching
3.4 Virtual LANs
3.5 Summary
3.6 Glossary
3.7 Further Readings
3.8 Answers to the self learning exercises
3.9 Unit end questions

3.0 OBJECTIVE

Students who complete this unit should be able to understand the following tasks:

- how each network protocol is used to perform networking
- the reader will be able to understand why each protocol is needed, how it is used, and what other protocols it relies upon
- Protocol suite – TCP/IP and UDP
- Switching techniques
- LANs crossing the boundaries of geographical limitations - VLANs
- How routers are used for communication between VLANs

3.1 INTRODUCTION

This unit is primarily about TCP/IP network protocols and Ethernet network architectures, but also briefly describes other protocol suites, network architectures, and other significant areas of networking. This networking tutorial is written for all audiences, even those with little or no networking experience. It explains in simple terms the way networks are put together, and how data packages are sent between networks and subnets along with how data is routed to the internet.

This networking tutorial explains the data encapsulation techniques in preparation for transport along with some of the network protocols such as IP, TCP, UDP, ICMP, and IGMP. It explains how ARP and RARP support networking. In functional areas, such as routers, several examples are given so the user can get a grasp on how networking is done in their particular situation. This

networking tutorial covers routing, and firewalls and gives some explanation of how they work. Firewalls and the available packages are described, but how to set them up is left to other documentation specific to the operating system and the package. Application protocols such as FTP and Telnet are also briefly described. Networking terms are also explained and defined.

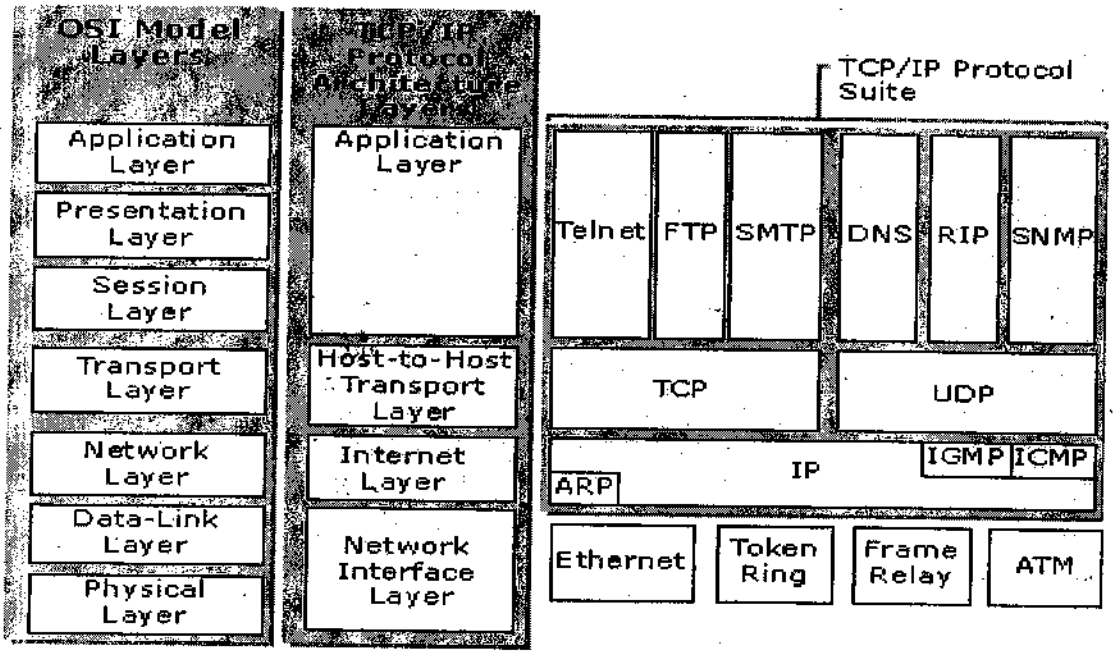
This unit provides an overview of virtual LANs (VLANs). It explains routing between VLANs and provides some basic information about designing VLANs.

3.2.1 TCP/IP

TCP/IP Protocol Architecture

TCP/IP protocols map to a four-layer conceptual model known as the *DARPA model*, named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model.

The figure given below shows the TCP/IP protocol architecture.



TCP/IP Protocol Architecture

Network Interface Layer

The *Network Interface layer* (also called the Network Access layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

The Network Interface layer encompasses the Data Link and Physical layers of the OSI model. Note that the Internet layer does not take advantage of sequencing and acknowledgment services that might be present in the Data-Link layer. An unreliable Network Interface layer is assumed, and reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of the Transport layer.

Internet Layer

The *Internet layer* is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

- The *Internet Protocol* (IP) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The *Address Resolution Protocol* (ARP) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
- The *Internet Control Message Protocol* (ICMP) is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
- The *Internet Group Management Protocol* (IGMP) is responsible for the management of IP multicast groups.

The Internet layer is analogous to the Network layer of the OSI model.

Transport Layer

The *Transport layer* (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

- TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.
- UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

The Transport layer encompasses the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer.

Application Layer

The *Application layer* provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed.

The most widely-known Application layer protocols are those used for the exchange of user information:

- The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.
- The File Transfer Protocol (FTP) is used for interactive file transfer.
- The Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.

- Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:

- The Domain Name System (DNS) is used to resolve a host name to an IP address.
- The Routing Information Protocol (RIP) is a routing protocol that routers use to exchange routing information on an IP internetwork.
- The Simple Network Management Protocol (SNMP) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

Examples of Application layer interfaces for TCP/IP applications are Windows Sockets and NetBIOS. Windows Sockets provides a standard application programming interface (API) under Windows 2000. NetBIOS is an industry standard interface for accessing protocol services such as sessions, datagrams, and name resolution. More information on Windows Sockets and NetBIOS is provided later in this chapter.

TCP : A connection-oriented transport layer protocol

Connection-Oriented

Before two communicating TCPs can exchange data, they must first agree upon the willingness to communicate. Analogous to a telephone call, a connection must first be made before two parties exchange information.

Reliability

A number of mechanisms help provide the reliability TCP guarantees. Each of these is described briefly below.

Checksums. All TCP segments carry a checksum, which is used by the receiver to detect errors with either the TCP header or data.

Duplicate data detection. It is possible for packets to be duplicated in packet switched network; therefore TCP keeps track of bytes received in order to discard duplicate copies of data that has already been received.[2]

Retransmissions. In order to guarantee delivery of data, TCP must implement retransmission schemes for data that may be lost or damaged. The use of positive acknowledgements by the receiver to the sender confirms successful reception of data. The lack of positive acknowledgements, coupled with a timeout period (see timers below) calls for a retransmission.

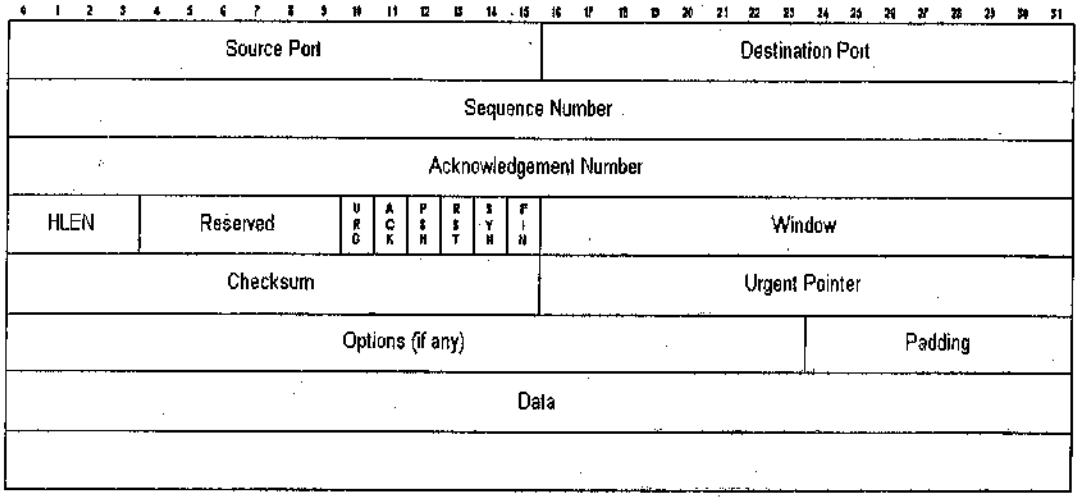
Sequencing. In packet switched networks, it is possible for packets to be delivered out of order. It is TCP's job to properly sequence segments it receives so it can deliver the byte stream data to an application in order.

Timers. TCP maintains various static and dynamic timers on data sent. The sending TCP waits for the receiver to reply with an acknowledgement within a bounded length of time. If the timer expires before receiving an acknowledgement, the sender can retransmit the segment.

TCP Header Format

Remember that the combination of TCP header and TCP in one packet is called a TCP segment. Figure 1 depicts the format of all valid TCP segments. The size of the header without options is 20 bytes. We will briefly define each field of the TCP header below.

TCP Header Format



Source Port

A 16-bit number identifying the application the TCP segment originated from within the sending host. The port numbers are divided into three ranges, well-known ports (0 through 1023), registered ports (1024 through 49151) and private ports (49152 through 65535). Port assignments are used by TCP as an interface to the application layer. For example, the TELNET server is always assigned to the well-known port 23 by default on TCP hosts. A complete pair of IP addresses (source and destination) plus a complete pair of TCP ports (source and destination) define a single TCP connection that is globally unique. See [5] for further details.

Destination Port

A 16-bit number identifying the application the TCP segment is destined for on a receiving host. Destination ports use the same port number assignments as those set aside for source ports [5].

Sequence Number

A 32-bit number identifying the current position of the first data byte in the segment within the entire byte stream for the TCP connection. After reaching 2^{32}-1, this number will wrap around to 0.

Acknowledgement Number

A 32-bit number identifying the next data byte the sender expects from the receiver. Therefore, the number will be one greater than the most recently received data byte. This field is only used when the ACK control bit is turned on (see below).

Header Length

A 4-bit field that specifies the total TCP header length in 32-bit words (or in multiples of 4 bytes if you prefer). Without options, a TCP header is always 20 bytes in length. The largest a TCP header may be is 60 bytes. This field is required because the size of the options field(s) cannot be determined in advance. Note that this field is called "data offset" in the official TCP standard, but header length is more commonly used.

Reserved

A 6-bit field currently unused and reserved for future use.

Control Bits

Urgent Pointer (URG). If this bit field is set, the receiving TCP should interpret the urgent pointer field (see below).

Acknowledgement (ACK). If this bit field is set, the acknowledgement field described earlier is valid.

Push Function (PSH). If this bit field is set, the receiver should deliver this segment to the receiving application as soon as possible. An example of its use may be to send a Control-BREAK request to an application, which can jump ahead of queued data.

Reset the Connection (RST). If this bit is present, it signals the receiver that the sender is aborting the connection and all queued data and allocated buffers for the connection can be freely relinquished.

Synchronize (SYN). When present, this bit field signifies that sender is attempting to "synchronize" sequence numbers. This bit is used during the initial stages of connection establishment between a sender and receiver.

No More Data from Sender (FIN). If set, this bit field tells the receiver that the sender has reached the end of its byte stream for the current TCP connection.

Window

A 16-bit integer used by TCP for flow control in the form of a data transmission window size. This number tells the sender how much data the receiver is willing to accept. The maximum value for this field would limit the window size to 65,535 bytes, however a "window scale" option can be used to make use of even larger windows.

Checksum

A TCP sender computes a value based on the contents of the TCP header and data fields. This 16-bit value will be compared with the value the receiver generates using the same computation. If the values match, the receiver can be very confident that the segment arrived intact.

Urgent Pointer

In certain circumstances, it may be necessary for a TCP sender to notify the receiver of urgent data that should be processed by the receiving application as soon as possible. This 16-bit field tells the receiver when the last byte of urgent data in the segment ends.

Options

In order to provide additional functionality, several optional parameters may be used between a TCP sender and receiver. Depending on the option(s) used, the length of this field will vary in size, but it cannot be larger than 40 bytes due to the size of the header length field (4 bits). The most common option is the maximum segment size (MSS) option. A TCP receiver tells the TCP sender the maximum segment size it is willing to accept through the use of this option. Other options are often used for various flow control and congestion control techniques.

Padding

Because options may vary in size, it may be necessary to "pad" the TCP header with zeroes so that the segment ends on a 32-bit word boundary as defined by the standard.

Data

Although not used in some circumstances (e.g. acknowledgement segments with no data in the reverse direction), this variable length field carries the application data from TCP sender to receiver. This field coupled with the TCP header fields constitutes a TCP segment.

3.2.2 UDP

UDP is a connectionless, best-effort Internet protocol that offers fewer features than TCP (for example, no handshaking, flow control or reliability mechanisms), in exchange for speedier delivery of data.

This makes it useful for applications in which the data must arrive quickly at an endpoint, such as videoconferencing and streaming media. In fact, the multimedia protocol SIP relies on UDP (although it adds its own retransmission mechanism since UDP is an unreliable protocol). SNMP (Simple Network Management Protocol) and DNS (Domain Name Service), and TFTP (Trivial File Transfer Protocol) also use UDP.

The User Datagram Protocol offers only a minimal transport service — non-guaranteed datagram delivery — and gives applications direct access to the datagram service of the IP layer. UDP is used by applications that do not require the level of service of TCP or that wish to use communications services (e.g., multicast or broadcast delivery) not available from TCP.

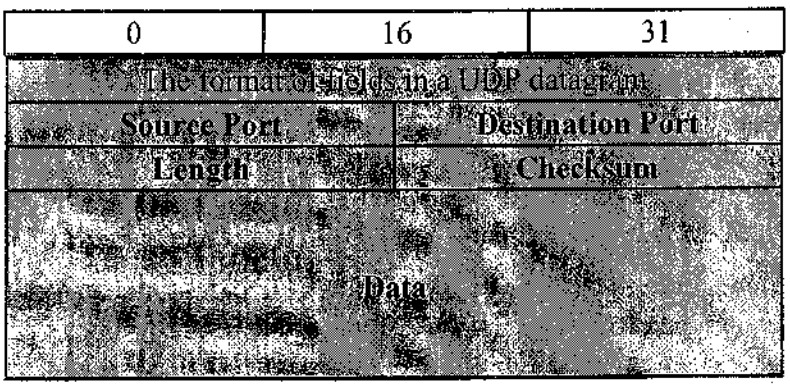
UDP is almost a null protocol; the only services it provides over IP are checksumming of data and multiplexing by port number. Therefore, an application program running over UDP must deal directly with end-to-end communication problems that a connection-oriented protocol would have handled — e.g., retransmission for reliable delivery, packetization and reassembly, flow control, congestion avoidance, etc., when these are required.

UDP packets or datagrams (also known as datagrams) contain, in addition to the lower level headers, a checksum, the packet length, source and destination ports.

UDP Message Format

The UDP message, or as it is usually called, UDP segment, consists of two parts:

- A UDP header (64 bits)



Header Fields

The UDP header has only four fields, each consisting of 16 bits.

Source Port

This is an optional field. When meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

Destination Port

This field has a meaning within the context of a particular internet destination address, and it is used to demultiplex datagrams among the processes waiting to receive them.

Length

This field's value is the length in octets of this user datagram, including the UDP header and the user data. Thus, the minimum value of the length field is eight - the length of the header alone. The maximum length of a datagram varies depending on the operating environment. With **Length** field of two bytes, the theoretical maximum length is 65535 bytes. However, some implementations of UDP restrict the datagram to a smaller number, sometimes as low as 8192 bytes.

Checksum

The UDP Checksum is optional, and a value of 0 means that the checksum has not been computed. The protocol designers chose to leave the checksum optional to allow implementations to operate with little computational overhead when using UDP over a highly reliable LAN. However, as IP does not compute a checksum on the data portion of an IP datagram, the UDP checksum provides the only way to guarantee that the data has arrived intact and should be used.

When a checksum is computed, the value of this field is the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded with a zeros octet at the end (if necessary) to make a multiple of two octets. A computed checksum of zero is not a problem, as one's complement arithmetic has two representations for zero: all bits set to zero or all bits set to one. Thus, when the computed checksum is zero, the all-ones representation will be chosen.

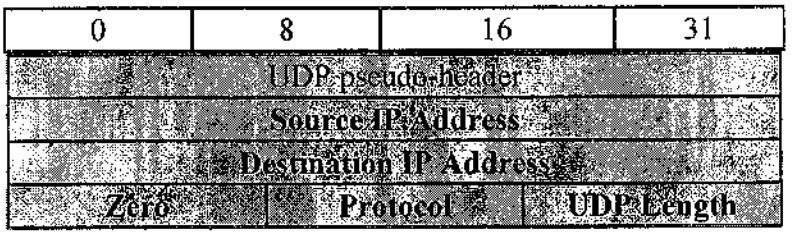
Although UDP provides error checking, it does not do anything to recover from an error. Some implementations of UDP simply discard the damaged segment, while others pass the damaged segment to the application with a warning.

UDP Pseudo-Header

The UDP checksum covers more information than is present in th UDP datagram alone. To compute the checksum, UDP prepends a pseudo-header to the UDP datagram, appends an octet of zeros (if needed) to pad the datagram to an exact multiple of 16 bits, and then computes the checksum over the entire object. The octet used for padding and the pseudo-header are **not** transmitted with the UDP datagram, nor are they included in the length field.

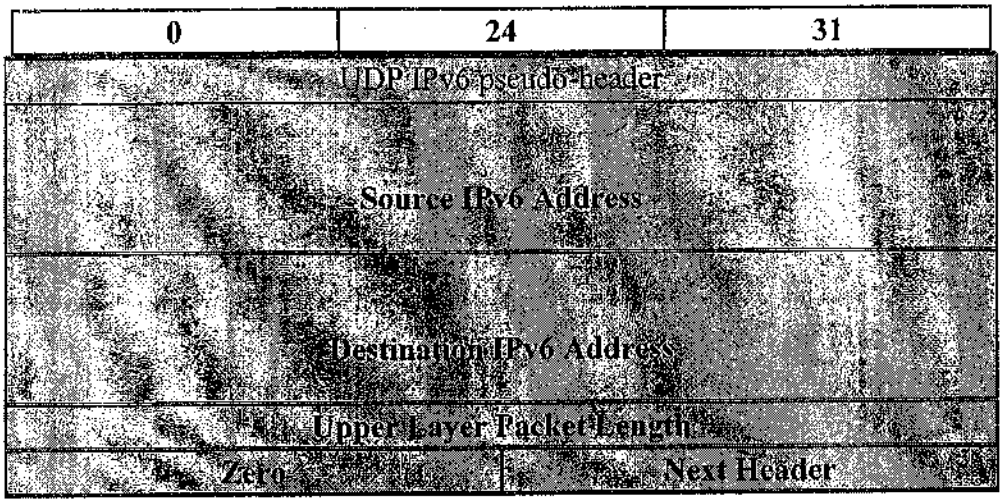
The pseudo-header is used in order to verify that the UDP datagram has reached its correct destination. As mentioned above, the UDP header only specifies the destination port, while the final destination of a datagram is a combination of the destination IP address and the destination UDP port. Therefore, UDP on the sending computer calculates a checksum that covers both destination IP address and destination UDP port. At the recipient side, UDP verifies the checksum using the destination IP address obtained from the header of the IP datagram that carried the UDP message. If the checksums agree, then it must be true that the datagram has reached its correct final destination.

When transported by IPv4, the pseudo-header contains the following fields:



The pseudo-header consists of 12 octets. The fields *Source IP Address* and *Destination IP Address* contain the source and destination IP addresses that will be used when sending the UDP message. The field *Protocol* contains the IP protocol type code (17 for UDP), and the ***field UDP Length*** contains the length of the UDP datagram (not including the pseudo-header). To verify the checksum, the receiver must extract these fields from the IP header, assemble them into the pseudo-header format, and recompute the checksum.

The checksum is not optional when transported by IPv6. In this case, the pseudo-header contains the following fields:



The *Source IPv6 Address* and *Destination IPv6 Address* are 128-bit fields, representing the addresses of the source and destination hosts. The *Upper Layer Packet Length* in the pseudo-header is the length of the upper-layer header and data. In the case of UDP, this field is equal to the *Length* field in the UDP header. The *Next Header* value in the pseudo-header identifies the upper-layer protocol (17 for UDP). The field *Zero* is used for padding.

Characteristic / Description	UDP	TCP
General Description that interfaces	Simple, high-speed, low-functionality "wrapper" applications to the network layer and does little else.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol Connection Setup	Connectionless; data is sent without setup.	Connection-oriented; connection must be established prior to transmission.
Data Interface To Application	Message-based; data is sent in discrete packages by the application	Stream-based; data is sent by the application with no particular structure.
Reliability and Acknowledgments	Unreliable, best-effort delivery without acknowledgments.	Reliable delivery of messages; all data is acknowledged.
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Features Provided to Manage Flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms.
Overhead	Very low	Low, but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Data Quantity Suitability	Small to moderate amounts of data (up to a few hundred bytes)	Small to very large amounts of data (up to gigabytes)
Types of Applications That Use The Protocol	Applications where data delivery speed matters more than completeness, where small amounts of ; data are sent or where multicast/broadcast are used.	Most protocols and applications sending data that must be received reliably, including most file and message transfer protocols
Well-KnownApplications and Protocols	Multimedia applications, DNS, BOOTP, DHCP, TFTP, SNMP, RIP, NFS (early versions)	FTP, Telnet, SMTP, DNS, HTTP, POP, NNTP, IMAP, BGP, IRC, NFS (later versions)

3.2.3 IPv4

Classful IP Addressing

When IP was first standardized in September 1981, the specification required that each system attached to an IP-based Internet be assigned a unique, 32-bit Internet address value. Systems that have interfaces to more than one network require a unique IP address for each network interface. The first part of an Internet address identifies the network on which the host resides, while the second part identifies the particular host on the given network. This creates the two-level addressing hierarchy that is illustrated in Table 1. In recent years, the network number field has been referred to as the network prefix because the leading portion of each IP address identifies the network number. All hosts on a given network share the same network prefix but must have a unique host number. Similarly, any two hosts on different networks must have different network prefixes but may have the same host number.

IP Address Class	High order bits	1st octet address range	No.of bits in Network address
Class A	0	0-127	8
Class B	10	128-191	16
Class C	110	192-223	24
Class D	1110	224-239	28

Table 1 : Classful IP Addresses used in IPv4

A router uses IP to forward packets from the source network to the destination network. The packets must include an identifier for both the source and destination networks. A router uses the IP address of the destination network to deliver a packet to the correct network. When the packet arrives at a router connected to the destination network, the router uses the IP address to locate the specific computer on the network. This system works in much the same way as the national postal system. When the mail is routed, the zip code is used to deliver it to the post office at the destination city. That post office must use the street address to locate the final destination in the city.

Every IP address also has two parts. The first part identifies the network where the system is connected and the second part identifies the system

Primary Address Classes

IP addresses are divided into classes to define the large, medium, and small networks. Class A addresses are assigned to larger networks. Class B addresses are used for medium-sized networks, and Class C for small networks. The first step in determining which part of the address identifies the network and which part identifies the host is identifying the class of an IP address.

IP Address Class	Network bits (N) Host bits (H) in IPv4
Class A	N.H.H.H
Class B	N.N.H.H
Class C	N.N.N.H

This is often referred to as classful addressing. Each class fixes the boundary between the network prefix and the host number at a different point within the 32-bit address.

3.2.4 IPv6

IP, the Internet Protocol, is one of the pillars which support the Internet. Almost 20 years old, first specified in a remarkably concise 45 pages in RFC 791, IP is the network-layer protocol for the Internet.

In 1991, the IETF decided that the current version of IP, called IPv4, had outlived its design. The new version of IP, called either IPng (Next Generation) or IPv6 (version 6), was the result of a long and tumultuous process which came to a head in 1994, when the IETF gave a clear direction for IPv6.

IPv6 is designed to solve the problems of IPv4. It does so by creating a new version of the protocol which serves the function of IPv4, but without the same limitations of IPv4. IPv6 is not totally different from IPv4: what you have learned in IPv4 will be valuable when you deploy IPv6. The differences between IPv6 and IPv4 are in five major areas: addressing and routing, security, network address translation, administrative workload, and support for mobile devices. IPv6 also includes an important feature: a set of possible migration and transition plans from IPv4.

Since 1994, over 30 IPv6 RFCs have been published. Changing IP means changing dozens of Internet protocols and conventions, ranging from how IP addresses are stored in DNS (domain name system) and applications, to how datagrams are sent and routed over Ethernet, PPP, Token Ring, FDDI and every other medium, to how programmers call network functions.

The IETF, though, is not so insane as to assume that everyone is going to change everything overnight. So there are also standards and protocols and procedures for the coexistence of IPv4 and IPv6: tunneling IPv6 in IPv4, tunneling IPv4 in IPv6, running IPv4 and IPv6 on the same system (dual stack) for an extended period of time, and mixing and matching the two protocols in a variety of environments.

So What's In It?

Even if you've never studied IPv6, you may know about its most famous feature: big addresses. IPv4 uses 32-bit addresses, and with the growth of the Internet, these have become a scarce and valuable commodity. Organizations have gone to great lengths to deal with the shortage and high cost of IPv4 addresses. The most visible change in IPv6 is that addresses balloon from 32-bits to 128-bits.

Feature	Change
Address Space	Increase from 32-bit to 128-bit address space
Management	Stateless autoconfiguration means no more need to configure IP addresses for end systems, even via DHCP
Performance	Predictable header sizes and 64-bit header alignment mean better performance from routers and bridges/switches
Multicast/Multimedia	Built-in features for multicast groups, management, and new "anycast" groups
Mobile IP	Eliminate triangular routing and simplify deployment of mobile IP-based systems
Virtual Private Networks	Built-in support for ESP/AH encrypted/authenticated virtual private network protocols; built-in support for QoS tagging

With such a huge address space, ISPs will have sufficient IP addresses to allocate enough addresses to every customer so that every IP device has a truly unique address—whether it's behind a firewall or not. NAT (network address translation) has become a very common technique to deal with the shortage of IP addresses. Unfortunately, NAT doesn't work very well for many Internet applications, ranging from old dependables, such as NFS and DNS, to newer applications such as group conferencing. NAT has also been an impediment for business-to-business direct network connections, requiring baroque and elaborate address translators to make everything work reliably, scaling poorly, and offering a highly vulnerable single point of failure. One of the goals of IPv6's address space expansion is to make NAT unnecessary, improving total connectivity, reliability, and flexibility. IPv6 will re-establish transparency and end-to-end traffic across the Internet.

Additional address space will also help the core of the Internet—it is hoped—by reducing the size and complexity of the global routing tables. Although IPv6 doesn't solve the problems of routing in the Internet, it can help in several areas, reducing the initial size of the tables and offering a hierarchical address space.

The new IPv6 addresses are large and cumbersome to deal with, so IPv6 reduces the number of people who have to read and write them. A second major goal of IPv6 is to reduce the total time which people have to spend configuring and managing systems. An IPv6 system can participate in "stateless" autoconfiguration, where it creates a guaranteed-unique IP address by combining its LAN MAC address with a prefix provided by the network router—DHCP is not needed. Of course, DHCP is still useful for other parameters, such as DNS servers, and is supported as DHCPv6 where needed. IPv6 also offers a middle ground between the two extremes with protocols such as SLP ("Service Location Protocol"), which may make the lives of network managers easier.

Although IPv4 is a simple protocol, it was not designed for giga-bit and tera-bit routers which need to look at millions of packets a second. The third major goal of IPv6 is to speed up the network, both from a performance and from a deployment point of view. IPv6 embodies the lessons learned at trying to build high-speed routers for IPv4 by changing the header of the IP packet to be more regular and to streamline the work of high-speed routers moving packets across the Internet backbone. IPv6 has fixed header sizes, and little-used IPv4 fields have been removed.

A side effect of the redesign of the IP packet header is that future extensions to IPv6 are simplified: adding a new option to IP can be done without a major re-engineering of IP routers everywhere.

High-bandwidth multimedia and fault tolerance applications are the focus of the fourth major goal of IPv6. Multimedia applications can take advantage of multicast: the transmission of a single datagram to multiple receivers. Although IPv4 has some multicast capabilities, these are optional and not every router and host supports them. With IPv6, multicast is a requirement. IPv6 also defines a new kind of service, called "anycast." Like multicast, anycast has groups of nodes which send and receive packets. But when a packet is sent to an anycast group in IPv6, it is only delivered to one of the members of the group. This new capability is especially appropriate in a fault-tolerant environment: web servers and DNS servers could all benefit from IPv6's anycast technology.

The fifth major goal of IPv6 is VPNs, virtual private networks. The new IPSec security protocols, ESP (encapsulating security protocol) and AH (authentication header) are add-ons to IPv4.

IPv6 builds-in and requires these protocols, which will mean that secure networks will be easier to build and deploy in an IPv6 world.

Another aspect of VPNs built into IPv6 is QoS (Quality of Service). IPv6 supports the same QoS features as IPv4, including the DiffServ indication, as well as a new 20-bit traffic flow field. Although the use of this part of IPv6 is not defined, it is provided as a solid base to build QoS protocols.

Self Learning exercises :

1. What are the common TCP/IP Application Protocols?
   a) DHCP b) DNS
   c) FTP d) STTP
2. What are the main features of IPv6 ?
   (a) It provides classless IP addressing
   (b) IPv6 uses 128-bit addresses
   (c) Both (a) and (b)
   (d) None of the above
3. Which one is not the protocol functioning at Internet layer of TCP/IP?
   (a) IGMP (b) ICMP
   (c) ARP (d) ATM

3.3 SWITCHING

In principle, two basic technologies are used for building high-capacity networks: circuit switching and packet switching. In circuit-switched networks, network resources are reserved all the way from sender to receiver before the start of the transfer, thereby creating a circuit. The resources are dedicated to the circuit during the whole transfer. Control signaling and payload data transfers are separated in circuit-switched networks. Processing of control information and control signaling such as routing is performed mainly at circuit setup and termination. Consequently, the transfer of payload data within the circuit does not contain any overhead in the form of headers or the like. Traditional voice telephone service is an example of circuit switching.

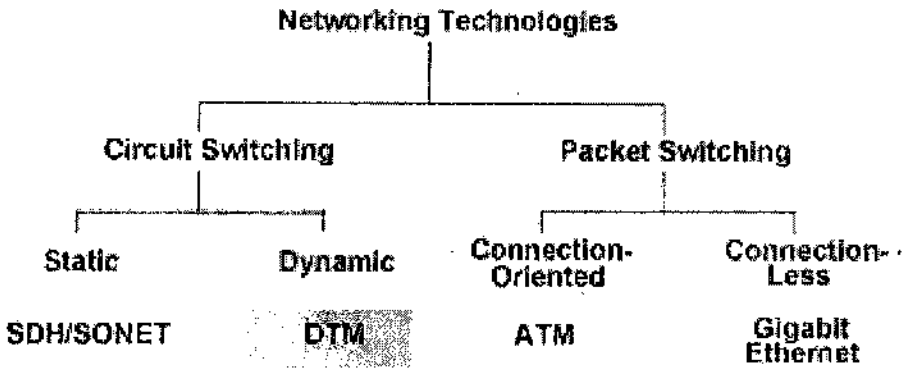
Circuit-Switched Networks

An advantage of circuit-switched networks is that they allow for large amounts of data to be transferred with guaranteed transmission capacity, thus providing support for real-time traffic. A disadvantage of circuit switching, however, is that if connections are short-lived—when transferring short messages, for example—the setup delay may represent a large part of the total connection time, thus reducing the network's capacity. Moreover, reserved resources cannot be used by any other users even if the circuit is inactive, which may further reduce link utilization.

Packet-Switched Networks

Packet switching was developed to cope more effectively with the data-transmission limitations of the circuit-switched networks during bursts of random traffic. In packet switching, a data stream is divided into standardized packets. Each contains address, size, sequence, and error-checking information, in addition to the payload data. The packets are then sent through the network, where specific packet switches or routers sort and direct each single packet.

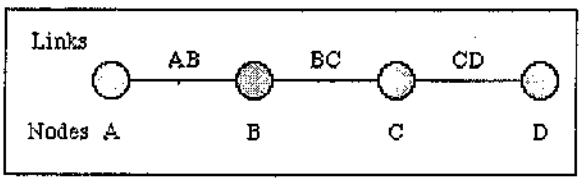
Packet-switched networks are based either on connectionless or connection-oriented technology. In connectionless technology, such as IP, packets are treated independently of each other inside the network, because complete information concerning the packet destination is contained in each packet. This means that packet order is not always preserved, because packets destined for the same receiver may take different paths through the network. In connection-oriented technology such as asynchronous transfer mode (ATM), a path through the network—often referred to as a logical channel or virtual circuit—is established when data transfer begins. Each packet header then contains a channel identifier that is used at the nodes to guide each packet to the correct destination.



Technology Overview

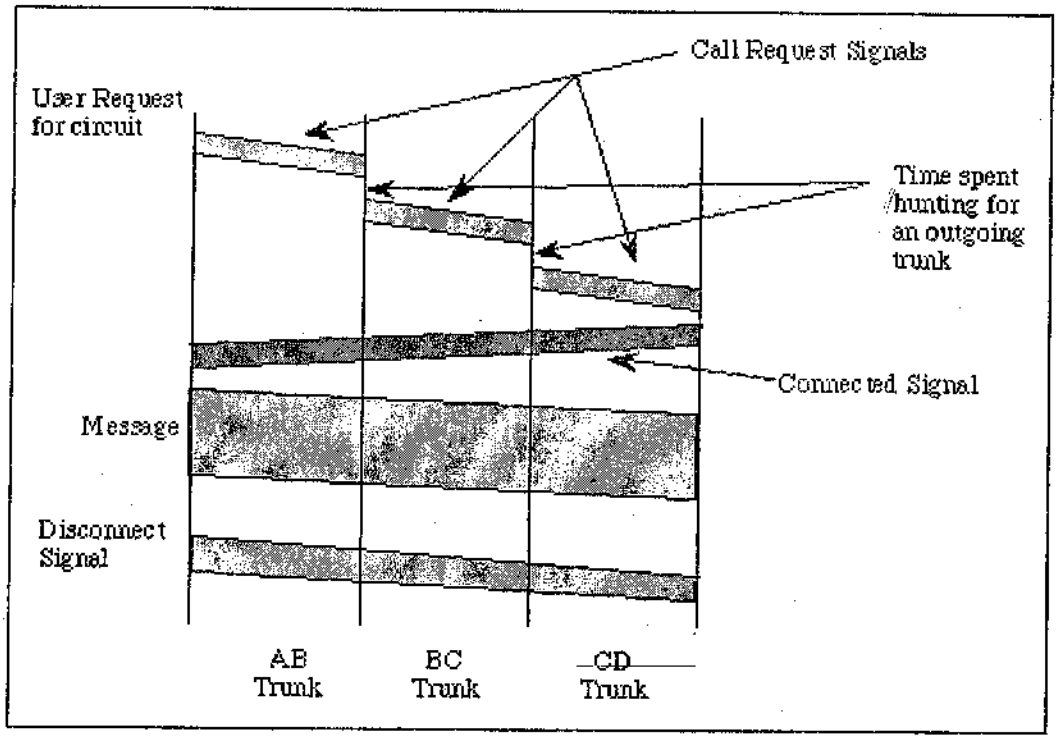
In many aspects, a packet-switched network is a network of queues. Each network node contains queues where incoming packets are queued before they are sent out on an outgoing link. If the rate at which packets arrive at a switch point exceeds the rate at which packets can be transmitted, the queues grow. This happens, for example, if packets from several incoming links have the same destination link. The queuing causes delay, and if the queues overflow, packets are lost, which is called congestion. Loss of data generally causes retransmissions that may either add to the congestion or result in less-effective utilization of the network. The ability to support real-time traffic in packet-switched networks thus calls for advanced control mechanisms for buffer handling and direction. As a result, the complexity and necessary ability to process information, and therefore the need for computer power, increases sharply when striving for high transmission capacity.

Circuit switching is the most familiar technique used to build a communications network. It is used for ordinary telephone calls. It allows communications equipment and circuits, to be shared among users. Each user has sole access to a circuit (functionally equivalent to a pair of copper wires) during network use. Consider communication between two points A and D in a network. The connection between A and D is provided using (shared) links between two other pieces of equipment, B and C.



A connection between two systems A & D formed from 3 links

Network use is initiated by a connection phase, during which a circuit is set up between source and destination, and terminated by a disconnect phase. These phases, with associated timings, are illustrated in the figure below.



A circuit switched connection between A and D

(Information flows in two directions. Information sent from the calling end is shown in pink and information returned from the remote end is shown in blue)

After a user requests a circuit, the desired destination address must be communicated to the local switching node (B). In a telephony network, this is achieved by dialing the number.

Node B receives the connection request and identifies a path to the destination (D) via an intermediate node (C). This is followed by a circuit connection phase handled by the switching nodes and initiated by allocating a free circuit to C (link BC), followed by transmission of a call request signal from node B to node C. In turn, node C allocates a link (CD) and the request is then passed to node D after a similar delay.

The circuit is then established and may be used. While it is available for use, resources (i.e. in the intermediate equipment at B and C) and capacity on the links between the equipment are dedicated to the use of the circuit.

After completion of the connection, a signal confirming circuit establishment (a connect signal in the diagram) is returned; this flows directly back to node A with no search delays since the circuit has been established. Transfer of the data in the message then begins. After data transfer, the circuit is disconnected; a simple disconnect phase is included after the end of the data transmission.

Delays for setting up a circuit connection can be high, especially if ordinary telephone equipment is used. Call setup time with conventional equipment is typically on the order of 5 to 25 seconds after completion of dialing. New fast circuit switching techniques can reduce delays. Trade-offs between circuit switching and other types of switching depend strongly on switching times.

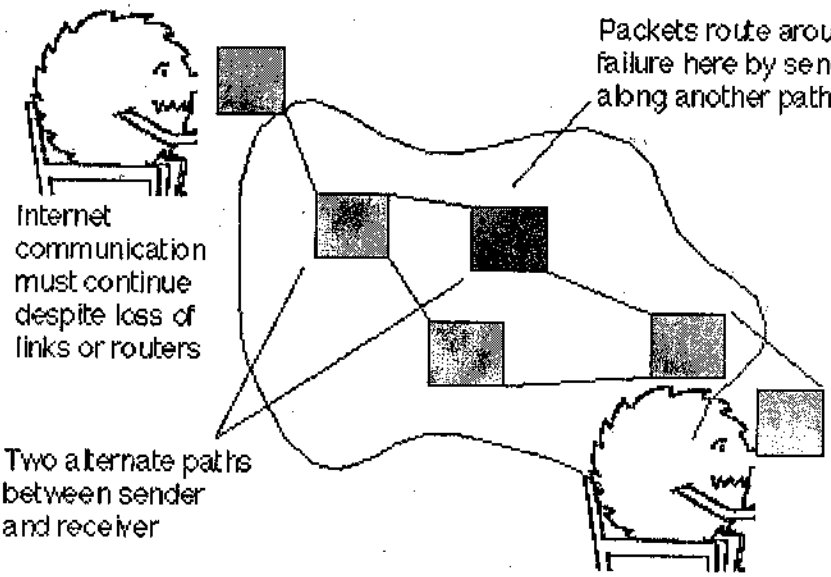
Datagram Packet Networks

Datagram transmission uses a different scheme to determine the route through the network of links. Using datagram transmission, each packet is treated as a separate entity and contains a header with the full information about the intended recipient. The intermediate nodes examine the header of a packet and select an appropriate link to an intermediate nodes which is nearer the destination. In this system, the packets do not follow a pre-established route, and the intermediate nodes (usually known as routers) do not require prior knowledge of the routes that will be used.

A datagram network is analogous to sending a message as a series of postcards through the postal system. Each card is independently sent to the final destination (using the postal system). To receive the whole message, the receiver must collect all the postcards and sort them into the original order. Not all postcards need be delivered by the postal system, and not all take the same length of time to arrive.

In a datagram network delivery is not guaranteed (although they are usually reliably sent). Enhancements, if required, to the basic service (e.g. reliable delivery) must be provided by the end systems (i.e. user's computers) using additional software. The most common datagram network is the Internet which uses the IP network protocol. Applications which do not require more than a best effort service can be supported by direct use of packets in a datagram network (using the User Datagram Protocol (UDP) transport protocol). Such applications include Internet Video, Voice Communication, messages notifying a user that she/he has received new email, etc. Most Internet applications need additional functions to provide reliable communication (such as end-to-end error and sequence control). Examples include sending email, browsing a web site, or sending a file using the file transfer protocol (ftp). This reliability ensures all the data is received in the correct order with no duplication or omissions. It is provided by additional layers of software algorithms implemented in the end systems (A,D). Two examples of this are the Transmission Control Protocol (TCP), and the Trivial File Transfer Protocol (TFTP) which uses UDP.

One merit of the datagram approach is that not all packets need to follow the same path (route) through the network (although frequently packets do follow the same route). This removes the need to set-up and tear-down the path, reducing the processing overhead, and a need for Intermediate Systems to execute an additional protocol.



Packets may also be routed around busy parts of the network when alternate paths exist. This is useful when a particular intermediate system becomes busy or overloaded with excessive volumes of packets to send. It can also provide a high degree of fault tolerance, when an individual intermediate system or communication circuit fails. As long as a route exists through the network between two end systems, they are able to communicate. Only if there is no possible way to send the packets, will the packets be discarded and not delivered. The fate (success/failure) of an application therefore depends only on existence of an actual path between the two End Systems (ESs). This is known as "fate sharing" - since the application shares the "fate" of the network.

There is another type of network known as a virtual circuit network. This has some advantages in particular scenarios.

Virtual Circuit Packet Networks

In virtual circuit packet switching, an initial setup phase is used to set up a fixed route between the intermediate nodes for all packets which are exchanged during a session between the end nodes (analogous to the circuit-switched telephony network). At each intermediate node, an entry is made in a table to indicate the route for the connection that has been set up. Packets can then use short headers, since only identification of the virtual circuit rather than complete destination address is needed. The intermediate nodes (B,C) process each packet according to the information which was stored in the node when the connection was established.

Enhancements to provide reliability may also be provided. Delivery of packets in proper sequence and with essentially no errors is guaranteed, and congestion control to minimise queuing is common. Delays are more variable than they are with a dedicated circuit, however, since several virtual circuits may compete for the same resources. An initial connection setup phase and a disconnect phase at the end of data transfer are required (as in the circuit-switched network). The most common form of virtual circuit network were ATM and X.25, which for a while were commonly used for public packet data networks.

Differences between datagram and virtual circuit networks

There are a number of important differences between virtual circuit and datagram networks. The choice strongly impacts complexity of the different types of node. Use of datagrams between intermediate nodes allows relatively simple protocols at this level, but at the expense of making the end (user) nodes more complex when end-to-end virtual circuit service is desired.

The Internet transmits datagrams between intermediate nodes using IP. Most Internet users need additional functions such as end-to-end error and sequence control to give a reliable service (equivalent to that provided by virtual circuits). This reliablility may be provided by the Transmission Control Protocol (TCP) which is used end-to-end across the Internet, or by applications such as the trivial file transfer protocol (tftp) running on top of the User Datagram Protocol (UDP).

Self learning exercises :

4. In which type of switching do all the datagrams of a message follow the same channels of path ?

   (a) circuit switching (b) datagram packet switching

   (c) virtual circuit packet switching (d) message switching

5. Which type of switching uses the entire capacity of a dedicated link ?

   (a) circuit switching (b) datagram packet switching

   (c) virtual circuit packet switching (d) message switching

6. The delivery of message is not in order, but provides a fast means of Communication ?

   (a) circuit switching (b) datagram packet switching

   (c) virtual circuit packet switching (d) message switching

3.4 VLANS : AN OVERVIEW

An important feature of Ethernet switching is the virtual local-area network (VLAN). A VLAN is a logical grouping of devices or users. These devices or users can be grouped by function, department, or application despite the physical LAN segment location. Devices on a VLAN are restricted to only communicating with devices that are on their own VLAN. Just as routers provide connectivity between different LAN segments, routers provide connectivity between different VLAN segments. Cisco is taking a positive approach toward vendor interoperability, but each vendor has developed its own proprietary VLAN product and it may not be entirely compatible.

VLANs increase overall network performance by logically grouping users and resources together. Businesses often use VLANs as a way of ensuring that a particular set of users are logically grouped regardless of the physical location. Therefore, users in the Marketing department are placed in the Marketing VLAN, while users in the Engineering Department are placed in the Engineering VLAN.

VLANs can enhance scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.

VLANs are powerful tools for network administrators when properly designed and configured. VLANs simplify tasks when additions, moves, and changes to a network are necessary. VLANs improve network security and help control Layer 3 broadcasts. However, improperly config-

ured VLANs can make a network function poorly or not function at all. Understanding how to implement VLANs on different switches is important when designing a network.

Why Implement VLANs?

Network managers can group logically networks that span all major topologies, including high-speed technologies such as, ATM, FDDI, and Fast Ethernet. By creating virtual LANs, system and network administrators can control traffic patterns and react quickly to relocations and keep up with constant changes in the network due to moving requirements and node relocation just by changing the VLAN member list in the router configuration. They can add, remove, or move devices or make other changes to network configuration using software to make the changes.

Issues regarding benefits of creating VLANs should have been addressed when you developed your network design. Issues to consider include

- Scalability
- Performance improvements
- Security
- Network additions, moves, and changes

A VLAN is a group of network services not restricted to a physical segment or LAN switch. VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network. All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.

Configuration or reconfiguration of VLANs is done through software. Physically connecting or moving cables and equipment is unnecessary when configuring VLANs.

A workstation in a VLAN group is restricted to communicating with file servers in the same VLAN group. VLANs function by logically segmenting the network into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN. VLANs consist of hosts or networking equipment connected by a single bridging domain. The bridging domain is supported on different networking equipment. LAN switches operate bridging protocols with a separate bridge group for each VLAN.

VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations. VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management. Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain. Traffic should only be routed between VLANs.

Overview of Routing between Virtual LANs

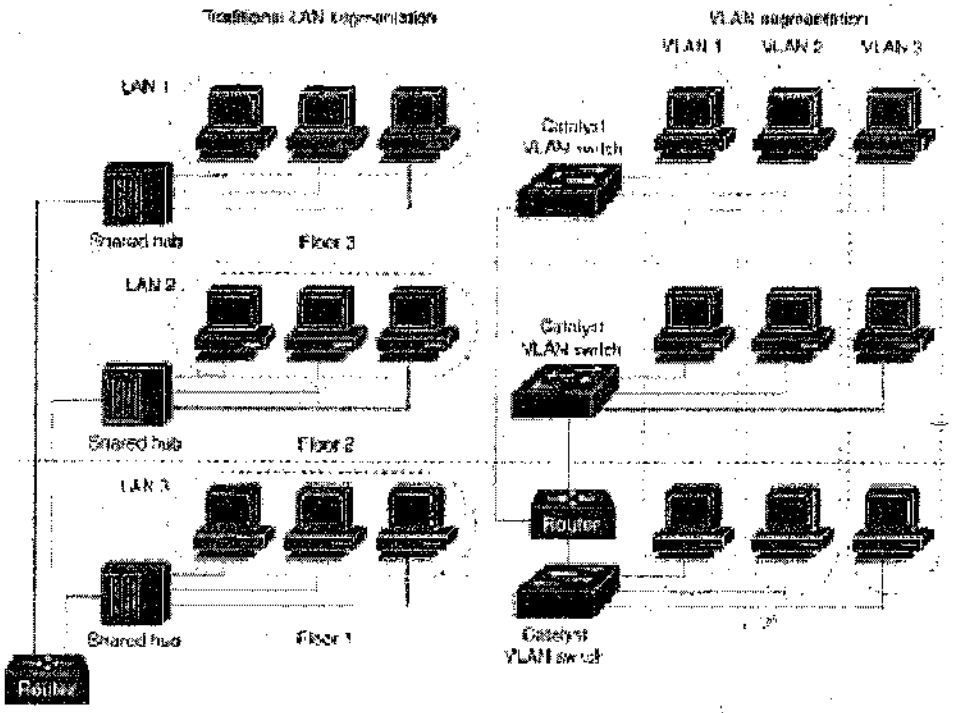
- LAN Segmentation
- Security
- Broadcast Control
- Performance
- Network Management
- Communication between VLANs

LAN Segmentation

VLANs allow logical network topologies to overlay the physical switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer 2 broadcast domains whereby packets are switched between ports designated to be within the same VLAN. By containing traffic originating on a particular LAN only to other LANs in the same VLAN, switched virtual networks avoid wasting bandwidth, a drawback inherent to traditional bridged and switched networks in which packets are often forwarded to LANs with no need for them. Implementation of VLANs also improves scalability, particularly in LAN environments that support broadcast- or multicast-intensive protocols and applications that flood packets throughout the network.

Figure 8 illustrates the difference between traditional physical LAN segmentation and logical VLAN segmentation.

LAN Segmentation and VLAN Segmentation



Security

VLANs also improve security by isolating groups. High-security users can be grouped into a VLAN, possible on the same physical segment, and no users outside that VLAN can communicate with them.

Broadcast Control

Just as switches isolate collision domains for attached hosts and only forward appropriate traffic out a particular port, VLANs provide complete isolation between VLANs. A VLAN is a bridging domain and all broadcast and multicast traffic is contained within it.

Performance

The logical grouping of users allows an accounting group to make intensive use of a networked accounting system assigned to a VLAN that contains just that accounting group and its servers. That group's work will not affect other users. The VLAN configuration improves general network performance by not slowing down other users sharing the network.

Network Management

The logical grouping of users allows easier network management. It is not necessary to pull cables to move a user from one network to another. Adds, moves, and changes are achieved by configuring a port into the appropriate VLAN.

Communication between VLANs

Communication between VLANs is accomplished through routing, and the traditional security and filtering functions of the router can be used. Cisco IOS software provides network services such as security filtering, quality of service (QoS), and accounting on a per VLAN basis. As switched networks evolve to distribute VLANs, Cisco IOS provides key inter-VLAN communications and allows the network to scale.

VLAN Colors

VLAN switching is accomplished through *frame tagging* where traffic originating and contained within a particular virtual topology carries a unique VLAN identifier (VLAN ID) as it traverses a common backbone or trunk link. The VLAN ID enables VLAN switching devices to make intelligent forwarding decisions based on the embedded VLAN ID. Each VLAN is differentiated by a *color*, or VLAN identifier. The unique VLAN ID determines the *frame coloring* for the VLAN. Packets originating and contained within a particular VLAN carry the identifier that uniquely defines that VLAN (by the VLAN ID).

The VLAN ID allows VLAN switches and routers to selectively forward packets to ports with the same VLAN ID. The switch that receives the frame from the source station inserts the VLAN ID and the packet is switched onto the shared backbone network. When the frame exits the switched LAN, a switch strips header and forwards the frame to interfaces that match the VLAN color. If you are using a Cisco network management product such as Vlan Director, you can actually color code the VLANs and monitor VLAN graphically.

Communicating between VLANs

Cisco IOS provides full-feature routing at Layer 3 and translation at Layer 2 between VLANs. There are three different protocols available for routing between VLANs:

- Inter-Switch Link (ISL)
- IEEE 802.10
- ATM LAN Emulation

All three of these technologies are based on OSI Layer 2 bridge multiplexing mechanisms, and are detailed in CCNA - Second year companion guide (Cisco Press).

Self Learning Exercises :

7. Which one is not an advantage of VLANs ?
   (a) VLAN topologies provide broadcast filtering
   (b) VLAN topologies provide security
   (c) VLAN topologies provide traffic flow management
   (d) All of the above
8. Which device is needed for inter-VLAN communication?
   (a) Router (b) NIC
   (c) Switch (d) Hub

3.5 SUMMARY

In the OSI reference model, there are seven numbered layers, each of which illustrates a particular network function: application, presentation, session, transport, network, data link, and physical. The TCP/IP model has the following four layers: application, transport, Internet, and network access.

Although some of the layers in the TCP/IP model have the same name as layers in the OSI model, the layers of the two models do not correspond exactly. The TCP/IP application layer is equivalent to the OSI application, presentation, and session layers. The TCP/IP model combines the OSI data link and physical layers into the network access layer.

No matter which model is applied, networks layers perform the following five conversion steps in order to encapsulate and transmit data:

1. Images and text are converted to data.
2. The data is packaged into segments.
3. The data segment is encapsulated in a packet with the source and destination addresses.
4. The packet is encapsulated in a frame with the MAC address of the next directly connected device.
5. The frame is converted to a pattern of ones and zeros (bits) for transmission on the media.

3.6 GLOSSARY

- **ATM** - Asynchronous Transfer Mode may be used over a variety of media with both baseband and broadband systems. It uses fixed length data packets of 53 bytes called cell switching.
- **ARP** - Address resolution Protocol is used to resolve the hardware address of a card to package the ethernet data. It works at the data link layer. RFC 826.
- **Datagram** - IP header and what is called a message or segment. The message or segment is a transport header (TCP or UDP) and application data. The term datagram is used to describe the information before IP fragmentation or after reassembly
- **DHCP** - Dynamic Host Configuration Protocol is used to assign IP addresses dynamically to network cards works at the application layer. RFC 1541.
- **DNS** - Domain Name System is used on the internet to correlate between IP address and readable names. RFC 1034, 1035, 1535-1537, 1591.

- **Frame** - The unit of transmission in a link layer protocol, consisting of a link-layer header (ethernet) followed by a packet (IP header and data). It may be a part of a fragmented datagram.
- **Frame Relay** - Error checking is handled by devices at both sides of the connection. Frame relay uses frames of varying length and it operates at the data link layer of the OSI model. A permanent virtual circuit (PVC) is established between two points on the network. Frame relay speed is between 56Kbps and 1.544Mbps.
- **FTP** - File Transport Protocol is a TCP/IP protocol running at the application layer.
- **Gateway** - A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Not the same as a default gateway used by a client to send packets to.
- **HTTP** - Hypertext Transfer Protocol is the protocol used to communicate between web servers and web browser software clients.
- **Hub** - A type of repeater used on several network architectures which usually connects several stations.
- **ICMP** - Internet Control Message Protocol is used to perform network error reporting and status. It works at the transport layer. RFC 792.
- **IETF** - Internet Engineering Task Force. Sets Internet technical standards.
- **IGMP** - Internet Group Management Protocol, used for managing multicast groups. RFC 1112.
- **IP** - Internet Protocol os used for software addressing of computers and works at the data link layer. RFC 791.
- **IRTF** - Internet Research Task force.
- **NIC** - Network interface card. Also called LAN adapters.
- **OSI** - Open Systems Interconnect is a suite of protocols developed by the International Standards Organization (ISO) which corresponds with the layers of the OSI model.
- **Packet** - Includes an IP header and data. It may be a complete IP datagram or a fragment of an IP datagram.
- **Segment** - The unit of end-to-end transmission in the TCP protocol which consists of a TCP header followed by application data.
- **SMTP** - Simple Mail Transfer Protocol is a TCP protocol for mail transport running at the application layer. RFC 821, 822.
- **SNMP** - Simple Network Management Protocol. RFC 1155, 1157, 1213, 1441.
- **Subnet** - A part of a network. A class B network may have several class C subnets. Usually routers are used to connect subnets.
- **TCP** - Transport Control protocol is a connection oriented reliable protocol working at the transport layer. RFC 793.
- **TFTP** - Trivial File Transfer Protocol. RFC 1350.
- **Telnet** - Remote session at the application layer. RFC 854.
- **UDP** - User Datagram Protocol is a connection less unreliable protocol working at the transport layer. RFC 768.
- **Unicast** - A transmission to a single interface card.
- **URL** - Universal Resource Relocator is a term used to describe the name of a web based resource such as a web page or location of a file for down loading.

3.7 FURTHER READINGS

1. Data Communication & Networking - Behrouz Forouzan
2. Computer Networks : A.Tanenbaum
3. Data & Computer Networks : William Stallings
4. CCNA - Second year Companion Guide - Cisco Press

3.8 ANSWERS TO THE SELF LEARNING EXERCISES

1. b
2. c
3. d
4. c
5. a
6. b
7. d
8. a

3.9 UNIT END QUESTIONS

1. What is TCP/IP? What are the other well-known standard protocols in the TCP/IP family?
2. Which is more efficient, circuit switching or virtual-circuit switching? Why?
3. What is the fundamental difference between circuit switching and Packet Switching?
4. What is the main difference between TCP and UDP?
5. List out two ways in which the OSI reference model and TCP/IP model Are the same. Now list two ways in which they differ.
6. What tasks are performed by transport layer of TCP/IP?

UNIT - IV

INTERNET

STRUCTURE OF THE UNIT

4.0 Objectives
4.1 Introduction
4.2 Internet
4.3 Intranet
4.4 Internet Architecture
4.4.1 The Open Systems Interconnection (OSI) Model
4.4.2 Internet protocols
4.4.3 Encapsulation
4.4.4 Routing
4.4.5 Domains and the Domain Name System (DNS)
4.5 Summary
4.6 Solutions/Answers
4.7 Unit end questions

4.0 OBJECTIVES

After going through this unit you are able to:

- I know what is Internet and why it is needed.
- I know the difference between Internet and Intranet.
- I learn architecture/structure of Internet.
- I know how Internet works and what are its protocols.

4.1 INTRODUCTION

Data communication has become a fundamental part of how institutions, corporate, and individuals now do business. Worldwide networks gather data and technical information about all subjects. Groups establish electronic mailing to share information. Corporations keep service orders, customer records, inventory, and customer service information in large-scale client/server systems. We have evolved to a stage where the corporation is the network. A few years ago, most networks were independent entities. Users choose hardware technology appropriate to their communication needs. In past couple of decades, internetworking technology made it possible to interconnect many disparate physical networks and use them as a coordinated system. This technology permits computers to communicate independently of their physical network connections.

An internet consists of a set of interconnected government, educational, and business computer networks that act as an integrated whole to provide universal interconnections allowing individual groups to use whichever hardware is best suited to their need. In fact Internet is network of networks. A person at a computer terminal or personal computer with the proper software communicates across the Internet by placing data in an IP packet and "addressing" the packet to a particular destination on the Internet. TCP guarantees end-to-end integrity. Communications software on the intervening networks between the source and destination network "read" the

addresses on packets moving through the Internet and forward the packets towards their destinations. Millions of networks world over are connected to Internet.

4.2 INTERNET

As a complex system of interlinked networks, the Internet supports millions of server computers housing large volume of all sorts of information. The Internet is where millions of friends can chat. It lets people browse through thousands of on-line libraries, play new games, and trade on-line with no geographic bounds. With the introduction of World Wide Web (WWW) browsers, it has become much easier to access information stored in server computers world over. User search the Internet for all types of information, including images, graphics, sound and movie clips, in an even growing number of remote host computers. User receives and distributes this information to others.

Interestingly, nobody owns the Internet (collection of backbone and access network and homed servers), or centrally controls what happens there. The networks within different countries are funded and managed according to local policies. The Internet allows any end system that is equipped with a minimum set of communication capabilities to connect to a large pool of information. The specifications of the Internet technology are publicly available, allowing more anyone to develop the software needed to communicate over the Internet.

4.3 INTRANET

Internet-based technology has now migrated to what are called intranets. These networks are corporate networks that use the same networking/transport protocols and locally based web servers to provide access to vast amount of corporate information in a cohesive fashion. These private intranets use the structure and standards of the Internet and WWW, but are separated from the public Internet by firewalls. These firewalls allow employees to access the Internet while preventing unauthorized users from entering the corporate intranet. The intranet is an inexpensive yet very effective alternative to other form of internal communications in that it provides the mechanism to eliminate paper while increasing accessibility to the information. Example of intranet-based information includes internal telephone books, procedure manuals, training materials, and requisition forms. All of this information can be converted to electronic form on the Web and updated in a low-cost manner.

An intranet is a private network that uses TCP/IP and other Internet protocols. It can run Web servers, Web clients, mail servers and mail clients. It works like a small, private Internet. This is a network that is not available to the world outside of the intranet. If the intranet network is connected to the Internet, the intranet will reside behind a firewall and, if it allows access from the Internet, will be an Extranet. The firewall helps to control access between the intranet and Internet to permit access to the intranet only to people who are members of the same company or organization. In its simplest form, an intranet can be set up on a networked PC without any PC on the network having access via the intranet network to the Internet. For example, consider an office with a few PCs and a few printers all networked together. The network would not be connected to the outside world. On one of the drives of one of the PCs there would be a directory of web pages that comprise the intranet. Other PCs on the network could access this intranet by pointing their browser (Netscape or Internet Explorer) to this directory - for example

U:\inet\index.htm.

From then onwards they would navigate around the intranet in the same way as they would get around the Internet.

An intranet starts with a LAN and adds Internet protocols services. These LANs run LAN communication protocols and TCP/IP simultaneously. An intranet can run on a network larger than a LAN, too, such as wide area networks (WANs), the network that large organizations use to connect geographically separate locations. You can also create extranet, an intranet that allows people to connect into the network over the Internet.

Advantages and disadvantages of intranet

LANs and intranet both let you share hardware, software, and information by connecting computers together. You don't need an intranet to share files and printers, or to send e-mail among the people on your network: a LAN can do all those jobs. The following are some reasons to convert a LAN to an intranet, or to connect your computers together into an intranet:

Intranet uses standard protocols such as TCP/IP. More development is happening for Internet-based communication than other type of communication. For example intranet user can choose a wide variety of e-mail programs, because many have been written for the Internet.

Intranets are scalable because TCP/IP works fine on the Internet, which has millions of computers. So your network can grow without any worry about the communication protocol.

Intranet components are relatively cheap and some are free.

Intranet enables you to setup Internet-style information services. You can have your own private Web, using Web servers on your intranet to serve Web pages to members of your organization only. You can also support chat, Usenet, telnet, FTP, or other Internet services privately on your network.

Intranets let people share their information by creating Web pages for the intranet. Because many word processing programs can now save documents as Web pages, creating pages for an intranet doesn't require a lot of training. Rather than printing and distributing reports, people can put them on the intranet and send e-mails to tell everyone where the report is stored.

Intranet is having some disadvantages too.

Intranet costs money to upgrade computers, buy new software, and run new cabling, and teach people to use the new systems.

People in an organization may waste time if you connect your intranet to the Internet. People may spend hours watching sports results, or checking stock market data. Even if you don't connect your intranet to the Internet, people can waste time designing web site for their personal use, sending e-mails about new product in market.

4.4 INTERNET ARCHITECTURE

The Internet is basically a hierarchy that allows any Internet connected device in one geographic location, talk to another Internet connected device in another geographic location. The way that the information is transmitted varies greatly, and in some countries, wireless ham radios are even used to transmit email. Keep in mind that the word "connected" is used very loosely here.

The Internet system consists of a number of interconnected packet networks supporting communication among host computers using the Internet protocols. These protocols include the Internet Protocol (IP), the Internet Control Message Protocol (ICMP), the Internet Group Management Protocol (IGMP), and a variety transport and application protocols that depend upon them. The Internet Engineering Steering Group periodically releases an Official Protocols memo listing all the Internet protocols.

All Internet protocols use IP as the basic data transport mechanism. IP is a datagram or connectionless, internetwork service and includes provision for addressing, type-of-service specification, fragmentation and reassembly, and security. ICMP and IGMP are considered integral parts of IP, although they are architecturally layered upon IP. ICMP provides error reporting, flow control, first-hop router redirection, and other maintenance and control functions. IGMP provides the mechanisms by which hosts and routers can join and leave IP multicast groups.

Reliable data delivery is provided in the Internet protocol suite by Transport Layer protocols such as the Transmission Control Protocol (TCP), which provides end-end retransmission, resequencing and connection control. Transport Layer connectionless service is provided by the User Datagram Protocol (UDP).

4.4.1 The Open Systems Interconnection (OSI) Model

The seven open systems interconnection layers (OSI) are a staple of most networking textbooks. The idea is that a network will work on many different levels, or "layers" each of which will perform a supporting function for the next layer.

The Network layers are the first three, being the physical link layer, the link layer, and the Network layer. Since the Internet is based on the Internet protocol which is in the Network Layer, and since the Internet can run on any number of different types of layers below that, we normally are not too concerned with the physical layers unless we are building an Ethernet cable, or transmitting an Internet signal through wireless means, and not to interested in the link layer unless we are registering a network card or router MAC address with our service provider.

The top three layers (session, presentation, and application layers) are for program communication, and are completely independent of the network so that the two communicating programs could even be on the same machine.

We also sometimes include the transport layer when discussing the Internet, and often link the transport with the network layer as in the TCP/IP protocols. Transmission Control Protocol (TCP) is in the transport layer, and Internet Protocol (IP) is in the Network layer. Most Internet based functions such as the World Wide Web, and email, uses TCP/IP, so this is a basic building block for the Internet.

The transport layer also makes sure that the top three layers are network independent.

4.4.2 Internet protocols

Of relevance in this subject is a set of protocols used to build the Internet. Figure 1 shows a simplified view of the Internet protocol architecture. This represents an actual protocol implementation and it is easy to see that it bears some similarity to the ISO model.

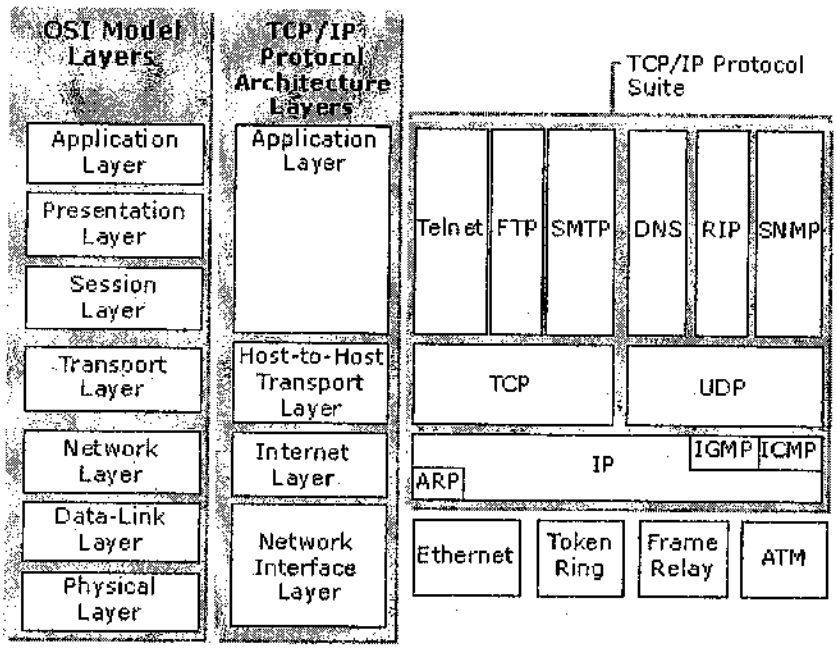


Figure 1: Internet protocol architecture

The layers in this model are:

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set

up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine that can store it for future use.

IP the Internet Protocol, the method or protocol, by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. The packets that follow the IP specification are called an IP datagram. The Internet sends an IP datagram across a single network by placing it inside a network packet. For network the entire IP datagram is data. When network packet arrives at the next computer, the computer opens the packet and extracts the datagram. The receiver examines the destination address on the datagram to determine how to process it. When a router, determines that datagram must be sent across the network, the router creates a new network packet, encloses the datagram inside the packet and sends the packet across another network towards its destination. When a packet carrying a datagram arrives at its final destination, local software on the machine opens the packet and processes the datagram. Because a message is divided into a number of packets, a different route can be used by different packets. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It is up to another protocol, the Transmission Control Protocol (TCP) to put them back in right order. IP is a connectionless protocol, which means that there is no established connection between the end points that are communicating. Each packet that arrives through the Internet is treated as an independent unit of data without any relation to any other unit of data.

ARP (Address Resolution Protocol) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long (the physical machine address is also known as a Media Access Control or MAC address.). A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

4.4.3 Encapsulation

Suppose an application sends some data using UDP. The data will pass through each of the protocol layers: UDP first, then the IP layer, then on to the network layer. Similarly, any data that is received from the network traverses these layers in the reverse order: then network layer first, then the IP layer, then the UDP layer, after which it is delivered to the application. To help with the exchange, each of these layers adds its own control and status information to the data. This extra information can be added at the beginning of the data as a header or at the end of the data as a trailer; the data itself is referred to as the payload. We say that a layer encapsulates the data passed to it from the layer above.

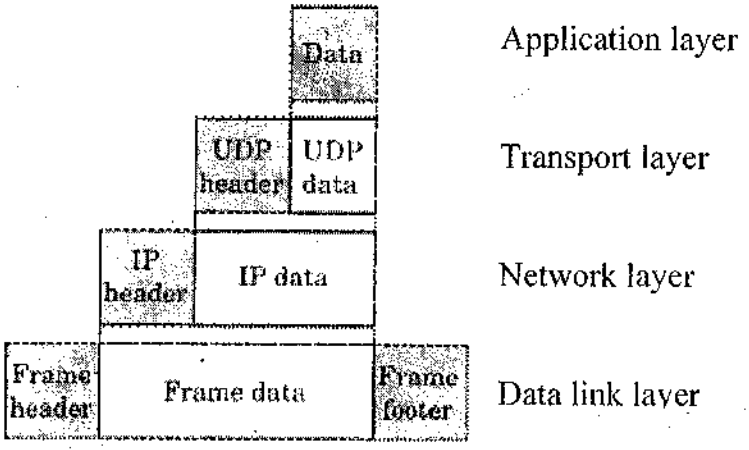


Figure 2: Encapsulation of data within a UDP datagram within an IP packet

4.4.4 Routing

In reality, the Internet is really a collection of smaller networks linked together in many places. If we accept this model, then the process of routing or sending Internet packets around the Internet is quite simple.

A packet that follows the IP specification is called an IP *datagram*. A datagram travels across the Internet independent of the sender. The Internet sends an IP datagram across a single network by placing it inside a network packet. As far as the network is concerned, the entire datagram is data. When the packet arrives at the next computer, the packet is "opened" to extract the datagram. The receiver examines the destination address on the datagram to determine how to process it. In particular, if a router decides that the datagram must be sent across another network, the router "encloses" the datagram inside another network packet and sends it on its way.

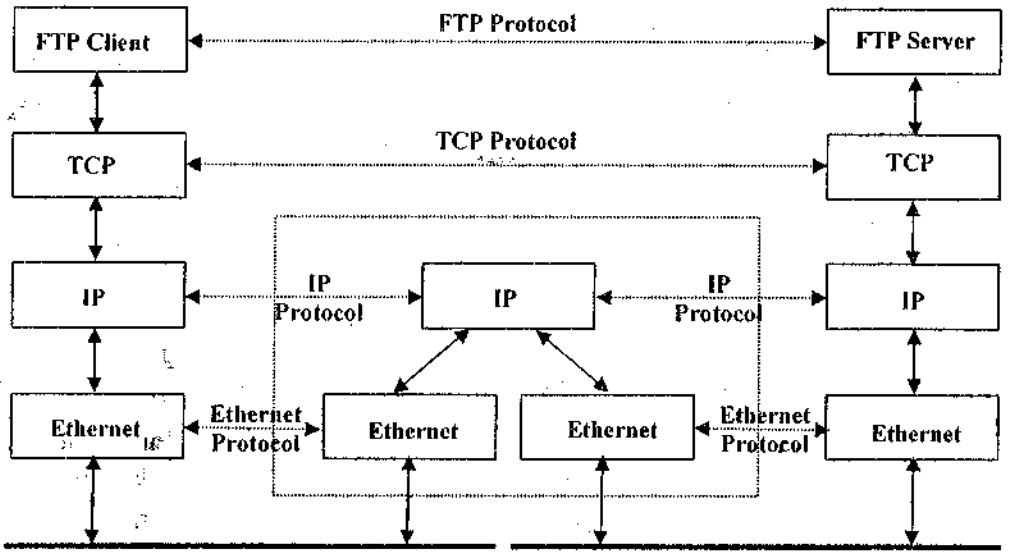


Figure 3: Routing in TCP/IP

Each datagram has a source IP address and a destination IP address in the IP header information. As a datagram is passed to the gateway (each host knows who its gateway is), it follows rules as to where it should go. Simply put, the router, or gateway looks at the packet and says "is this destination IP address in my network, or should I send it off to my gateway?". Obviously there is much more to it, but at the simplest level (recall our home firewall router example), that is really what happens in a "static routing table". There are, of course extremely complex rules automatically set by protocols such as border gate protocol (BDP) by higher level upstream providers (Telus, Sprint, etc.) since your destination IP address may not just be upstream, but may also be downstream somewhere too.

A router consists of a computer with at least two network interfaces, a rudimentary operating system, and the IP software, as shown in the dotted box above. This figure shows the router connected to two Ethernet networks. In fact, any suitable link layer can be used to transfer the IP datagrams.

4.4.5 Domains and the Domain Name System (DNS)

All this talk about numbers is great for computers, but for us humans, we remember names better. After all it is much easier to remember a name like www.redhat.com, than 66.187.232.50. Names are also useful incase we do something like change all the numbers on the Internet and make them REALLY hard to remember as will be the case as IPV6 is slowly introduced. IP addresses change, but names are supposed to be more static changing only when there is a human reason for it.

A domain name is a name given to a network for ease of reference by humans. But somebody ultimately has to translate these domain names into IP addresses, because it is only 32-bit IP addresses of computers that the Internet understands. In some organizations computers are identified by some names. Two computers in a network cannot have same name. For Internet too, computer names are made unique globally. Internet naming convention uses a simple idea. Additional strings are added to the names. Full name of a computer consists of its local name followed by a period followed by the organization's suffix. For example if Himalaya is a computer in IBM, then its name can be himalaya.ibm.

When ARPAnet moved to TCP/IP, the population of the Internet exploded, and this primitive "hosts" scheme no longer worked.

To solve this, a distributed database called the Domain Name System was created. The idea is to have a robust, and high performing database that is accessible to all devices on the Internet. Many use a phone book as an analogy for this system where your computer or device has a number similar to a phone number, and the DNS system, similar to a phone book lets you look up that number to find another device on the Internet.

The structure of the hierarchy is that there is one "root" point, and several nodes coming off of that root point called "top level domains", or tld's for short. We all have heard of "dot-com". Dot-com (.com) is a top level domain. So is .ca, .net, .org, .cc, .info, .uk, .edu, and a whole bunch of others. The website of the authority for the "root" of the Internet is at IANA.org. IANA is an acronym for the Internet Assigned Numbers Authority. The actual root point is not a single computer, but several core networks possibly separately corporately owned, but it is simpler to imagine it as a single point.

IANA does many things including distributing Internet numbers to providers. To do this they delegate to a non-profit organization whose website is ICANN.org.

The structure of the domain names below the top level domains is organized by the sponsors. For the ".uk", and ".au" domains, for example, the domain names are sub-divided into sub roots such as .co.uk, or .com.au whereas in the gTLD's we have all the names directly below the root name such as in compeng.net. In Canada we allow any Canadian legal entity to have a subdomain right below the tld such as computerengineering.ca. We also allow province level sub-domains such as compusmart.ab.ca, and at one time allowed city level sub-domains such as joesgarage.edmonton.ab.ca.

Code	Applicable for
.com	Commercial organizations
.net	Network organizations
.gov	Parts of governments
.edu	Organizations of higher education
.mil	Non-classified military networks
.org	Organization that do not fit the commercial or educational designations.

Non-Geographic domains

Country	Domain Name
AUSTRALIA	.au
CHINA	.cn
GERMANY	.de
INDIA	.in
JAPAN	.jp
UNITED KINGDOM	.uk
UNITED STATES	.us

Geographic Domains

In the example of computerengineering.ca, the owner of that domain (Computer Engineering Inc.) has full authority over all of its sub-domains, so that they can create sub-domains on there such as www.computerengineering.ca, or this.is.a.great.company.computerengineering.ca

Check Your Progress 1

1. State whether True or False:
   (a) TCP and UDP are part of the transport layer.
   (b) The Internet layer follows a datagram philosophy.
   (c) A computer can resolve another computer's address even if both the computers are on different physical network.
   (d) IP is a connection oriented protocol.
   (e) The transport layer runs on the top of the Internet layer.
   (f) The firewall helps to control access between the Intranet and Internet.
2. What are the responsibilities of IP layer?
3. What is the purpose of Domain Name System?

4.5 SUMMARY

This unit described the basic concepts about Internet and intranet. Internet is a network of networks where lots of information is available and is meant to be utilized by you. No one owns the Internet. It consists of a large number of interconnected autonomous networks that connect millions of computers across the world. TCP/IP is the main protocol used on Internet. This protocol is very much similar to OSI. Intranet is basically a private network which uses feature and protocols of the Internet and provide similar services on there network. Unit also described various protocols used in Internet along with some basic concepts like Domain, Domain Name System and routing concepts. Unit also discussed the way a message is divided into smaller packets and delivered to destination using Internet protocols.

4.6 SOLUTIONS/ANSWERS

Check your progress 1

1. (a) True (b) True
   (c) False (d) False
   (e) True (f) True.
2. IP is the protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. Each packet contains sender's and receiver's IP address. It is responsibility of IP to deliver or forward these packets in right direction towards receiver.
3. On Internet each computer or network is identified by its IP address which is a 32-bit number. Numbers are easy for computers but it is difficult to remember these addresses. So human use domain names when referring to computers on the Internet. Domain Name System (DNS) is a database containing the mapping between the domain names and IP addresses scattered across different computers. The DNS is consulted whenever any message is sent to any other computer on the Internet.

4.7 UNIT END QUESTIONS

1. What is TCP/IP?
2. What is Internet and Intranet?
3. What is DNS?
4. Explain the Routing in TCP/IP.

UNIT - V

INTERNET FEATURES

STRUCTURE OF THE UNIT

5.0 Objectives
5.1 Introduction
5.2 Internet services
5.2.1 E-mail
5.2.1.1 How Internet e-mail works
5.2.1.2 E-mail Transfer Protocols
5.2.1.3 How to send Email
5.2.1.4 Spamming
5.2.1.5 Privacy problems regarding e-mail
5.2.2 Internet telephony
5.2.2.1 Voice over Internet Protocol
5.3.2.2 Technical Barriers
5.3.2.3 Future of Internet Telephony
5.2.2.4 Advantages of Internet Telephony
5.2.3 World Wide Web
5.2.3.1 Structure of WWW
5.2.3.2 The Hypertext Document
5.2.3.3 Web Server
5.2.4 Internet Relay Chat (IRC)
5.2.4.1 Internet Relay Chat (IRC) Features
5.2.5 News Groups
5.2.6 File Transfer
5.2.6.1 Criticisms of FTP
5.2.6.2 Security problems
5.2.6.3 Anonymous FTP
5.2.6.4 Data formats
5.2.7 Remote login and TELNET
5.3 Internet Hardware
5.3.1 MODEM selection
5.3.2 MODEM Installation
5.4 Summary
5.5 Solutions/Answers
5.6 Unit end questions

5.0 OBJECTIVES

This section describes various services available on Internet. The most frequently used services are e-mail, World Wide Web (WWW), file transfer, remote login, Usenet and chat. Each service has its own protocol, which are discussed in this section.

5.1 INTRODUCTION

For many Internet users, electronic mail (e-mail) has practically replaced the Postal Service for short written transactions. Electronic mail is the most widely used application on the Net. You can also carry on live "conversations" with other computer users, using Internet Relay Chat (IRC). More recently, Internet telephony hardware and software allows real-time voice conversations. You can transfer files to and from remote computers using the File Transfer Protocol (FTP). You may want to log-in to a remote computer using the Telnet, which enables you to use the remote system and its software, data, and other facilities. You may form a user network through Usenet. You may like to chat with other members of your group through Internet Relay Chat (IRC).

The most widely used part of the Internet is the World Wide Web (often abbreviated "WWW" or called "the Web"). Its outstanding feature is hypertext, a method of instant cross-referencing. In most Web sites, certain words or phrases appear in text of a different color than the rest; often this text is also underlined. When you select one of these words or phrases, you will be transferred to the site or page that is relevant to this word or phrase. Sometimes there are buttons, images, or portions of images that are "clickable." If you move the pointer over a spot on a Web site and the pointer changes into a hand, this indicates that you can click and be transferred to another site.

5.2 INTERNET SERVICES

The number of Internet users and uses are growing phenomenally. Presently, many services are available through the Internet. Main services available on Internet are:

- E-mails
- Net telephony / Voice over IP (VOIP)
- World Wide Web (WWW)
- Internet Relay Chat (IRC)
- News and USENET
- File transfer (FTP and anonymous FTP)
- Remote Login (Telnet)
- The Gopher
- Wireless Application Protocol (WAP)
- Web casting of video.
- e-Commerce
- Wide Area Information Service (WAIS)

Now we discuss some of these popular Internet services in detail.

5.2.1 E-MAIL

E-mail is an electronic version of sending a letter. You can send e-mail from your computer at any time of the day to any address around the world and your electronic letter will arrive at its destination seconds after you send it... even if the receiver lives on the other side of the world. The receiver has to "pick-up" their mail - usually this means dialing their local Internet Service

Provider to check their mail box before they will receive your e-mail. Today many people use broadband Internet connections that are "always on", and often work with computers daily, meaning they receive their e-mail more regularly. E-mail messages are usually encoded in ASCII text. However, you can also send non-text files, such as graphic images and sound files, as attachments sent in binary streams. E-mail was one of the first uses of the Internet and is still the most popular use. A large percentage of the total traffic over the Internet is e-mail. E-mail can also be exchanged between online service provider users and in networks other than the Internet, both public and private.

E-mail can be distributed to lists of people as well as to individuals. A shared distribution list can be managed by using an e-mail reflector. Some mailing lists allow you to subscribe by sending a request to the mailing list administrator. A mailing list that is administered automatically is called a list server.

E-mail is one of the protocols included with the Transport Control Protocol/Internet Protocol (TCP/IP) suite of protocols. A popular protocol for sending e-mail is Simple Mail Transfer Protocol (SMTP) and a popular protocol for receiving it is POP3. Both Netscape and Microsoft include an e-mail utility with their Web browsers.

Your E-mail Address

Your e-mail address is usually your user name, followed by an @ sign, followed by the domain name of the Internet Service Provider (ISP) through which you are connecting to the Internet.

If your name is "Mary Smith" and your user name is "msmith", and you are connecting through the ISP Ozemail, your e-mail address will be "msmith@ozemail.com.au".

Like a URL on the web, the "ozemail.com.au" is the domain name of the server you will dial to send and receive your e-mail. The "ozemail" is the name of the service provider, the "com" means "company" or "commercial", the "au" denotes "Australia" (if you left the "au" off the end then the e-mail message might be delivered to a mail server in America if there happen to be a "ozemail.com" domain name server there).

5.2.1.1 How Internet e-mail works

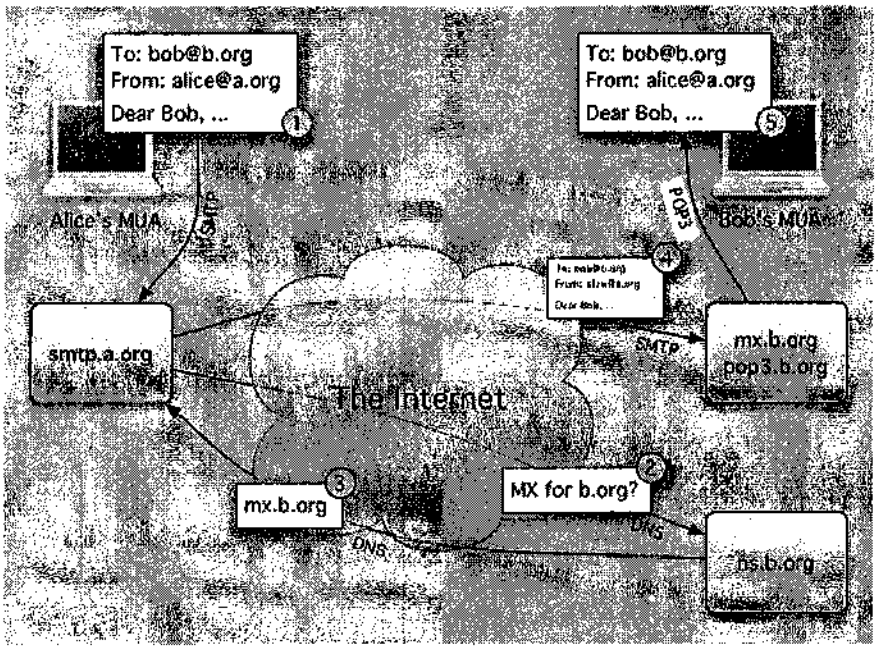


Figure 1: Working of e-mail on Internet

The diagram above shows a typical sequence of events that takes place when Alice composes a message using her mail user agent (MUA) software. She types in, or selects from an address book, the e-mail address of her correspondent. She hits the "send" button.

Her MUA formats the message in Internet e-mail format and uses the Simple Mail Transfer Protocol (SMTP) to send the message to the local mail transfer agent (MTA), in this case **smtp.a.org**, run by Alice's Internet Service Provider (ISP).

The MTA looks at the destination address provided in the SMTP protocol (not from the message header), in this case **bob@b.org**. An Internet e-mail address is a string of the form **localpart@domain.example**, which is known as a Fully Qualified Domain Address (FQDA). The part before the @ sign is the local part of the address, often the username of the recipient, and the part after the @ sign is a domain name. The MTA looks up this domain name in the Domain Name System(DNS) to find the mail exchange servers accepting messages for that domain. The DNS server for the **b.org** domain, **ns.b.org**, responds with an MX record listing the mail exchange servers for that domain, in this case **mx.b.org**, a server run by Bob's ISP. **smtp.a.org** sends the message to **mx.b.org** using SMTP, which delivers it to the mailbox of the user bob. Bob presses the "get mail" button in his MUA, which picks up the message using the Post Office Protocol (POP3).

This sequence of events applies to the majority of e-mail users. However, there are many alternative possibilities and complications to the e-mail system:

- Alice or Bob may use a client connected to a corporate e-mail system, such as IBM's Lotus Notes or Microsoft's Exchange. These systems often have their own internal e-mail format and their clients typically communicate with the e-mail server using a vendor-specific, proprietary protocol. The server sends or receives e-mail via the Internet through the product's Internet mail gateway which also does any necessary reformatting. If Alice and Bob work for the same company, the entire transaction may happen completely within a single corporate e-mail system.
- Alice may not have a MUA on her computer but instead may connect to a web mail service.
- Alice's computer may run its own MTA.
- Bob may pick up his e-mail in many ways, for example using the Internet Message Access Protocol, by logging into **mx.b.org** and reading it directly, or by using a web mail service.
- Domains usually have several mail exchange servers so that they can continue to accept mail when the main mail exchange server is not available.

It used to be the case that many MTAs would accept messages for any recipient on the Internet and do their best to deliver them. Such MTAs are called open mail relays. This was important in the early days of the Internet when network connections were unreliable. If an MTA couldn't reach the destination, it could at least deliver it to a relay that was closer to the destination. The relay would have a better chance of delivering the message at a later time. However, this mechanism proved to be exploitable by people sending unsolicited bulk e-mail and as a consequence very few modern MTAs are open mail relays, and many MTAs will not accept messages from open mail relays because such messages are very likely to be spam.

5.2.1.2 E-mail Transfer Protocols

For email messaging, every domain has email server computer set up which run protocol software that enable email communication. There are two main email protocols: SMTP and POP.

SMTP is responsible for transmitting an email message between the sender and the recipient, whereas POP is concerned with the retrieval of an email message stored on a server computer. Both the email protocol software programs run on server. Internet Message Access Protocol version 4 (IMAP4) is the latest new standard in place of POP3.

Simple Mail Transfer Protocol (SMTP)

The SMTP actually transfers the email message from the SMTP server of the sender to the SMTP server of the recipient. SMTP runs on the top of TCP/IP. At the sender's end, an SMTP server takes the message sent by a user's computer and transfers the message to the SMTP server of the recipient. The SMTP server at the recipient's end then takes the email message and stores it in the appropriate user's mailbox.

Post Office Protocol (POP):

The POP provides a standard mechanism for retrieving emails from a remote server for email recipient. When a person X sends an email to person Y, this email is stored in the mailbox of Y provided by the email server. When Y connects to the Internet and wants to see the new emails arrived for him, he opens his email client program, which in turn invokes the POP client. POP client contacts the POP server, which opens the mailbox for user Y and sends the emails arrived for him to the POP client running at user's computer. POP has two modes: the delete mode and the keep mode. In the delete mode, the mail is deleted from the mailbox after each retrieval. In the keep mode, the mail remains in the mailbox after retrieval. The current version of POP is 3, and therefore it is sometimes also known as POP3.

Internet Message Access Protocol (IMAP)

IMAP 4 permits the following:

- Message status flags to indicate whether the message has been read or answered.
- Three modes: On-line, off-line and disconnect network modes. Disconnect mode helps in synchronizing the connection.
- Concurrent access to a common mailbox at the server.
- User can search the contents of the email for a specific string prior to downloading.
- Allows mail to be sent and received simultaneously.
- User can partially download email if bandwidth is limited and the email contains multimedia with high bandwidth requirements.
- User can create, delete, or rename mailboxes on the mail server.
- User can create hierarchy of mailboxes in a folder for email storage.

5.2.1.2 Internet e-mail format

Internet e-mail messages consist of two major sections:

- **Header** - Structured into fields such as summary, sender, receiver, and other information about the e-mail
- **Body** - The message itself as unstructured text; sometimes containing a signature block at the end

The header is separated from the body by a blank line. The message header consists of fields, usually including at least the following:

From: The e-mail address, and optionally name, of the sender of the message

To: The e-mail address(es), and optionally name(s), of the receiver(s) of the message

Subject: A brief summary of the contents of the message

Date: The local time and date when the message was originally sent

Each header field has a name and a value. Informally, the field name starts in the first character of a line, followed by a ":", followed by the value which is continued on non-null subsequent lines that have a space or tab as their first character. Field names and values are restricted to 7-bit ASCII characters. Non-ASCII values may be represented using MIME encoded words.

Note that the "**To**" field in the header is not necessarily related to the addresses to which the message is delivered. The actual delivery list is supplied in the SMTP protocol, not extracted from the header content. The "**To**" field is similar to the greeting at the top of a conventional letter which is delivered according to the address on the outer envelope. Also note that the "**From**" field does not have to be the real sender of the e-mail message. It is very easy to fake the "**From**" field and let a message seem to be from any mail address. It is possible to digitally sign e-mail, which is much harder to fake. Some Internet service providers do not relay e-mail claiming to come from a domain not hosted by them, but very few (if any) check to make sure that the person or even e-mail address named in the "**From**" field is the one associated with the connection. Some internet service providers apply e-mail authentication systems to e-mail being sent through their MTA to allow other MTAs to detect forged spam that might apparently appear to be from them.

Other common header fields include:

Cc: carbon copy

Received: Tracking information generated by mail servers that have previously handled a message

Content-Type: Information about how the message has to be displayed, usually a MIME type Many e-mail clients present "**Bcc**" (Blind carbon copy, recipients not visible in the "**To**" field) as a header field. Since the entire header is visible to all recipients, "**Bcc**" is not included in the message header. Addresses added as "**Bcc**" are only added to the SMTP delivery list, and do not get included in the message data.

5.2.1.3 How to send Email

When you have got an email address and logged into your email account, how do you send email? This is very simple and most email programs (outlook express) use the same functions. All you need to do to send email is click on the "compose"/"write mail" email button, then enter the email address you want to send to, the subject of the email, the message of the email and then press the "send" button. In most email programs you will find the below functions,

- Include a file in a mail message
- Access and read your incoming mail
- Print incoming mail
- Save incoming mail in a file
- Send and reply to a message
- Import/export special objects into/from your mail

Receiving a message

A summary of the mail you have received can be viewed in the "Inbox" folder. To open the Inbox, either double click on the Inbox folder or go to "Mailbox", then "In". To open the Inbox in Outlook Express, simply click once on the Inbox folder.

The Inbox window displays the details of each new e-mail in a single line. This line item is called a "message header". In order it shows, the unread icon (a bullet on an unopened envelop), the mail priority, the author, the date, the size in kilobytes, and the subject.

To view individual mail, simply double click on the line describing the mail to be viewed. In Outlook you can "preview" each message by single clicking on the message header. This will display the message in the bottom "frame" of your screen. All the frame borders, horizontal and vertical are re-sizable the Outlook Express. Simple bring your mouse over the border and it will change to a double-headed black arrow. Click and hold to drag the border up or down, or left or right.

Replying, Forwarding and Re-directing

In some cases you will want to reply to, forward on or redirect mail. With an e-mail open and in the active window, any of these actions can be taken by selecting the appropriate toolbar button. If you mouse over a button, and pause, it will pop up a little help message telling you what that button does.

When you reply to or forward mail, a new window is opened and the text of the original mail is copied into the new message area. This original mail text is distinguished by leading every line with a '>' or a "|" sign. Notice that the subject line has had the characters "Re:" automatically put there when you hit the "Reply" button, or "Fw:" for when you hit the "Forward" button.

If you are forwarding mail, you must enter a new e-mail address. If you are replying to mail, this is automatically set to the address of the original author. You simply enter your reply and hit the "Send" button. If you wish to reply to all those that received a "Cc" of the original message (a Reply All), then hold down the shift key when selecting "Reply" button.

Redirecting mail is like redirecting an unopened postal envelope. The only difference the final recipient will notice is in the "From:" field which will contain both the original author's name and a 'by way of' reference to yourself.

5.2.1.4 Spamming

The usefulness of e-mail is being threatened by three phenomena: spamming, phishing and e-mail worms. Spamming is unsolicited commercial e-mail. Because of the very low cost of sending e-mail, spammers can send hundreds of millions of e-mail messages each day over an inexpensive Internet connection. Hundreds of active spammers sending this volume of mail results in information overload for many computer users who receive tens or even hundreds of junk messages each day.

E-mail worms use e-mail as a way of replicating themselves into vulnerable computers. Although the first e-mail worm affected UNIX computers, the problem is most common today on the more popular Microsoft Windows operating system.

The combination of spam and worm programs results in users receiving a constant drizzle of junk e-mail, which reduces the usefulness of e-mail as a practical tool.

A number of anti-spam techniques mitigate the impact of spam. You can mark spam emails so that in future you will not receive spam from same source. Some countries are making laws for spam which puts some restrictions on spams.

Here are some tricks you can do to reduce or remove Spam

Remove junk mail before you download it to your PC. Use a free POP account checker like http://www.mail2web.com/ to view your POP account contents before downloading your mail in

Outlook Express (OE) or your preferred e-mail client. There are a number of tools and web sites you can use to query your mail box before download.

Use your email client's blocked senders feature. Blocking a sender means that you will no longer receive mail from that source. Most spammers however are already ahead of this feature, and change or hide the address from which they send the spam, so your Blocked Senders list does not recognize the new sender as a blocked one. To block a sender in Outlook Express simply single click a message header, then go MESSAGE> BLOCK SENDER... Outlook will remove all inbound mail from that source and delete future mail from the same source. This method takes a bit of persistence, but pays dividends over time.

Use your email client's message rules feature. Outlook Express message rules feature is really aimed at allowing you to file messages as they arrive. You can however set up rules that look for certain words and characters, say in the subject line of an inbound e-mail, and file that message in the Deleted Items folder or delete it from the server. You could for example ask Outlook Express to look for occurrences of the words like "loan repayments" or "great offer" and have these messages automatically filed in the Deleted Items or removed before downloading them. If you do this however, you should be aware that you could be accidentally deleting bona fide message from people you know.

Do not post your email address in newsgroups or on web pages generally. If you really must post an email address in a newsgroup, consider obtaining a free web mail account from a provider such as Hotmail. Use this to monitor your newsgroup or post questions in forums etc, and discard it when the spam level increases. In the meantime your "real" email address is still used by your contacts and receives less spam.

Install spam blocking software like Spam Inspector (recently acquired by Microsoft) or Spamihilator (freeware). There are several techniques that these programs use to counter spam for example, constructing a blacklist and a whitelist of senders so that immediately, the program can separate trusted and junk mail. For senders not on either list the software can make rule-based judgments based on the appearance of certain words in the email subject and body text. Suspected spam is usually quarantined in a separate folder so that you can review it, just in case a genuine email has been accidentally trapped. Note that because the use of spam blocking software is increasing, you may consider avoiding the use of certain words in emails to people who use it.

Change you email addresses- sounds extreme, but very effective. Here's how. Make two new email addresses for your domain. Decide on a public one that will go on your web site, and a private one that will only ever be passed on by word of mouth and email to your chosen correspondents. Encode the new public email address at Email Address Encoder. It is a hack, and not valid html, but it works. Use the encoded characters on your web site (and in forms). This will slow the spammer's recognition of what is an email address from amongst the code on your site. When the spammers do eventually catch up with your new, public email address, just change it and encode it again... maybe on a six month basis. This works! You can reduce your spam to nil. The best thing about this solution is unlike any of the above ideas; with this one spam does not come any where near your pc. You will have to tell people though what your new private email address is, and not use the public one on business livery, but that can be phased in quickly.

5.2.1.5 Privacy problems regarding e-mail

E-mail privacy, without some security precautions, can be compromised because

- e-mail messages are generally not encrypted;

- e-mail messages have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages;
- Many Internet Service Providers (ISP) store copies of your e-mail messages on their mail servers before they are delivered. The backups of these can remain up to several months on their server, even if you delete them in your mailbox;
- The Received: headers and other information in the email can often identify the sender, preventing anonymous communication.

There are cryptography applications that can serve as a remedy to one or more of the above. For example, Virtual Private Networks or the Tor anonymity network can be used to encrypt traffic from the user machine to a safer network while GPG, PGP or S/MIME can be used for end-to-end message encryption, and SMTP STARTTLS or SMTP over Transport Layer Security/Secure Sockets Layer can be used to encrypt communications for a single mail hop between the SMTP client and the SMTP server.

5.2.1.6 Check Your Progress 1

1. What are the names of the protocols used for email over the Internet?
2. What are the two main parts of an email?
3. What is the purpose of MUA and MTA?
4. What is spamming?
5. Explain working of POP.

5.2.2 INTERNET TELEPHONY

Internet telephony refers to communications services — voice, facsimile, and/or voice-messaging applications—that are transported via the Internet, rather than the public switched telephone network (PSTN). The basic steps involved in originating an Internet telephony call are conversion of the analog voice signal to digital format and compression / translation of the signal into Internet protocol (IP) packets for transmission over the Internet; the process is reversed at the receiving end. Internet Telephony is a general term for technologies that use the Internet Protocol's packet-switched connections to exchange voice, fax, video and other forms of information. Internet Telephony converges voice, video and data, effectively collapsing three networks into one. To date, however, Internet telephony does not offer the same quality of telephone service as direct telephone connections.

Internet Telephony utilizes established data communication networks to provide telephone services between users. The user phone (or multimedia package on a PC) is attached to a specialized Digital Signal Processing (DSP) device where the voice signal is converted into data packets. Special software on the conversion device translates the destination phone number into an IP address, attaches the appropriate IP header information to the packet, and forwards it to the nearest IP data router to be forwarded to the destination address. The destination system utilizes its DSP to convert the data packets into a voice signal that can be heard on a regular phone receiver or PC speakers.

There are three different ways to place a call using Internet Telephony -

ATA – The most common way to place a telephone way using Internet Telephony is ATA. ATA stands for analog telephone adapter; and it takes the analog signals from your phone and converts it to digital data ready for transmission over the Internet. ATA allows you to connect a standard telephone device to your computer for use with Internet Telephony. You need special software to make it work, but overall is very easy to use.

IP Phones – IP phones look and function just like your ordinary everyday phones but instead of routing your phones through the PSTN lines they route your calls through the Internet Protocol.

Computer to computer – This is by far the simplest way to use Internet Telephony. All you need are special software programs that can route your calls. There are many software available that you can use to call directly using your Computer. Other than the software you need a microphone, speakers, sound card and a fast Internet connection.

5.2.2.1 Voice over Internet Protocol

Although progressing rapidly, Internet telephony still has some problems with reliability and sound quality, due primarily to limitations both in Internet bandwidth and current compression technology. As a result, most corporations looking to reduce their phone bills today confine their Internet-telephony applications to their intranets. With more predictable bandwidth available than the public Internet, intranets can support full-duplex, real-time voice communications. Corporations generally limit their Internet voice traffic to half-duplex asynchronous applications (e.g., voice messaging).

Internet telephony within an intranet enables users to save on long-distance bills between sites; they can make point-to-point calls via gateway servers attached to the local-area network (LAN). No PC–based telephony software or Internet account is required.

For example, User A in New York wants to make a (point-to-point) phone call to User B in the company's Geneva office. He picks up the phone and dials an extension to connect with the gateway server, which is equipped with a telephony board and compression-conversion software; the server configures the private branch exchange (PBX) to digitize the upcoming call. User A then dials the number of the London office, and the gateway server transmits the (digitized, IP–packetized) call over the IP–based wide-area network (WAN) to the gateway at the Geneva end. The Geneva gateway converts the digital signal back to analog format and delivers it to the called party.

This version of Internet telephony also enables companies to transmit their (digitized) voice and data traffic together over the intranet in support of shared applications and whiteboarding.

5.2.2.2 Technical Barriers

The ultimate objective of Internet telephony is, of course, reliable, high-quality voice service, the kind that users expect from the PSTN. At the moment, however, that level of reliability and sound quality is not available on the Internet, primarily because of bandwidth limitations that lead to packet loss. In voice communications, packet loss shows up in the form of gaps or periods of silence in the conversation, leading to a clipped-speech effect that is unsatisfactory for most users and unacceptable in business communications.

The Internet, a collection of more than 130,000 networks, is gaining in popularity as millions of new users sign on every month. The increasingly heavy use of the Internet's limited bandwidth often results in congestion which, in turn, can cause delays in packet transmission. Such network delays mean packets are lost or discarded.

In addition, because the Internet is a packet-switched or connectionless network, the individual packets of each voice signal travel over separate network paths for reassembly in the proper sequence at their ultimate destination. While this makes for a more efficient use of network resources than the circuit-switched PSTN, which routes a call over a single path, it also increases the chances for packet loss.

Network reliability and sound quality also are functions of the voice-encoding techniques and associated voice-processing functions of the gateway servers. To date, most developers of Internet-telephony software, as well as vendors of gateway servers, have been using a variety of speech-compression protocols. The use of various speech-coding algorithms—with their different bit rates and mechanisms for reconstructing voice packets and handling delays—produces varying levels of intelligibility and fidelity in sound transmitted over the Internet. The lack of standardized protocols also means that many Internet-telephony products do not interoperate with each other or with the PSTN.

5.2.2.3 Future of Internet Telephony

Several factors will influence future developments in VoIP products and services. Currently, the most promising areas for VoIP are corporate intranets and commercial extranets. Their IP–based infrastructures enable operators to control who can—and cannot—use the network.

Another influential element in the ongoing Internet-telephony evolution is the VoIP gateway. As these gateways evolve from PC–based platforms to robust embedded systems, each will be able to handle hundreds of simultaneous calls. Consequently, corporations will deploy large numbers of them in an effort to reduce the expenses associated with high-volume voice, fax, and videoconferencing traffic. The economics of placing all traffic—data, voice, and video—over an IP–based network will pull companies in this direction, simply because IP will act as a unifying agent, regardless of the underlying architecture (i.e., leased lines, frame relay, or ATM) of an organization's network.

Commercial extranets, based on conservatively engineered IP networks, will deliver VoIP and facsimile over Internet protocol (FAXoIP) services to the general public. By guaranteeing specific parameters, such as packet delay, packet jitter, and service interoperability, these extranets will ensure reliable network support for such applications.

VoIP products and services transported via the public Internet will be niche markets that can tolerate the varying performance levels of that transport medium. Telecommunications carriers most likely will rely on the public Internet to provide telephone service between/among geographic locations that today are high-tariff areas. It is unlikely that the public Internet's performance characteristics will improve sufficiently within the next two years to stimulate significant growth in VoIP for that medium.

However, the public Internet will be able to handle voice and video services quite reliably within the next three to five years, once two critical changes take place:

- an increase by several orders of magnitude in backbone bandwidth and access speeds, stemming from the deployment of IP/ATM/synchronous optical network (SONET) and ISDN, cable modems, and x digital subscriber line (xDSL) technologies, respectively
- the tiering of the public Internet, in which users will be required to pay for the specific service levels they require

On the other hand, FAXoIP products and services via the public Internet will become economically viable more quickly than voice and video, primarily because the technical roadblocks are less challenging. Within two years, corporations will take their fax traffic off the PSTN and move it quickly to the public Internet and corporate Intranet, first through FAXoIP gateways and then via IP–capable fax machines. Standards for IP–based fax transmission will be in place by the end of this year.

Throughout the remainder of this decade, videoconferencing with data collaboration will become the normal method of corporate communications, as network performance and interoperability increase and business organizations appreciate the economics of telecommuting. Soon, the video camera will be a standard piece of computer hardware, for full-featured multimedia systems.

5.2.2.4 Advantages of Internet Telephony

With a traditional telephone line or PSTN line you pay for the actual time usage. The more time you spend on the telephone talking to people the higher will be your telephone utility bill that you pay to the telephone service provider. Where as in the case of VoIP you can talk as much as you want and the only bill you have to pay is the regular internet bill which any way you have to pay to the internet service provider.

On a regular telephone line you can only talk to one person at a time but in case of VoIP you can talk with as many people - who are connected to the internet - at any given time as you want. And this is only at the costs of your internet bill.

And since you are already connected to the internet you can as well exchange data or audio / video with any one at the same time as you talk, which is impossible with the regular telephone line.

Even though basic IP telephony and facsimile are the initial applications for VoIP, the longer term benefits are expected to be derived from multimedia and multi-service applications. For example, Internet commerce solutions can combine WWW access to information with a voice call button that allows immediate access to a call center agent from the PC. Needless to say, voice is an integral part of conferencing systems that may also include shared screens, white boarding, etc. Combining voice and data features into new applications will provide the greatest returns over the longer term. Videoconferencing also can be greatly enhanced.

Thousands of consumers are collectively saving millions of dollars by replacing or supplementing their traditional telephone lines with VoIP. Widespread adoption of broadband Internet service (cable or DSL) in the last few years though has in turn fueled a surge in the growth of much-improved personal VoIP. To get started, you need an analog telephone adapter (ATA) to convert your voice into data packets. In most cases, all you have to do is connect the ATA to your broadband modem and a conventional phone, and you're ready to start making calls to any phone in the world.

5.2.3 WORLD WIDE WEB (WWW)

The World Wide Web is a continuously expanding large collection of hypertext documents (called web pages) that often combine text, images and sounds. On WWW, you can find information on subjects from aardvark to zyzzyva. You can shop for cars, clothes, music, food specialty items, and more. You can tour a virtual museum and view images of paintings. You can get the latest news. You can find and download computer software programs. You can even listen to radio shows that originate in other parts of the world.

WWW is creating social change in the way people interact with each other. It is changing the way we get the information. It provides an information superhighway. It is platform independent and has search engine facility for finding desired information in seconds, multimedia capabilities, and GUI features.

5.2.3.1 Structure of WWW

The World Wide Web is the combination of four basic ideas:

- **Hypertext:** a format of information which allows, in a computer environment, one to

move from one part of a document to another or from one document to another through internal connections among these documents (called "hyperlinks");

- **Resource Identifiers:** unique identifiers used to locate a particular resource (computer file, document or other resource) on the network - this is commonly known as a URL or URI, although the two have subtle technical differences;
- **The Client-server model of computing:** a system in which client software or a client computer makes requests of server software or a server computer that provides the client with resources or services, such as data or files; and
- **Markup language:** characters or codes embedded in text which indicates structure, semantic meaning, or advice on presentation.

On the World Wide Web, a client program called a user agent retrieves information resources, such as Web pages and other computer files, from Web servers using their URLs. If the user agent is a kind of Web browser, it displays the resources on a user's computer. The user can then follow hyperlinks in each web page to other World Wide Web resources, whose location is embedded in the hyperlinks. It is also possible, for example by filling in and submitting web forms, to post information back to a Web server for it to save or process in some way. Web pages are often arranged in collections of related material called "Web sites." The act of following hyperlinks from one Web site to another is referred to as "browsing" or sometimes as "surfing" the Web.

Viewing a Web page or other resource on the World Wide Web normally begins either by typing the URL of the page into a Web browser, or by following a hypertext link to that page or resource. The first step, behind the scenes, is for the server-name part of the URL to be resolved into an IP address by the global, distributed Internet database known as the Domain name system or DNS. The browser then establishes a TCP connection with the server at that IP address.

The next step is for an HTTP request to be sent to the Web server, requesting the resource. In the case of a typical Web page, the HTML text is first requested and parsed by the browser, which then makes additional requests for graphics and any other files that form a part of the page in quick succession. This is the distinction between a single page view and the many hits or web requests that are often necessary to view the page.

The Web browser then renders the page as described by the HTML, CSS and other files received, incorporating the images and other resources as necessary. This produces the on-screen 'page' that the viewer sees.

Most Web pages will themselves contain hyperlinks to other relevant and informative pages and perhaps to downloads, source documents, definitions and other Web resources. Such a collection of useful, related resources, interconnected via hypertext links, is what has been dubbed a 'web' of information. Making it available on the Internet created the World Wide Web.

5.2.3.2 The Hypertext Document

A hypertext document contains information from multiple sources like image, voice, music, video, news, gopher, table, form, databases, indices, or even from another web page. A hypertext document contains various links (hyperlinks) defined by a URL address. Each hyperlink is an underlined text or different colour text. Images and icons are also used as hyperlinks. A mouse click on hyperlink readily leads us to another local or remote resource. Hyperlinks provide both sequential as well as nonlinear method to read a page or resource. We use a language HyperText Mark-up Language (HTML) to prepare the hypertext documents called static web pages.

Information contents of these pages do not change over time until the page is modified on web server. When HTML documents are embedded with programmable features using Scripts (e.g. JavaScript, VBScript), Servlets and COMs, the dynamic functionality imbibes. These dynamic web pages can interact with user, and can respond to user action. Sometimes more features are added to the web server hosting these web pages. Web server can generate customized web pages as per user's requirement, or user's action. These web pages are called Active web pages and these are usually generated on demand by some program residing at web server. These pages look differently for different user or on different point of time. Your mail box is one example of such active web pages where you see your own name, list of received mails, list of stored mail addresses in address book etc. Different user see different mail box and even same user see different list of received mails on different days.

5.2.3.3 Web Server

A web server is a server that provides web and Internet services. It is also called a host for the web sites it stores and Internet services it provides. The WWW is collection of such hosts connected by routers. Usually Internet Service Provider (ISP) acts as web server. A host may offer rent-paid services. You have to pay rent to host your web site on a host. Host provides some memory space for you web site for some duration according to contract. A large number of big and small organizations, universities, companies and government organizations and individuals posses their own web sites. Each web site is registered and assigned a domain name like "www.vmoukota.ac.in". Owner of the web site can continuously modify the contents of its web pages. A single web server can host many registered web sites and registered users. Some web servers offer free web hosting all over the world. They provide limited memory space (usually (5MB to 10MB) to host individual's web site.

5.2.4 INTERNET RELAY CHAT

Internet Relay Chat (IRC) is one of the most popular and most interactive services on the Internet. Sure, the Web is nice for finding info and E-mail beats snailmail hands down, but when you've been wondering 'where the others are?', then IRC is what you're looking for. Internet Relay Chat lets people all over the world participate in real-time conversations. IRC is where the Net comes alive!

Using an IRC client (program) you can exchange text messages interactively with other people all over the world. Some of the more popular chat clients are mIRC, Pirch, and Virc for Windows and Homer or Ircle for Mac's. What program you use doesn't really matter; all of them connect to the same chat networks. When logged into a chat session, you "converse" by typing messages that are instantly sent to other chat participants.

IRC is great fun and you'll sure meet lots of interesting people and find nice spots to hang out. But, IRC is not something that you should just jump into without first reading up on it. You could feel very lost if you do not know some basic commands before you enter IRC, and you might not even know how to get out of IRC after that.

5.2.4.1 Internet Relay Chat (IRC) Features

Direct point-to-point support: A Chat program can permit direct client-to-client (DCC) support without using the IRC servers. Both communicate directly on-line through the e-mail address.

Address book: A Chat address list helps you in selecting whom to join in the channel.

Yellow pages: These are important addresses in a list in the Chat program. Chat sites can be quickly searched to locate a group of interest.

URL support: Web pages can be attached as clickable URLs in a conversation. Corresponding hypertext document can be opened by clicking on the links.

Chat schedule: This helps to switch to the web browser and connect to a scheduled page for a Chat. A third party plug-in may be needed by the web browser.

Multi Frames or Split Screens support: There can be different frames for conversation between different participants. This gives ease of reading and images can also scale into the frames.

Channel filtering: This allows us to conduct a search using keywords. The channels that match can filter in. Criteria for filtering can be defined using the logical terms AND, OR, and NOT.

Aliases or Nicknaming: We may store the abbreviations of the standard replies or names of the participants. An alias or nickname can automatically be expanded to the full standard reply or name.

Macros, New Buttons and Hot Keys support: These features save our time on Internet. We can define macro for a reply. We can convey an emotion, say laughing by the macro. For example the heart <3.::::, smile:::: for a scene in a drama or play. We can also define hot key or a combination of keys instead of a macro. For example, define F4 key as hot key for laughing and F5 key for sad expression.

Multi session support: There can be multiple sessions of conversations between multiple participants. We may switch between various sessions.

Coloured and Styled Text support: This is a support for sending text in different colours and style.

User Identity support: A personal biography of participants can be stored on Chat server for finding the real name, e-mail address, phone numbers and address of a Chat channel members.

Event handlers: It is a utility to convey the joining and quitting of a member.

Drag and Drop: We can drag an object or image from a file into the conversation during the chat.

Quote support: It permits users to paste or append quotations from an object to make the conversation lively.

Sound support: Some Chat programs may have sounds or voice to make conversation lively.

Check Your Progress 2

1. What is ATA (Analog Telephone adapter)?
2. List the technical barriers for Internet Telephony.
3. List the advantages of Internet Telephony.
4. Define the terms Web page, Web site, Web server, URL and home page.
5. What is the purpose of HTTP?
6. What is meant by a hyperlink? How is it useful?

5.2.5 NEWS GROUPS

Newsgroup is just like a notice board or bulletin board where news is put up. Consider example of a college having a notice board. Teachers put news of seminars and other activities on the board. The board is the bulletin board of the college. Similarly, there can be an electronic bulletin

board of a group. A subscriber to a group could be living anywhere in the world and he can get news from electronic board or he can post news on bulletin board. A Newsgroup is similar to a bulletin board on Internet where anyone can drop in to listen, ask a question, disagree with a claim, or offer advice. Some people drop by for just a minute, while others are active daily for months or years. Some Newsgroups attract serious people who share technical information and help each other solving perplexing problems. Some exist purely for entertainment. And others are national bulletin boards of wantads. There are moderated Newsgroups, which are run by moderators who approve information before it can be posted, and there are unmoderated Newsgroups, which allow any message to be posted. Some Newsgroups are available to users all over the world, while others are restricted to a particular region. The Usenet is a service for accessing a globally distributed bulletin board. Usenet is the name of the Internet service that provides a means for access by a particular Newsgroup of specific information of different kind.

Some examples of Newsgroup are

(i) A group of students from a university. They graduated and then joined various organizations. Each one engaged in different profession. They can be kept in touch using Newsgroup where they can share news of marriage, job changeover, new e-mail addresses, new achievements, etc.

(ii) A business group who would like to announce a new product for distributors and users of that product using a Newsgroup.

(iii) A hobby group on roses who would like to post news of a new variety genetically engineered by a member and which is in full bloom.

Newsgroup are really discussion groups, organized within a large hierarchy and distributed by special news servers dedicated to Usenet communications. Each message that appears on a Usenet newsgroup is called an article, and each article contains a header just like an e-mail header. To read and post Usenet articles, you need to access to a Usenet news server (ISP services normally include Usenet access) and a special piece of client software called a news reader. Many browsers include their own news readers, so if you run Navigator or Internet explorer, you can use their news readers to get started.

The Usenet newsgroups are organized hierarchically, with a small number of names that are used to identify broad categories at the highest level. Newsgroup names start with the broad categories on the left and move down through successive subcategories from left to right. There are 103 top-level Usenet categories, but most of the traffic occurs in the "Big Eight:"

biz	Business-related topics
comp	Computer-related topics
sci	Scientific topics
misc	Miscellaneous topics
soc	Social issues and topics
talk	Debates and lengthy conversations
news	News and topical subjects
rec	Hobbies and recreational topics

plus another major newsgroup category, alt, an alternative topic hierarchy.

Newsgroup names are self-explanatory and usually tell you what a newsgroup is about. Some examples of newsgroup are:

sci.optics

sci.techniques.mag-resonance

comp.infosystems.www.browsers.misc

misc.health.alternative.diabetes

The Usenet newsgroups are constantly evolving. New group emerges when enough interest in a topic materializes. Old groups can die if interest in them wanes. Newsgroup creation is subject to many bureaucratic requirements. The process requires submitting a "Request For Discussion" (RFD) and a "Call For Votes" (CFV). Votes are collected via e-mails according to a strict voting procedure. If the newsgroup vote passes, then there is a waiting period before the newsgroup is finally created.

Usenet articles are continuously cycled through each news server. The oldest articles are deleted to make room for new articles. The lifecycle of an article depends on your particular news server. If space is tight on that server, article will be recycled quickly, within two or three days. On a server with more memory, articles may linger for a week or two. Most news servers carry a subset of the available newsgroups because of limited available space. Usenet communications rely on a text based protocol, NNTP (Network News Transport Protocol), which does not accept binary files. However, on some newsgroups user can post graphics files or executable programs.

5.2.6 FILE TRANSFER

FTP or **file transfer protocol** is used to connect two computers over the Internet so that the user of one computer can transfer files and perform file commands on the other computer.

Specifically, FTP is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol (such as the Internet or an intranet). There are two computers involved in an FTP transfer: a server and a client. The **FTP server**, running FTP server software, listens on the network for connection requests from other computers. The client computer, running FTP client software, initiates a connection to the server. Once connected, the client can do a number of file manipulation operations such as uploading files to the server, download files from the server, rename or delete files on the server and so on. Any software company or individual programmer is able to create FTP server or client software because the protocol is an open standard. Virtually every computer platform supports the FTP protocol. This allows any computer connected to a TCP/IP based network to manipulate files on another computer on that network regardless of which operating systems are involved (if the computers permit FTP access). There are many existing FTP client and server programs.

FTP runs exclusively over TCP. FTP servers by default listen on port 21 for incoming connections from FTP clients. A connection to this port from the FTP Client forms the control stream on which commands are passed to the FTP server from the FTP client and on occasion from the FTP server to the FTP client. For the actual file transfer to take place, a different connection is required which is called the data stream. Depending on the transfer mode, the process of setting up the data stream is different.

In active mode, the FTP client opens a random port (> 1023), sends the FTP server the random port number on which it is listening over the control stream and waits for a connection from the FTP server. When the FTP server initiates the data connection to the FTP client it binds the source port to port 20 on the FTP server.

In passive mode, the FTP Server opens a random port (> 1023), sends the FTP client the port on which it is listening over the control stream and waits for a connection from the FTP client. In this case the FTP client binds the source port of the connection to a random port greater than 1023.

While data is being transferred via the data stream, the control stream sits idle. This can cause problems with large data transfers through firewalls which time out sessions after lengthy periods of idleness. While the file may well be successfully transferred, the control session can be disconnected by the firewall, causing an error to be generated.

When FTP is used in a UNIX environment, there is an often-ignored but valuable command, "reget" (meaning "get again") that will cause an interrupted "get" command to be continued, hopefully to completion, after a communications interruption. The principle is obvious-the receiving station has a record of what it got, so it can spool through the file at the sending station and re-start at the right place for a seamless splice. The converse would be "reput" but is not available. Again, the principle is obvious: The sending station does not know how much of the file was actually received, so it would not know where to start.

The objectives of FTP are:

To promote sharing of files (computer programs and/or data).

To encourage indirect or implicit use of remote computers.

To shield a user from variations in file storage systems among different hosts.

To transfer data reliably and efficiently.

5.2.6.1 Criticisms of FTP

- Passwords and file contents are sent in clear text, which can be intercepted by eavesdroppers. There are protocol enhancements that circumvent this.
- Multiple TCP/IP connections are used, one for the control connection, and one for each download, upload, or directory listing. Firewall software needs additional logic to account for these connections.
- It is hard to filter active mode FTP traffic on the client side by using a firewall, since the client must open an arbitrary port in order to receive the connection. This problem is largely resolved by using passive mode FTP.
- It is possible to abuse the protocol's built-in proxy features to tell a server to send data to an arbitrary port of a third computer.
- FTP is a high latency protocol due to the number of commands needed to initiate a transfer.
- No integrity check on the receiver side. If transfer is interrupted the receiver has no way to know if the received file is complete or not. It is necessary to manage this externally for example with MD5 sums or cyclic redundancy checking.
- No error detection. FTP relies on the underlying TCP layer for error control, which uses a weak checksum by modern standards.
- No date/timestamp attribute transfer. Uploaded files are given a new current timestamp, unlike other file transfer protocols such as SFTP, which allow attributes to be included. There is no way in the standard FTP protocol to set the time-last-modified (or time-created) datestamp that most modern file systems preserve. There is a draft of a proposed extension that adds new commands for this, but as of yet, most of the popular FTP servers do not support it.

5.2.6.2 Security problems

The original FTP specification is an inherently insecure method of transferring files because there is no method specified for transferring data in an encrypted fashion. This means that under most network configurations, user names, passwords, FTP commands and transferred files can be "sniffed" or viewed by anyone on the same network using a packet sniffer. This is a problem common to many Internet protocol specifications written prior to the creation of SSL such as HTTP, SMTP and Telnet. The common solution to this problem is to use either SFTP (SSH File Transfer Protocol), or FTPS (FTP over SSL), which adds SSL or TLS encryption to FTP as specified in RFC 4217.

5.2.6.3 Anonymous FTP

Many sites that run FTP servers enable so-called "anonymous ftp". Under this arrangement, users do not need an account on the server. The user name for anonymous access is typically 'anonymous' or 'ftp'. This account does not need a password. Although users are commonly asked to send their email addresses as their passwords for authentication, usually there is trivial or no verification, depending on the FTP server and its configuration. Internet Gopher has been suggested as an alternative to anonymous FTP, as well as Trivial File Transfer Protocol.

5.2.6.4 Data formats

While transferring data over the network, several data representations can be used. The two most common transfer modes are:

- ASCII mode
- Binary mode

The two types differ in the way they send the data. When a file is sent using an ASCII-type transfer, the individual letters, numbers, and characters are sent using their ASCII character codes. The receiving machine saves these in a text file in the appropriate format (for example, a Unix machine saves it in a Unix format, a Macintosh saves it in a Mac format). Hence if an ASCII transfer is used it can be assumed plain text is sent, which is stored by the receiving computer in its own format. Translating between text formats entails substituting the end of line and end of file characters used on the source platform with those on the destination platform, e.g. a Windows machine receiving a file from a Unix machine will replace the line feeds with carriage return-line feed pairs. ASCII transfer is also marginally faster, as the highest-order bit is dropped from each byte in the file.

Sending a file in binary mode is different. The sending machine sends each file bit for bit and as such the recipient stores the bit stream as it receives it. Any form of data that is not plain text will be corrupted if this mode is not used. By default, most FTP clients use ASCII mode. Some clients try to determine the required transfer-mode by inspecting the file's name or contents.

The FTP specifications also list the following transfer modes:

- EBCDIC mode
- Local mode

In practice, these additional transfer modes are rarely used. They are however still used by some legacy mainframe systems

5.2.7 REMOTE LOGIN AND TELNET

Remote login facility enables a user at a terminal or personal computer to log on to a remote computer and function as if directly connected to that computer. The network terminal protocol

(TELNET) was designed to provide remote login facility initially for simple scroll-based terminals. User starts a remote session by specifying a computer to connect to. From that time until user finishes the session, anything user types is sent to the other computer. In Windows operating system, you can start a remote session by executing "telnet 172.16.1.1" like command. Here 172.16.1.1 is IP address of remote computer. The remote system then asks the user to log in and give password. A TCP connection is established between user's computer and remote login server. It then passes keystrokes from the user's keyboard attached to the remote server. Remote server processes the input received from user and generates some response, which is carried back to the user's screen. When user logges off the other computer, the TELNET program exits, and user will find himself talking to his own computer.

Working of TELNET

The steps in Figure 2 shows how TELNET works. Details of these steps are as follows:

1. Commands and characters typed by the user are sent to the operating system on the common server computer. The operating system does not interpret the commands and character entered by the user.
2. Instead, the local operating system sends these commands and characters to a TELNET client program, which is located on the same local computer.
3. The TELNET client transforms the characters entered by the user to a universally agreed format known as Network Virtual Terminal (NVT) characters and sends them to the TCP/IP protocol stack of the server computer. TELNET was designed to work between any host and any terminal. NVT is an imaginary device, which is the commonality between the client and the server. The client operating system maps whatever terminal type the user is using to NVT. At the other end, the server operating system maps NVT onto whatever actual terminal type the server is using.
4. The commands or text in the NVT format then travel from the server computer to the TCP/IP stack of the server via the Internet infrastructure. Commands or text are first broken into TCP then IP packets, and are sent across the physical medium from the local client computer to the server.
5. At the server computer's end, the TCP/IP collects all the IP packets, verifies their correctness and completeness, and reconstructs the original command so that it can be handed over to that computer's operating system.
6. The operating system of the server computer hands over these commands or text to the TELNET server program, which is running on that remote computer, passively waiting for requests from TELNET client.
7. The TELNET server program on the remote server computer then transforms the commands or text from the NVT format to the format understood by the remote computer. However, the TELNET server cannot directly handover the commands or text to the operating system, because the operating system is designed so that it can accept characters only from a terminal driver, not from a TELNET server. To solve this problem, a software program known as pseudo-terminal driver is added, which pretends that the characters are coming from a terminal and not from a TELNET server. The TELNET server hands over the commands or text to this pseudo-terminal driver.

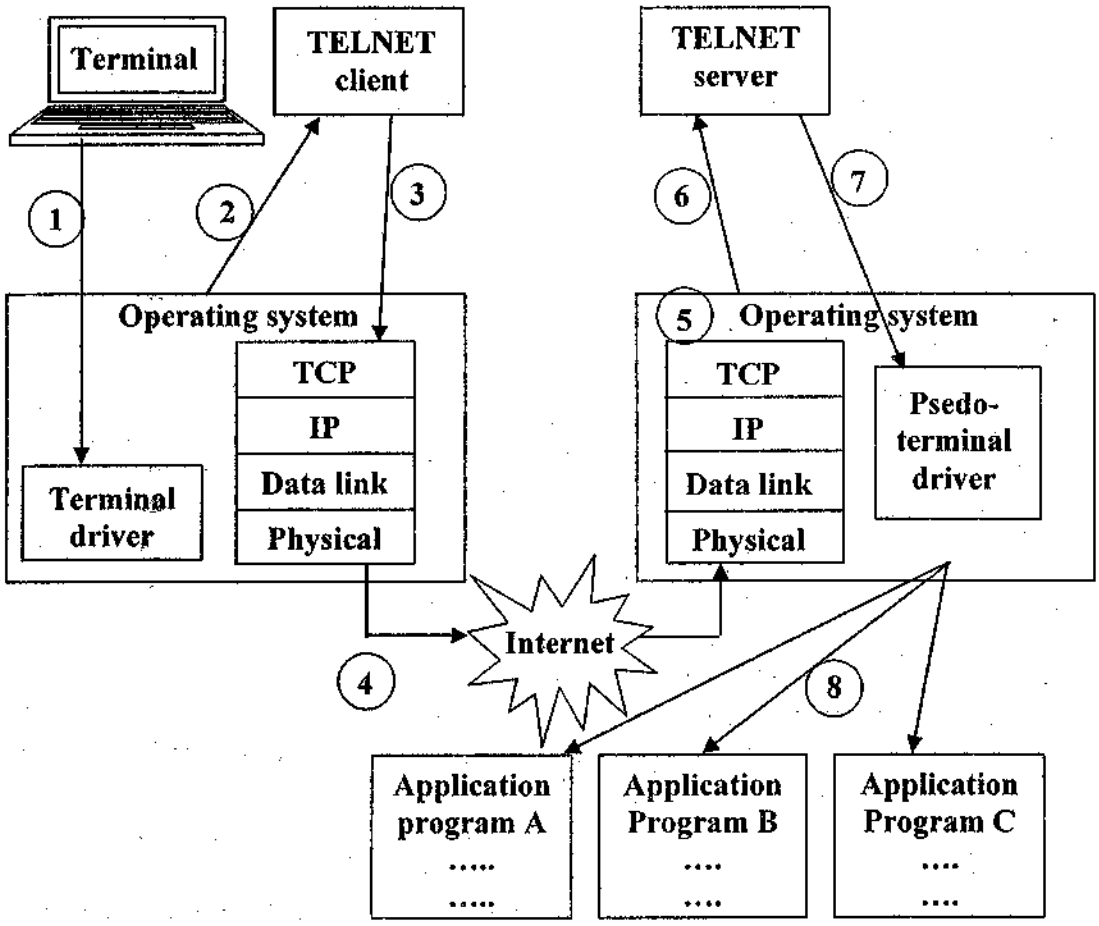


Figure: 2 Remote login using TELNET

8. The pseudo-terminal driver program then hands over the commands or text to the operating system of the remote computer, which then invokes the appropriate application program on the remote server.

Response generated by the server operating system finally travels back to the client terminal. The client using the terminal on the other side, can, thus access this remote computer as if it were a local server computer.

Technically, the TELNET server is quite complicated. It has to handle requests from many clients at the same time. These concurrent requests must be responded to in real time, as the users perceive TELNET as a real-time application. To handle this issue effectively, the TELNET server uses the principle of delegation. Whenever there is a new client request for a TELNET connection, the TELNET server creates a child process and lets that child process handle that client's TELNET connection. When the client wants to close down the TELNET connection, the child process terminates itself. TELNET uses only one TCP/IP connection. The server waits for TELNET client connection requests (made using TCP) at a well known port 23. The client opens a TELNET connection (made using TCP) from its side whenever the user requests for

one. The same TCP connection is used to transfer data and control characters. The control characters are embedded inside data characters. Each sequence of control characters are preceded by a special control character known as *Interpret As Control (IAC)*.

Check Your Progress 3

1. What us Usenet?
2. What are the objectives of FTP?
3. What do you understand by Anonymous FTP?
4. Explain why pseudo-terminal driver is used?

5.4 INTERNET HARDWARE

Hardware requirement for Internet depends upon the way of accessing Internet. Most popular Internet access method is using dial-up modem. Various devices for accessing the Internet are discussed in the next unit. These include dial-up modems, cable modem and DSL equipments. Some of the Internet hardware related to networking are already discussed in previous units. These devices include routers, bridges, gateways, switches, hubs and repeaters. Devices for video teleconferencing are discussed in next unit. Here are some guidance for dial-up medem selection and installation.

5.4.1 MODEM SELECTION

Selection of a dial-up modem is made on various features discussed next.

External vs. Internal

A modem can be either an external device or a card installed inside the machine. An external modem is a stand-alone unit connected to your computer with a serial cable. Another cable connects the modem to a telephone jack. You must also plug the modem into an electrical outlet. Internal modems are more likely to be found in portable computers. A cable from the back of the computer plugs directly into a telephone jack. Internal modems do have disadvantages. Moving the modem to a different machine is tedious. Resetting an internal modem usually requires rebooting the machine. Troubleshooting is more difficult and requires that you take the entire computer to the shop. An internal modem permanently occupies one serial port on your computer - you cannot easily remove it temporarily to plug some other device into that serial port.

Newer portables have PCMCIA slots that accommodate a credit card-sized modem. Easily inserted and removed, these have the convenience of internal modems for travelers, and the benefits of external modems for troubleshooting. Some machines have only one PCMCIA slot; if you wish to alternate between a modem and PCMCIA Ethernet device, you have to switch the two cards, buy an external modem, or buy a combination modem/Ethernet card. Laptop users may prefer the convenience of an internal modem.

External modems have a number advantages, some of these are:

- You can avoid the issue of serial port conflicts with an external modem.
- External modems usually contain lights which you the status of your connection. With an internal modem there is no visual verification that you are connected to a service or that data is being sent or received.
- External modems usually have easily adjustable speaker volumes.
- If your modem does not hang-up correctly you can simply turn it off. With an internal modem you may need (from time-to-time) to shut down your machine, turn off the power and then restart your machine to hang-up the modem.

- You do not need to open your machine to install the modem.
- You do not need to (possibly) configure jumpers on an external modem.
- We have seen a number of internal modems which claim to be the counterpart of an external model which actually lack certain essential features.
- Finally, you can always use an external modem (easily) on more than one machine and take it with you when you upgrade to a new computer.

Speed Ratings

Modems are rated by the speed, measured in bits per second (bps), at which data is transferred over a phone line. Common speeds are: 300, 1200, 2400, 9600, 14,400, and 28,800 bps. Some applications, such as email, may work at slower speeds. However, if you plan to use Telephone or any other Internet provider to access resources with a graphical interface, such as the World Wide Web, you will need a high-speed modem. It is recommended to buy a modem running at 14,400 bps or higher.

Modulation Protocols

For two devices to communicate, they must agree on a set of modulation protocols, or "rules of the road" by which the data will travel. The basic line speed supported by your modem depends on its compliance with modulation protocols. These include V.22, V.32 (9600 bps), V.32bis (14,400 bps), and V.34 (28,800 bps). Look for a statement saying that the modem supports V.32, V.32bis, or V.34. Buy a V.34 modem for speeds higher than 14,400 bps.

5.4.2 MODEM INSTALLATION

To install the modem hardware on your computer, refer to the manufacturer's documentation. Generally, the following instructions apply:

- If you have an internal modem with jumpers, set the jumpers for Plug and Play for Windows XP or, if that option is unavailable, for Windows 95, Windows 98, Windows NT, Windows 2000, or Windows Millennium Edition. See your modem documentation for information about setting the jumpers.
- Install an internal modem in an empty slot. Attach an external serial modem to an unused communication (COM) port.
- If you have an external modem, make sure that it is attached to the computer, plugged into the power source, and turned on before you turn on the computer and start Windows.
- Make sure that your modem is properly connected to the phone line and to your computer.

Most modems manufactured now are compatible with Plug and Play and installed automatically after they are connected to the computer. However, older modems and external serial modems may not be detected. If your modem is not installed automatically, use Phone and Modem Options in Control Panel to install it manually. To open Phone and Modem Options, click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Phone and Modem Options**.

To install a modem

You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.

Open **Phone and Modem Options** in Control Panel.

If you are prompted for location information, specify the dialing information for your location, and then click **OK**.

On the **Modems** tab, click **Add**.

Follow the instructions in the Install New Modem Wizard.

- To open Phone and Modem Options, click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Phone and Modem Options**.
- If the Install New Modem Wizard does not detect your modem, or you cannot find it listed, then follow instructions about installing an unsupported modem.
- If you are installing an external modem, and a cable is not provided, refer to the manufacturer's instructions for cable requirements. Most common cables will work, but some cables do not have all of the pins connected. Do not use the 9-to-25 pin converters that come with most mouse hardware, because some of them do not carry modem signals.

To install an unsupported modem

You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.

Open **Phone and Modem Options** in Control Panel.

If you are prompted for location information, specify the dialing information for your location, and then click **OK**.

On the **Modems** tab, click **Add**.

In the Install New Modem Wizard, select the **Don't detect my modem; I will select it from a list** check box, and then click **Next**.

Do one of the following:

If a modem is listed that is a good match for your modem: On the list of modems, click the manufacturer and model that is the best match for your modem, and then click **Next**.

If your modem is not listed, and you have an installation disk or **.inf** file provided by the manufacturer then Click **Have Disk** and specify the location of the disk or .inf file.

Follow the remaining instructions provided by the Install New Modem Wizard.

- To open Phone and Modem Options, click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Phone and Modem Options**.
- If possible, get the latest installation disk or modem **.inf file** designed for Windows XP from the manufacturer. This can usually be downloaded from the manufacturer's Web pages. If Windows XP installation files are unavailable, you can try using an installation disk or .inf file for Windows 95, Windows 98, Windows NT, Windows 2000, or Windows Millennium Edition. It may work correctly in Windows XP as well.
- If no installation file is available for the modem, the manufacturer's instructions that came with the modem may specify a compatible modem. Otherwise, click **(Standard Modem Types)** in **Manufacturers**, and try choosing the standard modem with the speed that matches your modem.
- If a cable is not provided with an external modem, refer to the manufacturer's instructions for cable requirements. Most, but not all, off-the-shelf cables will work. Some

cables do not have all the pins connected. Do not use the 9-to-25 pin converters that come with most mouse hardware, because some of them do not carry modem signals.

Check Your Progress 4

1. What type of modem you will select for your laptop?
2. Who are permitted to install a new modem in a system?
3. What are the common speeds of modems?

5.4 SUMMARY

This unit described the various tools available on the Internet and the various services provided by the Internet to the users. We talked about the most popular services e-mail and WWW. We explained how to send, receive, compose emails and features of mailbox. We also discussed protocols used for e-mail. In WWW section, we described concepts of web pages, hypertext, web sites, web servers etc. We also discussed various other services like newsgroup, chatting, File Transfer, and Remote login. In the last sections we intruduced Internet hardware and software along with dialup modem selection guide and installation guide.

5.5 SOLUTIONS/ANSWERS

Check Your Progress 1

1. Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP).
2. Header and Body.
3. MUA: Composing, reading, replying, forwarding and handling message boxes.
   MTA: To send and receive emails on Internet.
4. Spamming is unsolicited commercial e-mails received in your mailbox.
5. POP is responsible for retrieving e-mails from mailbox. When someone sends an e-mail, it is stored in mailbox of receiver. When receiver connects to the Internet and wants to see the new emails arrived for him, he opens his email client program, which in turn invokes the POP client. POP client contacts the POP server, which opens the mailbox for user and sends the emails arrived for him to the POP client running at user's computer.

Check Your Progress 2

1. ATA is a device used to connect a standard telephone device to your computer for use with Internet Telephony. It takes the analog signals from telephone and converts it to digital data ready for transmission over the Internet. Special software makes this possible and easy to use.
2. Technical barriers:
   Loss of packets,
   Level of reliability and sound quality on Internet,
   Delays in packet transmission due to limited bandwidth,
3. Advantages of Internet Telephony:
   It is cheaper because you have to pay Internet charges only,
   Teleconferencing is possible and cheap,
   Exchange data or audio / video with any one at the same time as you talk,
4. Web page: A Web page refers to a document on the Web. Web page can be used to display written text, show pictures, play music/sound effects and run video.
   Web site: Collection of interlinked Web pages containing information about an organization.

Web server: A computer or computer network which hosts Web sites which can be accessed through Internet. It usually runs a program which accepts requests for web pages from different clients according to a protocol HTTP. The server processes these requests and sends the requested web pages back to clients.

URL: unique identifiers used to locate a particular resource (computer file, document or other resource) on the network known as a URL It contains domain name followed by path and file name of the document.

Home page: This is usually first page of any web site.

5. It is a protocol used on Internet for exchange of information. Web server and client machines communicate using this protocol. Clients send requests to web server which runs a program which accepts requests for web pages from different clients according to HTTP. The server processes these requests and sends the requested web pages back to clients.
6. Hyperlink is a highlighted portion of a web page which allows you to navigate from one web page to another on the same computer or on different computers.

Check Your Progress 3

1. Usenet is the name of the Internet service that provides a means for access by a particular Newsgroup of specific information of different kind.
2. The objectives of FTP are:
   To promote sharing of files (computer programs and/or data).
   To encourage indirect or implicit use of remote computers.
   To shield a user from variations in file storage systems among different hosts.
   To transfer data reliably and efficiently.
3. In Anonymous FTP, users do not need an account on the server. The user name for anonymous access is typically 'anonymous' or 'ftp'. This account does not need a password. Although users are commonly asked to send their email addresses as their passwords for authentication, usually there is trivial or no verification, depending on the FTP server and its configuration.
4. The TELNET server program on the remote server computer transforms the commands or text from the NVT format to the format understood by the remote computer. However, the TELNET server cannot directly handover the commands or text to the operating system, because the operating system is designed so that it can accept characters only from a terminal driver, not from a TELNET server. To solve this problem, a software program known as pseudo-terminal driver is added, which pretends that the characters are coming from a terminal and not from a TELNET server. The TELNET server hands over the commands or text to this pseudo-terminal driver.

Check Your Progress 4

1. Internal modem.
2. An administrator or a member of the Administrators group is having permission to install a new modem.
3. Common speeds are: 300, 1200, 2400, 9600, 14,400, and 28,800 bps.

5.6 Unit end questions

1. What is FTP?
2. How will you differentiate between Web address and E-mail address?
3. Explain the features of IRC.

UNIT - VI

INTERNET CONNECTIVITY

STRUCTURE OF THE UNIT

6.0 Objectives
6.1 Introduction
6.2 Internet Browsers
6.2.1 Lynx
6.2.2 Netscape Navigator
6.2.3 Internet Explorer
6.2.4 Opera
6.2.5 Mozilla
6.3 Internet Connections
6.3.1 Dial-up Connection
6.3.2 Leased Line
6.3.3 ISDN
6.3.4 Cable Modem
6.3.5 Asymmetric Digital Subscriber Lines (ADSL)
6.4 Voice Mail
6.5 Video Conferencing
6.6 Internet Privacy
6.6.1 Cookies
6.7 Internet security
6.7.1 Antivirus
6.7.2 Firewalls
6.7.2.1 Packet Filters
6.7.2.2 Higher Layer Inspection Firewalls
6.7.2.3 Proxy Servers
6.8 Summary
6.9 Solutions/Answers
6.10 Unit end questions

6.0 OBJECTIVES

This section introduces various popular Internet browsers like Lynx, Netscape Navigator, Internet Explorer, Opera and Mozilla. Some of the common features required in browsers are discussed first. Various types of Internet access methods are available like dial-up, leased line, ISDN, cable, DSL etc. Each one is discussed here. Voicemail and videoconferencing are two major applications of Internet which require special hardware and high speed Internet connection. Some aspects of Internet privacy and concept of cookies are also described in this section. Internet security features like anti virus and firewalls are also covered at end.

6.1 INTRODUCTION

Most popular application running on the Internet is the World Wide Web (WWW). It is an application like email and File Transfer. WWW is all about accessing web sites which are collection of web pages digitally stored on web servers. Users run special software called web browser for accessing these web sites. A web browser acts as the client in the WWW interaction. Using this program, a user requests for a web page stored on a web server. The web server locates this page and sends it back to the client computer. The web browser then interprets the web page written in the HTML language/format and then displays it on the client computer.

Internet can be accessed in a number of ways. Initially the only way to access the Internet was by obtaining a telephone connection, and then purchasing an account with an Internet Service Provider (ISP). The telephone company would carry the data between the user's premises and the ISP's office. Now the ways of connecting to the ISP from a user's premises have changed dramatically. Technological progress has meant that now there are many ways in which one can connect to the ISP for different needs. Leased line, ISDN, cable and Digital Subscriber Line (DSL) provide Internet connectivity at various speed and cost.

Voicemail is an interesting Internet application. It is centralized system of managing telephone messages for a large group of people. In its simplest form it mimics the functions of an answering machine, uses a standard telephone handset for the user interface, and uses a centralized, computerized system rather than equipment at the individual telephone.

A videoconference is a set of interactive telecommunication technologies which allow two or more locations to interact via two-way video and audio transmissions simultaneously.

Internet privacy consists of privacy over the media of the Internet: the ability to control what information one reveals about oneself over the Internet, and to control who can access that information. Internet privacy forms a subset of computer privacy. Experts in the field of Internet privacy have a consensus that Internet privacy does not really exist. Privacy advocates believe that it should exist.

Internet security is the practice of protecting and preserving private resources and information on the Internet. Together, network security and a well-implemented security policy can provide a highly secure solution. Employees can then confidently use secure data transmission channels and reduce or eliminate less secure methods, such as photocopying proprietary information, sending purchase orders and other sensitive financial information by fax, and placing orders by phone.

A computer virus is probably the best known and most dangerous threat to computer security. Just like an organic virus, a computer virus attaches itself to healthy computer programs (body cells). A computer virus is a piece of code someone inserts into an otherwise legitimate computer program for the purpose of causing mischief. Viruses are also designed to spread from one machine to another through shared files.

The only way to know if a virus is present on your computer is with special software designed to detect viruses hiding in your file. These software also provide remedy from these viruses, and called antivirus software. A good antivirus software will look for thousands of viruses, and periodically software updates are released to keep up with new viruses. The best way to protect yourself against viruses is to buy a good anti-virus software package.

A firewall is a mechanism for protecting a local network from external, untrusted networks. Like the physical firewall used in some buildings to limit the spread of fire, a network firewall protects user's site from purposeful and inadvertent attacks from the outside. The firewall is placed as an interface between the server or network and the Internet or other external systems. Firewall can exist between different intra-networks to prevent security breaches from internal sources.

6.2 INTERNET BROWSERS

A browser is a computer program that resides on your computer enabling you to use the computer to view WWW documents and access the Internet, taking advantage of text formatting, hypertext links, images, sounds, motion, blogs, and other features. Firefox and Internet Explorer are currently the leading "graphical browsers" in the world (meaning they facilitate the viewing of graphics such as images and video and more). There are other browsers (e.g., Mozilla, Safari, Opera). Most offer many of the same features and can be successfully used to retrieve documents and activate many kinds of programs.

Browsers all rely on "plug-ins" to handle the fancier files you find on the Web. Plug-ins are subprograms stored within a browser or elsewhere in your computer especially to support special types of files you may click on. If you click on a link, and your computer does not currently have the plug-in needed for the file you clicked on, you are usually prompted with an opportunity to get the plug-in. Most plug-ins are free, and easy and safe to install on your computer.

The main way in which browsers differ is in the convenience features they offer for navigating and managing the Web and all the URLs you may want to keep track of. Netscape and Internet Explorer both offer the ability to e-mail documents, download them to diskette, print them, and keep track of where you've been and sites you want to "bookmark" or "Add to Favorites".

A browser typically performs following tasks.

1. **Navigates and shows** pages on browser's window. Navigation is done by a click on a URL, making available a hypertext link; the user can jump from that link to another, later from that to another and so on. A hypertext document can be anywhere on the internet. A URL consists of text, image, audio and video. The navigation browser also has multimedia capabilities. A home page is the first page that is opened when we open a URL.
2. **Saves bookmarks:** A book page-marker helps us to start reading from the last marked place. Similarly, if at a certain link, the user intends to revert later in the place of a home page, the browser provides for saving it as a bookmark.
3. **Saves history:** When user navigates through one link to another, the sequence of navigation is called the history. We can return to the previous link by a click on the 'Back' button and move forward by a click on the 'forward' button.
4. **Shows all hypertext links** (embedded links for obtaining additional contents) in a page by a different colour or underlined text.
5. **Create hypertext documents:** A HTML editing and authoring tool, if embedded within a browser, enables to create hypertext documents.
6. **Provisions for execution of Java Applets:** A browser, if Java enabled, executes a Java Applet. An Applet is an application program which uses another applications, the GUI (Graphical User Interface).
7. **Embeds (supports) the ActiveX controls:** A browser, if it supports ActiveX control can give the user access to the sound, animation and three-dimensional graphics features in hypertext documents. Microsoft MS OFFICE files can be directly viewed from the browser without first having to save the file and then open it using MS Word, MS Excel or MS PowerPoint.

8. **Embeds plug-ins for interpreting multimedia files** by using files of various formats, renders multimedia features, image, audio and video recordings. Shockwave animations, 3D images, compressed graphics, Acrobat files, multiple and multilingual fonts are currently available.
9. **Provides a front-end tool** for various application developments. With incorporation of features of file management and network management, the intranets too use the browsers. Recently, with the addition of these features, browsers of present days are moving almost towards providing a new operating system on their own.

Features of some of the popular browser are discussed next.

6.2.1 LYNX

Lynx is a fully-featured World Wide Web (WWW) browser for users running cursor-addressable, character-cell display devices (e.g., vt100 terminals, vt100 emulators running on PCs or Macs, or any other character-cell display). It will display Hypertext Markup Language (HTML) documents containing links to files on the local system, as well as files on remote systems running http, gopher, ftp, or finger and services accessible via logins to telnet, or rlogin accounts. Lynx is a World Wide Web browser that only displays text and therefore runs a lot faster than browser such as Microsoft's Internet Explorer. Version Lynx 2.8.3 runs on Unix, VMS, Windows 95/98/NT but not 3.1 or 3.11, on DOS (386 or higher) and OS/2 EMX.

How Lynx Works

Lynx allows you to perform two of the most basic navigational tasks: read documents and follow links to other documents. When reading a document, hit the space bar when you want to go to the next screen, and press either the 'b' key or the '-' (minus/hyphen) key when you want to go back to the previous screen.

Links are pointers which can take you to other documents, or to another section of an individual document, such as the explanatory notes in the body of a large document. At the top of this document there is a table of contents which serves two purposes: first, it informs you what information this document contains, and second, it provides you with the ability to jump directly to the section which interests you the most. Embedded in this sentence is another example of a jump-to link, which will take you back to the top of the page. Some documents are merely a list of links.

Whenever you choose a link, Lynx moves to a different document, or a different place in the same document. Even if the document is on a computer on the other side of the globe, Lynx will retrieve it automatically and almost instantaneously—depending, of course, on the time of day and the number of other people who are trying to access the document you selected. No matter where you are, the peak time for internet activity on the extends from approximately noon to midnight.

Moving to and Choosing Links

If you don't have Lynx set to display a bracketed number to the left of each link, you should—especially if you're using a speech-synthesizer. To set Lynx to display numbered links:

-Press 'o' to load the "Lynx Options Menu".

-Press 'k' to activate the "Keypad as Arrows or numbered links" text-entry field.

-Press any key to change the value of the option from "numbers act as arrows" to "links are
numbered"

-Press the enter key or hit the carriage return.

-Type a '>' (greater-than sign) to save this setting in the .lynxrc file, so that every time you

load

Lynx, a bracketed number will appear to the immediate left of a link, alerting you to its presence.

To choose a link, simply type the corresponding number, and then hit either enter or press the carriage return key.

You can also navigate from link to link by using the arrow keys on the keyboard. The up and down arrows move to the next and to the previous link, respectively. The current link (that is, the link to which you would be taken if you pressed enter) will be displayed on the terminal in an easily distinguishable manner—usually in reverse video, although the actual appearance of the highlighted link depends on the type of terminal you're using. Once you've reached the link you want to go to, press enter (or hit the carriage return) to choose that link.

Online Help

Lynx has two built-in help features. If you type 'h' or '?', Lynx will generate a menu, which lists a number of help files as well as the lynx Lynx Help Menu.

The second help feature is a list of keystroke commands, which you can view by pressing 'k'. Try it, and remember to press either 'u' or the left-arrow key to return to this page.

A Short Summary of Some Simple Lynx Commands:

- Use the spacebar to move forward through a document page by page, and use 'b' or '-' (the minus key) to go back a page.
- There are two ways to follow a link:

  - If the link is preceded by a bracketed number, simply type the number, and then press either the carriage return or enter.

  - Move to the desired link with the up-arrow or down-arrow keys. When the link you want to follow is highlight (displayed in reverse video) press either the carriage return key or enter.
- Once you've followed a link, you can always return to the document you just left by pressing either the 'u' key or the left-arrow key.
- You can search for a specified text-string in a document by pressing '/' (the forward slash). To find the next occurrence of the text-string, press 'n'.
- Whenever you load a searchable index, Lynx will prompt you to press either an upper or lower case 's'. If you want to perform a case-sensitive search, press shift-s; if you want to perform a case-insensitive search, simply press an 's', and Lynx will prompt you to "Enter a database query:" Type in the string for which you want to search, and then press enter to execute the search.
- If you want hard copy of the current document, press the 'p' key. Pressing 'p' generates the "Print Options Menu", which will present you with a choice of writing out a copy of the document to a file, sending it to yourself via email, or printing it. While email might seem like an odd choice, if you're on a terminal where you can't print out a copy of the document or can't save it as a file on your remote home directory, email might be the only way you can get a copy of the file. It's also a good way to send a copy of a document to a friend.

- Given the nature of hypertext and the web, it is often difficult to relocate a resource or a really cool site a couple of days after you first stumbled across it. To preserve a customized lists of your favorite links in "bookmark files" follow the following steps:
  - Press 'o' to load the "Lynx Options Menu"
  - Press 'b' to activate the "(B)ookmark file" text-entry field.
  - To change the name of the bookmark file from the default--lynx_bookmarks.html--hold down the control key and press the 'u' key, then type in a filename that corresponds to the type of links contained in the file (for example, news.html) will be easy for you to remember, and which ends with an .html extension
  - Press enter or the carriage return key to accept the value you set.
  - To exit the Lynx Options Menu press either 'r', which signals Lynx to use the file you just defined as the (B)ookmark file for the duration of the current session, or '>:' (greater-than), which instructs Lynx to use the file you just defined as the default (B)ookmark file.

Once you have defined your personal (B)ookmark file, typing the letter 'a' followed by 'd' (to save the currently displayed document), 'l' (to save the highlighted link), or 'c' to cancel the operation

- Note: choosing 'l' the is perfect way to save a link that sounds interesting, but to which Lynx was unable to connect.
- Press 'v' to view the bookmark file, and use the up and down arrows to move to a desired link.
- If, for any reason, the screen becomes garbled, hold down the control key and type 'w' or 'l' to refresh the screen. To reload the current page, hold down the control key and type 'r'.

6.2.2 NETSCAPE NAVIGATOR

Netscape Navigator was the most popular browser in the early to mid 1990's and lost it's crown to Internet Explorer in the mid to late 1990's. Netscape Navigator believed the reason for this was Microsoft giving away Internet Explorer with Windows. However Netscape Navigator still does an excellent job and doesn't integrate itself into the bowels of Windows like Internet Explorer.

Netscape main page has following bars from the top.

1. **Title Bar**: It is the top most bar displayed on screen. It displays the name of current application or document.
2. **Menu Bar:** Below the title bar is the menu bar which shows following buttons/options from left to right: File, Edit, View, Do, Communicator, and Help. On a click of mouse at each, a menu is displayed for selecting appropriate command.
3. **Navigation Tool Bar:** It is next to the menu bar. This bar contains several tool buttons. List of tools and their actions are listed below.

   Back - Displays the previous page in the history list. A history list references a hierarchy of pages you have already viewed. This tool lights up making it easy to navigate from one page to the previous page.

   Forward - Displays the next page in the history list. When you use **Back** or a history menu item to retrieve a page, using **Forward** gets the proceeding page. **Forward** is only available after you use **Back** or a history item.

Home - Displays the home page designated in the **General Preferences/Appearance** panel. The default for our school system computers is the CCPS home page location.

Reload - Redisplays the current Netscape page, reflecting any changes made prior to the original loading. Netscape checks the network server to see if any change to the page has occurred. If there's no change, the original page is retrieved from the cache. If there's a change, the updated page is retrieved from the network server.

Images - Loads images into pages. This is useful when the **Options|Auto Load Images** menu item is unchecked and icons have been substituted for images. By loading images, you replace the icons with the intended images.

Open - Lets you enter a URL to display the specified page in the content area.

Print - Prints the content area of the current Netscape page. A dialog box lets you select printing characteristics.

Find - Lets you specify a word or phrase to locate within the current Netscape page. You can specify case sensitivity and search direction. If a match is found, the text is selected and displayed.

Stop - Halts any ongoing transfer of page information.

4. **Address Bar:** It has a picture labeled 'address' on the left and a field for address (URL). This field shows address of current URL. On the right hand side there is a button 'Go'. If you enter a new address in address field, it can be executed using "Go' button. If arrow on the right side of address field is clicked, then the recently visited pages pop up from the history.
5. **Personal Tool Bar:** Using this tool, buttons can be created for various menus. The menus are for URLs of interest. This is done by dragging and dropping the URLs using mouse. Three menus which are already available are **Internet**, **New and Cool**, and **Lookup**.
6. **Status Bar:** Located at the bottom of the screen, this bar is used to show the status of mouse action. When content is being loaded, it shows the progress of loading. When loading is completed, it shows status 'done'.
7. **Page Viewing Window:** The latest downloaded web page is displayed in this area.
8. **Scroll Bars:** Horizontal and vertical scroll bars are provided for page viewing window for scrolling a larger web page.

Other features available in Netscape are:

Bookmarks

•Add Bookmark

Adds the title of the current Netscape page to the list of pages in the bookmark file. The Bookmarks menu grows as you add bookmarks. Initially, the menu contains two items: one that adds a bookmark item and another to view the Bookmarks window. Bookmarks are stored as a list and represented by a bookmark file on your hard disk. The bookmarks list can be viewed in the Bookmarks window.

•Bookmark *items*

The **Bookmarks** menu appends an item with the title of each page you add as a bookmark. Choose the menu item to display the page. Choose **Window/Bookmarks** to view the bookmark list.

Directory Buttons

Netscape's Directory buttons connect you to pages that are designed to help beginners take a tour of the Web. There are 2 Directory buttons in Netscape that you will use most frequently:

•Handbook

The Handbook button takes you to a full on-line handbook for Netscape. It contains all of the items that this tutorial covers plus many extra items that we don't cover here.

•Net Search

The Net Search button is a directory of Internet search engines that you can use to find specific information or a particular page, either by searching page titles, subject fields, document content, or other indexes and directories. Due to the fact that every search engine works differently, this tutorial will not attempt to go into depth on searching. For more information look for on-line help within each search engine.

6.2.3 INTERNET EXPLORER

Internet Explorer is a Web browser produced by the Microsoft Corporation.

The Toolbars

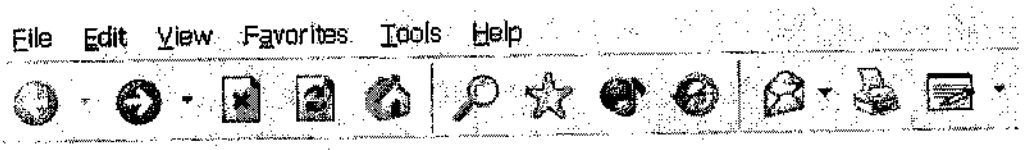


Figure 1: Internet Explorer toolbars

Internet Explorer has two toolbars at the top of the browser window:

Menu Bar: Contains menu items that open up dropdown lists for related options. Among the items are options for printing, customizing Internet Explorer, copying and pasting text, managing Favorites, and accessing Help.

Navigation Toolbar: Contains icons for a variety of features including navigating among Web pages, searching the Web using a selection of search tools, accessing and managing Favorites, viewing a History of visited pages, printing, and accessing email and newsgroups.

To go back to previous sites:

Click on the small **Back** left arrow on the navigation bar near the top left corner of your screen. Each time you click on this arrow, you will return to the next previous site that you visited. If you hold your mouse over the **Back** arrow, the title of the upcoming page will briefly appear.

To skip farther back, click on the small black triangle to the right of the word **Back**. This will bring up a list of pages you have visited. Click on any one of these choices to return to the desired page. This is the equivalent of clicking on the **Back** arrow several times.

To move forward:

When you have returned to previous sites with the **Back** arrow, you can go forward again by clicking on the small right-pointing arrow next to the **Back** arrow. If you hold your mouse over this arrow, the title of the upcoming page will briefly appear.

To move farther ahead, click on the small black triangle to the right of the Forward arrow in the menu bar at the top of the screen. This presents a list of several sites you have visited. Click on any of the choices to return to the desired site. This is the equivalent of clicking on the **Forward** arrow several times.

Additional Toolbar Options

Stop: The circle containing the X will stop a page while it is in the process of loading. This is useful if a page is not successfully or speedily retrieving.

Refresh: The square containing the two curved arrows re-retrieves the page you are currently viewing. This is useful if the page does not load successfully or completely.

Home: The home icon takes you back to the page that was on the screen when you first started IE 6. You can customize your selection.

Search: The search button opens up a function that uses one or more Web search tools. You can choose the search tool(s) you want as your default.

You can also customize your search experience. After clicking on **Search**, choose the **Customize** option and make your selection. A pop-up window called "Customize Search Settings" will appear. If you choose to "Use Search Assistant" broad search topics will be displayed and the appropriate search tool will be queried. You can also opt to have Internet Explorer remember your last 10 searches so that you can easily repeat them.

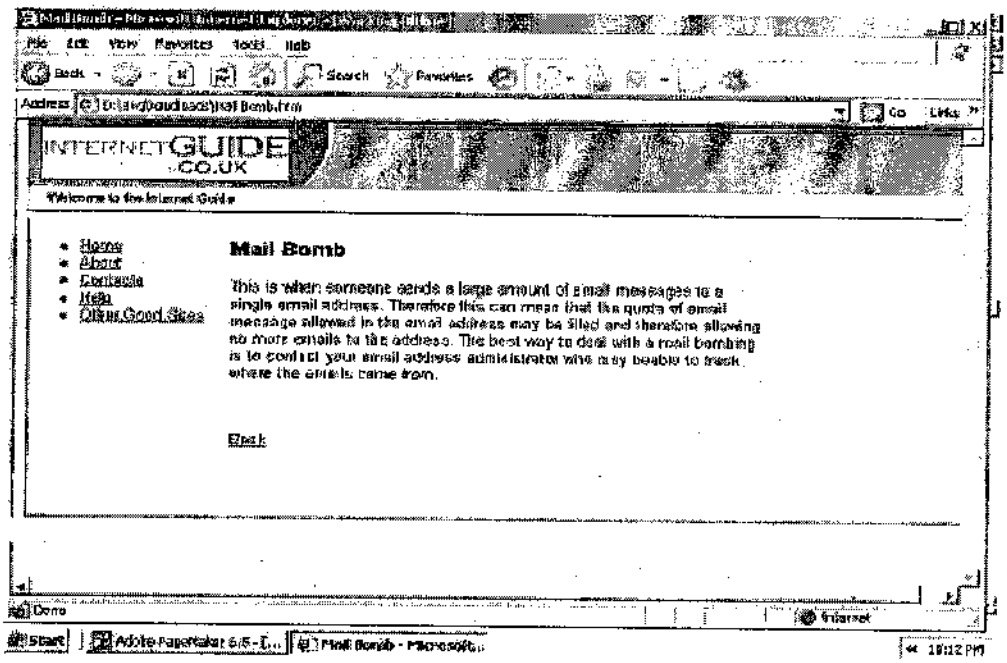


Figure 2: Internet Explorer snapshot

Also notice that you can click a button called "Autosearch settings." This allows you to choose the search tool you want when you use the Address bar as a search window. You can also customize this option on the "When searching" line. You can even choose to turn off the use of the Address bar as a search window. If you do this, all words you type into the Address bar will be interpreted as URLs.

Favorites: Favorites are Web sites you have visited that you would like to store for easy access. You can add, delete and organize your Favorites.

To *add* the current Web page as a favorite, click on **Favorites** and then **Add**. To choose the folder where you want to store this listing, click on **Create in** and choose the folder you want. At this point, you also have the option to create a new folder.

To *delete* a Favorite, simply right click on the item and choose **Delete**. Or, you can choose **Organize Favorites** select the desired item, and click on the **Delete** button.

To *move* a favorite to another folder, click on **Organize Favorites**, select the desired item, and click on **Move to folder**. In the pop-up window, select the folder where you would like to store this listing.

History: The history function allows you to view and select Web pages you have recently visited. You can sort your items by clicking on the black triangle to the right of the word View. You can sort by size, date, the number of times visited, and the order you have visited today.

Mail: You can read email from this window. Choose the email software you wish to use by going back to the Menu Bar and choosing Tools/Internet Options/Programs.

Print: Allows you to print the current page.

Edit: You may edit the current page in the HTML editor of your choice. Choose the editor by going back to the Menu Bar and choosing **Tools/Internet Options/Programs.**

Useful Options on the Menu Bar

The menu bar at the top of the screen includes some useful options. Here are a few highlights.

File/New/Window: You can open up a second copy of Internet Explorer by using this feature. This allows you to visit more than one Web page at a time.

File/Edit with...: You can edit the current Web page using the editor of your choice. Select the editor by going back to the Menu Bar and choosing **Tools/Internet Options/Programs**. You choices will be determined by software installed on your computer.

Edit/Find (on This Page): Internet Explorer allows you to do a text search of the document on your screen. Choose this option and type in the word or phrase you wish to search.

Tools/Show Related Links: Internet Explorer will display pages that are related in content to the current page. This is a service of Alexa, a Web content and traffic analysis company.

The **Tools** menu offers you many ways to customize Internet Explorer.

How to Download, Email, and Print

You can download to disk, email, or print the Web page on the Internet Explorer screen.

To DOWNLOAD

Click on **File/Save As** (top left of screen). A pop-up window will appear.

Save in: Choose the desired drive.

Save as type: Make sure you save the page to the file type that will be useful to you. If you save the page as a Web page, you will need a Web browser or HTML editor to view it. A text file (txt) can be viewed in a word processing program such a Word or WordPerfect.

Click on **Save.**

To EMAIL

Click on **File/Send** (top left of screen).

You may send the current page as an email message, or you may insert the link to the current page within an email message. Once you make your selection, your email software will open.

You can change the default software by going to the Menu Bar and choosing **Tools/Internet Options/Programs**. You choices will be determined by software installed on your computer.

To PRINT

To PRINT THE ENTIRE DOCUMENT

Click on the **Print** icon on the Tool Bar

Click on **OK**

Customizing Internet Explorer

Internet Explorer offers a number of customization options. This section will highlight some of the more useful features available under **Tools/Internet Options** on the Menu Bar.

Tools/Internet Options is divided into six tabs. Each one is explained below.

1. General

Home Page: Specify the URL of the page you want to appear whenever you open Internet Explorer, or whenever you click on the Home icon

Temporary Internet Files: This option allows you to view the files in your browser's cache. The cache holds viewed Web pages for subsequent quick viewing. Retrieving a file from the cache is much faster than repeated trips to the remote Web server where the file originated. You can customize the **Settings** to decide how often to check for newer pages, to specify how much disk space to reserve for your cache, and to view files in the cache.

History: This option customizes your access to pages you have visited with the **History** function. Here you can set the number of days to keep pages in your history.

Colors: Choose colors for links, visited links, and link hovers (the color appearing when your mouse is over a link). You can also set a default text and background color.

Fonts: Select the language script, the font displayed in Web pages, and the font displayed as plain text.

Languages: Select the language that will display Web pages accessed with Internet Explorer.

Accessibility: Choose to ignore colors, font sizes and font styles on Web pages. You can also set a style sheet as the display template for all Web pages viewed with Internet Explorer.

2. Security

Here you can set levels of security for individual Web pages. See Internet Explorer Help menus for more information.

3. Content

Content Advisor: You can enable ratings of objectionable content to control the pages that may be viewed with this browser.

Certificates: This feature allows you to manage the identification certificates you may have. See the Help menus for more information.

Personal Information: This consists of two options. **AutoComplete** will store entered Web address, information entered into forms, and usernames and passwords needed to access sites you have visited. When you are using your browser, previous entries will come up as choices so that you don't have to retype the information. This can make your work go much faster. You can customize these options, and delete your settings. **My**

Profile offers a template for entering personal information. If a Web site requests this information, you can give permission for it to be used.

4. Connections

Here you can store the information about your Internet Service Provider, configure your LAN settings, or send your browser requests through a proxy server.

5. Programs

Here you can set the programs you want the browser to use for HTML editing, email, Usenet news, collaboration ("Internet Call"), your calendar and contact list.

6. Advanced

This screen offers a number of options in the categories of accessibility, browsing, HTTP settings, Microsoft VM (Virtual Machine), multimedia access, printing, searching and security. Set these options if you are comfortable with them.

6.2.4 OPERA

Opera was designed to run on low-end and small computers, and with a commitment to computer accessibility for users who may have visual or mobility impairments.

- It is possible to control nearly every aspect of the browser using only the keyboard, and the default keyboard shortcuts can be modified to suit the user. Opera also supports the use of access keys to allow a computer user to immediately jump to a specific part of a web page via the keyboard. Opera was also one of the first browsers to support mouse gestures, allowing patterns of mouse movement to trigger browser actions, such as "back" or "refresh".
- Page zooming allows text, images and other content such as Macromedia Flash, Java and Scalable Vector Graphics to be increased or decreased in size (20% to 1000%) to help those with impaired vision. User stylesheets may also be used to do this and to enable high contrast coloured fonts.
- Voice control, co-developed with IBM, allows control of the browser without the use of a keyboard or mouse. It can also read aloud pages and marked text. IBM has a browser based on Opera.
- A "Fit to Window" feature that relies on technology similar to Opera Mini's Small Screen Rendering (SSR), allowing websites to fit within a smaller screen without the need for horizontal scrolling.

There are several new features in Opera. The most important ones are:

- Simple BitTorrent client, targeted towards novice users.
- Content blocker (also known as AdBlock).
- Thumbnail preview of tabs (when hovering mouse over them).
- Widgets - small standalone applications sitting on top of the browser.
- Site specific preferences (pop-up blocking, cookies, scripts, user style sheets, user java scripts, user-agent masking)
- The ability to create search engines from a textfield.
- Improved rich text editing (WYSIWYG editor)
- Redefined default hot keys to be more like Internet Explorer.
- Fraud-Protection (Introduced in Opera 9.1) is real-time security. Opera tests sites that you navigate to, against Phishtank database entries to see if they are "Verified" or "Fraud". This feature is disabled by default.

Users have the option of accessing common browsing functions with combinations of mouse movements. This option is similar to using keyboard shortcuts, as it saves time because users do not have to navigate to graphical buttons (thereby avoiding usability problems relating to Fitts' Law). Examples include:

- **Back** - Either pressing the left-mouse button while holding down the right button, or right-clicking anywhere and dragging the mouse towards the left.
- **Forward** - similar and opposite to the "back" gestures
- **New Tab** - holding down the right-click and dragging down.
- **Scroll Through Tabs** - scrolling with the mouse wheel while holding down the right-click (especially useful during sessions where many tabs are open within the same window)
- **Close Tab** - holding down the right-click and making an L-shape movement.

Panels Manager

The tools relating to browsing and email functions are organized within Opera Panels. Additionally, users may download additional tools or create their own.

- **Contacts** - serves as an email address book.
- **History** - provides a log of all pages accessed, in chronological order, starting with the most recent.
- **Links** - lists all links that the user has clicked on during navigation.
- **Notes** - allows the user to copy and paste content into a built-in text editor. As the name implies, this tool is aimed towards note-taking tasks.
- **Info** - displays page-specific information, including its MIME type, local cache, size, and encoding.
- **Windows** - provides a summary for all tabs and windows open during an Opera session.

Hotclick

Hotclick refers to double-clicking any word in a page. Hotclick can be enabled by going to Opera's Accessibility preferences. It was introduced in Opera version 6. It gives access to all search engines in Opera as defined by search.ini file, as well as giving access to the built-in translation, encyclopedia, and dictionary.

In addition to this, the Hotclick menu also gives access to the 'copy text', 'copy to note', and 'Send by email' functions. Using Hotclick is the fastest way to search for a word in Opera. Like all other menus, it can be customized by using a custom menu ini file.

Search facilities

Opera provides quick access to a variety of search engines and commerce sites, via the use of search plug-ins. Many search plug-ins are included with the browser, but they can also be user-defined or installed from an external sources. Opera also allows a user to translate a paragraph or look for meaning of a word directly by a right mouse click.

Since Opera 9, a user can have access to any Search Engine without opening the corresponding page. Right Click in a Search Field and then use the CREATE SEARCH option. The Search Engine will be listed in Opera in future. Previously this was only possible by editing search.ini file manually.

For example, Opera has a pre-set shortcut for using the Google search engine: "g." Therefore, if a user typed "g wikipedia" directly into the address bar, Opera performs a Google search for

Wikipedia. This feature has been available before the Mozilla Firefox browser introduced a similar tool in v. 2.0.

Download manager

Opera allows the user to list, pause, resume or restart the downloading of files. It also keeps history of recently downloaded files and allows opening them from within the browser. Since Opera 9 BitTorrent downloads can be handled just like regular HTTP/FTP downloads. Opera can also be used with external download managers.

6.2.5 MOZILLA

They are award-winning Mozilla web and e-mail applications developer. As leading innovators, they develop the next generation of web browsers, e-mail software, web page editors and more. Mozilla are the power behind the open source release of Netscape Communicator. Because it became open source Mozilla has since then been rewritten, including the layout engine, the networking library, and the front-end. Even though quite a lot of Mozilla code is still under Netscape Public License, it is none the less a growing community. One of the aims of the Mozilla foundation is to promote its goal of driving open standards on the Web.

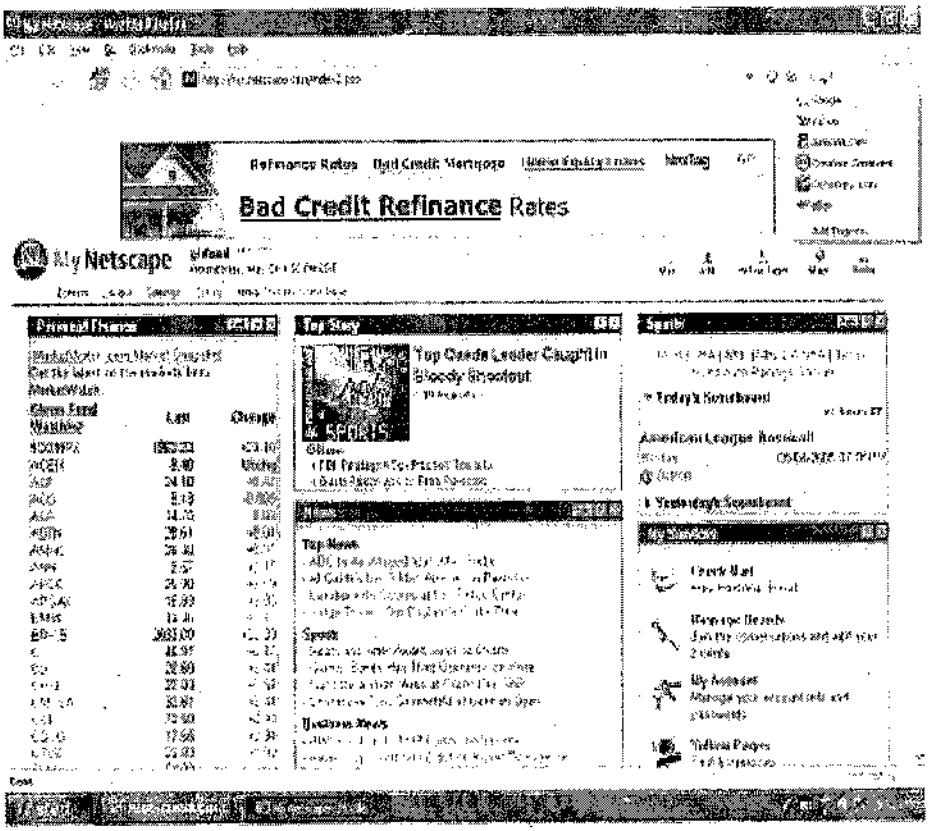


Figure 3: Snapshot of Mozilla Firefox browser.

Mozilla Features

History: Mozilla remembers what pages you have visited during a certain period of time, usually the last 10 days, but this can be changed as well. Mozilla also remembers what pages you

have visited during the current session. You can see a list of these pages by looking at the "Go" menu. The list of menu items in the bottom section of the menu are the titles of the pages that you have visited. The familiar "Back" and "Forward" buttons on the Mozilla toolbar move back and forward through this list. You can go directly to one of the pages on the list by selecting the corresponding menu item.

Also under the "Go" menu you can also select the "History" item to open a window that contains a list of all of the pages that you have visited lately. You can visit a page by double clicking on its name. Select "Close" under the "File" menu to close the history window.

Stop: If Mozilla is in the middle of loading a page and you want it to stop, you can click on the "Stop" button from the toolbar. You might want to do this if the page is taking too long to load.

External viewer: Mozilla can only display a few types of files: HTML files (.html), pictures (.gif and .jpg), and plain text. Yet any type of file can be retrieved over the Web, so Mozilla has a way of passing the files it doesn't understand to other programs. These other programs are called external viewers. Postscript files, MS Word files require external viewer. By default, when Mozilla doesn't know what program to run for a particular file, it asks you if you want to save the file to disk. For example when binary file, zip files are opened, Mozilla doesn't know what to do with it.

Bookmarks: Mozilla provides an easy way to return to a specific page besides remembering or writing down the URL. You can create a bookmark which will allow you to return to a page by selecting an item from a menu. For this you have to click at the "Bookmarks" menu. The first item, "Bookmark This Page", allows you to add bookmarks to your bookmarks list. To add a bookmark that points to the currently displayed page, just select "Bookmark This Page."

You can now return to this page at any time by selecting the "Bookmarks" menu item. You can try this out by moving to a different page (for example, by clicking the "Back" button), then selecting the menu item.

Mozilla also has some facilities for editing the bookmark list. This can be found as the "Edit Bookmarks..." option under the "Bookmarks" menu.

Selecting "Manage Bookmarks..." brings up another window. We won't get into the finer details of this window here, but its hierarchical format can be very useful if you have a large number of bookmarks that you want to manage. You can delete bookmarks, create folders, nest bookmarks inside folders, and drag bookmarks around at will. If you do this, the bookmarks menu itself will reflect the hierarchical organization of your bookmarks list.

Tabbed browsing: Mozilla provides a simple way to manage multiple browser windows. With Mozilla you can open links on a page in background "tabs" and then read them when you're ready. By default, if you have only one tab open the tab toolbar will not appear. Right-click on a link on your current page and select "Open Link in New Tab". The link is opened in a new window.

You can customize tabbed browsing to your personal taste. Simply select "Preferences.." from the "Edit" menu. Then click on the box next to the label "Navigator". Next click on "Tabbed Browsing". Experiment with different options to decide what you like the best.

Image loading controls: If you are using Mozilla over a slow modem link, it can take a long time to download images. If this the case, you can tell Mozilla not to download them automatically. To turn off automatic image loading, select "Preferences..." under the "Edit" menu. A new window will appear. Click on the box next to "Privacy and Security" and then click on the

section "Images". Click the button next to the label "Do not load any images". Then click on OK.

You can restore automatic image loading by returning to the window described above and clicking on the button that says "Accept all images" or if you wish to stop some ads and web bugs you can choose "Accept images that come from the originating server only".

If you wish to block images on a per-server basis you can simply click on the image with the right mouse button and select "Block Images from this Server" from the menu.

Popup blocking: Mozilla also allows you to block unrequested popup windows. These "popups" have become a problems for Internet users in recent years. To prevent these unpopular windows from appearing go to the "Edit" menu and select "Preferences". The click on "Privacy and Security" and then on the the section "Popup Windows". Select the box next to "Block unrequested popup windows". If you wish to allow popup again, simply uncheck this box. If you want to allow popup windows from a specific site you should go to the "Tools" menu, select "Popup Manager" followed by "Allow Popups From This Site".

Text zoom: Sometimes the text of a web page is too large or too small. To adjust the text to something more comfortable select the "View" menu, followed by the "Text Zoom" submenu. From this submenu select your preference for viewing this page.

Reload: If the information displayed by Mozilla needs to be redrawn for any reason, select the "Reload" option from the "View" menu. If the page that you are viewing uses Mozilla frames to divide the browser window (the page that you are looking at has the navigation bar in one frame and this text in another) the frame in which you have most recently clicked will be refreshed.

"Reload" refreshes the Mozilla display using information previously downloaded from the Web. Clicking on the "Reload" button and holding down the shift key, in contrast, will cause Mozilla to obtain a fresh copy of the page from the Web before redisplaying it. This can be useful if you interrupted the downloading of a page and now want to try again.

Page source: The "Page Source" option in the "View" menu will open a window that displays the HTML source of the current page. You will learn more about HTML files in a later lesson. "Page Info," the item immediately beneath "Page Source," brings up some specialized information about the HTML document currently being viewed.

Text Find: Select the "Find in This Page" option under the "Edit" menu. This will bring up a window that allows you to search the current frame for specific words. If you enter a word or phrase in the white box and then click on "Find", Mozilla will highlight the next occurrence of that word or phrase.

Page info dialog: Provides additional information about encoding, MIME type, referrer and meta tags. Some of this information is also available in IE's properties dialog although it isn't as detailed and the window isn't resizable.

Cookie Manager: The cookie manager lets you view the cookies that have been set, their values and their expiry times. Some people have mentioned that one can view Cookies by pressing a View Files button in the Options, but that just provides a list of all cached files. While the list does include cookies, hidden amongst the other files, it isn't tailored to cookies (it is just a generic file listing), so one cannot really view the data or expiry times easily.

The cookie manager lets you delete individual cookies without having to search around your file system. In IE's file view, it's tricky to distinguish cookies from similar domains, and all cookies from the same domain are stored in the same file.

Download Manager: The download manager provides a tabular view of all of the files that you have ever downloaded, allowing you to open them without having to search around on your file system. It provides progress indicators in the window as items download.

On the topic of downloading files, IE does not begin to download a file until you have selected where to save it to, while Mozilla begins as soon as the link is clicked, downloading in the background while you are selecting a place to save it. In Mozilla, one cause pause downloads. Some people may find this useful during long downloads.

Multiple pages as a home page: You can set a group as your home page, so multiple pages appear when you start Mozilla. To set this, open the pages you wish in tabs, and then choose Use Current Group in the Navigator preferences panel.

Check Your Progress 1

1. What are the browser action on a click at **Go**?
2. What are the browser action on a click at **Refresh**?
3. Explain the use of Back, Forward and History in a browser.
4. Describe the different bars in Netscape.

6.3 INTERNET CONNECTIONS

Internet can be accessed in a number of ways. Initially, the only way to access the Internet was through telephone line. User obtains a telephone connection, and purchases an account with some Internet Service provider (ISP). The telephone company would carry the data between the user's premises and the ISP's office. From this point onwards, the ISP would connect the user to the Internet.

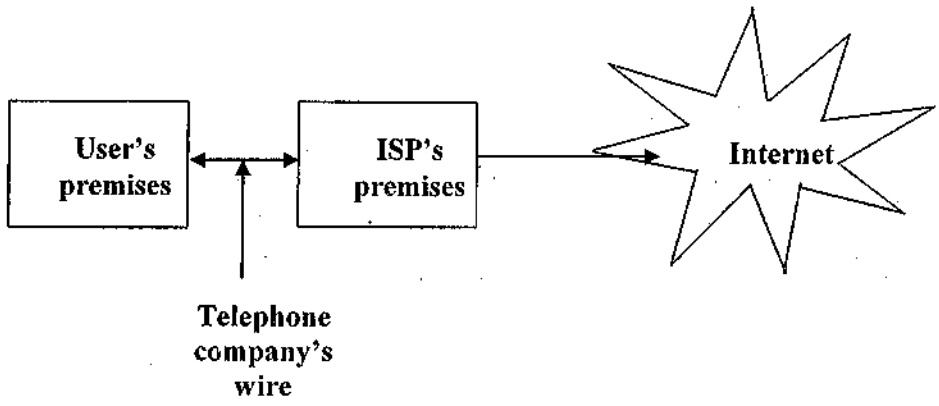


Figure 4: Basic Internet access method

6.3.1 DIAL-UP CONNECTION

Dial-up connections are the most common type of internet connection available from ISPs, they are also the slowest and (usually) the most inexpensive. A dial-up connection allows you to connect to the internet via a local server using a modem and a telephone line. Your PC literally dials a phone number (provided by your ISP) and connects to the server and therefore the internet.

Once connected you can utilize all aspects of the internet, the drawback with a dial-up connection is the speed, a standard 56k modem can theoretically transfer 56 Kilobits of data a second, this means that you can (again theoretically) transfer up to 7 Kilobytes a second (although to get a full 7k is near impossible due to the compression overhead).

When you consider the average web page including images is around 50 Kilobytes, this means it would take around 7 seconds for the web page to completely load in your browser. On top of this most (though not all) internet service providers charge by the minute for your connection, so the longer it takes to load the pages you visit, the more you pay for your connection. The cost is usually the same as you would pay for a local phone call so as long as they are used sensibly they can be a very cost effective internet connection.

Dial-up requires no additional infrastructure on top of the telephone network. As telephone points are available throughout the world, dial-up remains useful to travelers. Dial-up is usually the only choice available for most rural or remote areas where getting a broadband connection is impossible due to low population and demand. Sometimes dial-up access may also be an alternative to people who have limited budgets as it is offered for free by some, though broadband is now increasingly available at lower prices in India.

Dial-up requires time to establish a telephone connection (approximately several seconds, depending on the location) and perform handshaking before data transfers can take place. In locales with telephone connection charges, each connection incurs an incremental cost. If calls are time-charged, the duration of the connection incurs costs.

Dial-up access is a transient connection, because either the user or the ISP terminates the connection. Internet service providers will often set a limit on connection durations to prevent hogging of access, and will disconnect the user — requiring reconnection and the costs and delays associated with that.

Dial-up connections can be very economic and are widely available, the cost is *usually* the same as a local phone call or priced as a monthly plan. As these connections use a standard modem the hardware costs are minimal.

Dial-up connections are very slow compared to other connection types. When connected to the internet the same phone line cannot be used for phone calls so if anyone phones you when you are connected they will get the busy signal. Dial-up connections transfer data over an analog line so before the data is sent it has to be converted from digital to analog, likewise when data is received it has to be converted from analog to digital (this is what the modem does), this adds a performance overhead which affects the speed of the connection.

The Serial Line Internet Protocol (SLIP) or Point to Point Protocol (PPP) are two protocols which allow a user to dial into the Internet. They convert the normal telephone data stream into TCP/IP packets and send them to the network. With these, the user becomes a peer station on the Internet and has access to all the Internet's facilities.

Internet Service Provider (ISP) is an important component in the Internet system. Each ISP is a network of routers and communication links. The different ISPs provide a variety of different types of network access to the end system, including 56 Kbps dial-up modem access, residential broadband access such as cable modem or DSL, high-speed LAN access, and wireless access. ISPs also provide Internet access to content providers, connecting Web sites directly to the Internet. To allow communication among Internet users and to allow users to access world wide Internet content, these lower-tier ISPs are interconnected through national and international upper-tier ISPs. An upper-tier ISP consists of high speed routers interconnected with high-speed

fiber-optic links. Each ISP network, whether upper-tier or lower-tier, is managed independently, runs the IP protocol and confirms to certain naming and address conventions.

6.3.2 LEASED LINE

A large number of medium and large organizations generally needed a huge amount of bandwidth for connecting to the Internet, because the number of users is very high. For instance, suppose 100 users in an office need internet access at the same time. In such situation, the simplest option of obtaining 100 dial-up accounts from an ISP is not very attractive. The organization would need 100 telephone lines for 100 dial-up connections. Clearly this is not acceptable for reasons of cost and maintenance. Also, the moment a new user is added, a new Internet connection and a new telephone line would be required for that user.

Consequently, telephone companies and ISPs have come up with the option of offering more bandwidth from their premises, and the letting the organization divide it internally the way it wants. For this, an ISP provides an option of leasing lines to these kinds of organizations. A leased line can be thought of as a very thick pipe connecting the office of an organization with the Internet via the ISP. A medium-to-big organization obtains a leased line from an ISP for fixed charges per month (year), regardless of its actual use. The organization gets a huge bandwidth from ISP, which can be shared by multiple users at the same time. Access rate using leased line is between 64 Kbps to 2 Mbps, depending on the system in use. Equipment called Data Service Unit (DSU) and Channel Service Unit (CSU) are setup in pair, one at the customer site and other at the ISP site. There is no phone dialing required since the connection is direct. Also the only protocol needed to complete the access is TCP/IP, for much the same reason. Depending on the transfer rate required and the distance between the sites, cabling between them can be made with fiber optic cable or unshielded twisted pair (UTP) copper wire.

6.3.3 ISDN

ISDN (Integrated Services Digital Network) is a set of standards for digital transmission over ordinary telephone copper wire as well as over other media. Digitization of telephone network permits the transmission of audio, video and text over existing telephone lines. Home and business users who install an ISDN adapter (in place of a telephone modem) receive Web pages at up to 128 Kbps compared with the maximum 56 Kbps rate of a dialup modem connection. ISDN requires adapters at both ends of the transmission so your access provider also needs an ISDN adapter. ISDN is generally available from your phone company in most urban areas in India. In many areas where DSL and cable modem service are now offered, ISDN is no longer as popular an option as it was formerly.

There are two levels of service in ISDN: the Basic Rate Interface (BRI), intended for the home and small enterprise, and the Primary Rate Interface (PRI), for larger users. Both rates include a number of B-channels and a D-channel. Each B-channel carries data, voice, and other services. Each D-channel carries control and signaling information. Channel types in ISDN are listed in following table.

Channel	Name	Data rate (Kbps)
B	Bearer channel	64
D	Data channel	16,64
H	Hybrid channel	384, 1536,1920

The Basic Rate Interface consists of two 64 Kbps B-channels and one 16 Kbps D-channel. Thus, a Basic Rate user can have up to 128 Kbps service. The Primary Rate consists of 23 B-channels and one 64 Kpbs D-channel in the United States or 30 B-channels and 1 D-channel in Europe.

ISDN in concept is the integration of both analog or voice data together with digital data over the same network. Although the ISDN you can install is integrating these on a medium designed for analog transmission, broadband ISDN (BISDN) is intended to extend the integration of both services throughout the rest of the end-to-end path using fiber optic and radio media. Broadband ISDN encompasses frame relay service for high-speed data that can be sent in large bursts, the Fiber Distributed-Data Interface (FDDI), and the Synchronous Optical Network (SONET). BISDN is intended to support transmission from 2 Mbps up to much higher, but as yet unspecified, rates.

6.3.4 CABLE MODEM

Cable modems are devices that allow high-speed access to the Internet via a cable television network. While similar in some respects to a traditional analog modem, a cable modem is significantly more powerful, capable of delivering data approximately 500 times faster.

Cable modems are primarily used to deliver broadband Internet access, taking advantage of unused bandwidth on a cable television network. Bandwidth of business cable modem service typically range from 3 Megabits per second (Mbit/s) up to 30 Mbit/s or more. The upstream bandwidth on residential cable modem service usually ranges from 384 Kilobits per second (kbit/s) to 6 Mbit/s or more. There are few attempts to offer different service tiers beyond the traditional 'home' and 'business' designations.

In comparison, DSL tends to offer less speed and more variance between service packages and prices. Service quality is also far more dependent on the client's location in relation to the telephone company's nearest central office or Remote Terminal.

There are two potential disadvantages to cable internet:

Users in a neighborhood share the available bandwidth provided by a single coaxial cable line. Therefore, connection speed varies depending on how many people are using the service at the same time. In most areas this has been eliminated due to redundant and fiber networks. From a technical point of view, all networks, including DSL services, are sharing a fixed amount of bandwidth between a multitude of users but because cable networks tend to be spread over larger areas than DSL services, more care must be taken to ensure good network performance.

Many cable Internet providers are reluctant to offer cable modem access without tying it to a cable television subscription. They do this by charging higher rates, say Rs. 400 per month for cable modem only access, than if one bundles it with a cable TV plan where it might be Rs. 300 per month for cable modem service plus Rs. 200 per month for cable TV service.

How Cable Modems Work

Current Internet access via a 28.8-kbps, 33.6-kbps, or 56-kbps modem is referred to as voice band modem technology. Like voice band modems, cable modems **mo**dulate and **dem**odulate data signals. However, cable modems incorporate more functionality suitable for today's high-speed Internet services. In a cable network, data from the network to the user is referred to as downstream, whereas data from the user to the network is referred to as upstream. From a user perspective, a cable modem is a 64/256 QAM RF receiver capable of delivering up to 30 to 40 Mbps of data in one 6-MHz cable channel. This is approximately 500 times faster than a 56–

kbps modem. Data from a user to the network is sent in a flexible and programmable system under control of the head end. The data is modulated using a QPSK/16 QAM transmitter with data rates from 320 kbps up to 10 Mbps. The upstream and downstream data rates may be flexibly configured using cable modems to match subscriber needs. For instance, a business service can be programmed to receive as well as transmit higher bandwidth. A residential user, however, may be configured to receive higher bandwidth access to the Internet while limited to low bandwidth transmission to the network.

A subscriber can continue to receive cable television service while simultaneously receiving data on cable modems to be delivered to a personal computer (PC) with the help of a simple one-to-two splitter. The data service offered by a cable modem may be shared by up to sixteen users in a local-area network (LAN) configuration.

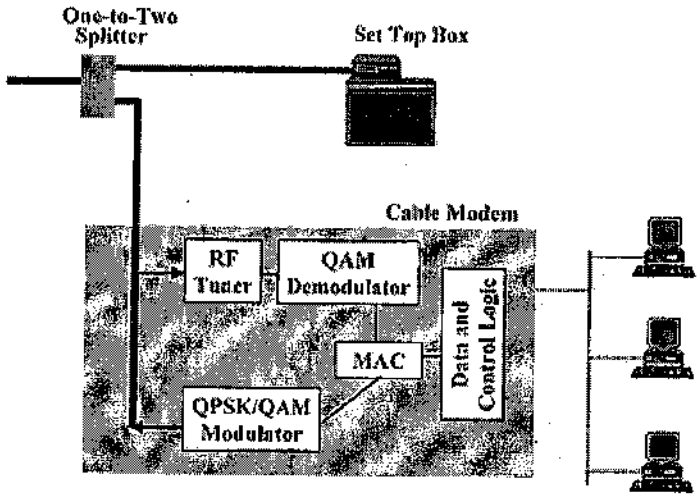


Figure 5: Cable modem at the subcriber location

Beyond modulation and demodulation, a cable modem incorporates many features necessary to extend broadband communications to wide-area networks (WANs). The network layer is chosen as Internet protocol (IP) to support the Internet and World Wide Web services. The data link layer is comprised of three sublayers: logical link control sublayer, link security sublayer conforming to the security requirements, and media access control (MAC) sublayer suitable for cable system operations. Current cable modem systems use Ethernet frame format for data transmission over upstream and downstream data channels. Each of the downstream data channels and the associated upstream data channels on a cable network form an extended Ethernet WAN. As the number of subscribers increases, a cable operator can add more upstream and downstream data channels to support demand for additional bandwidth in the cable data network. From this perspective, growth of new cable data networks can be managed in much the same fashion as the growth of Ethernet LANs within a corporate environment.

The link security sublayer requirements are further defined in three sets of requirements: baseline privacy interface (BPI), security system interface (SSI), and removable security module interface (RSMI). BPI provides cable modem users with data privacy across the cable network by encrypting data traffic between the user's cable modem and CMTS. The operational support provided by the EMS allows a CMTS to map a cable modem identity to paying subscribers and thereby authorize subscriber access to data network services. Thus, the privacy and security requirements protect user data as well as prevent theft of cable data services.

Early discussions in the Institute of Electrical and Electronic Engineers (IEEE) 802.14 Committee referred to the use of asynchronous transfer mode (ATM) over cable data networks to facilitate multiple services including telephone, data, and video, all of which are supported over cable modems. Although current cable modem standards incorporate Ethernet over cable modem, extensions are provided in the standards for future support of ATM or other protocol data units. IP–telephony support over cable data networks is expected to be a new value-added service in the near term.

6.3.5 ASYMMETRIC DIGITAL SUBSCRIBER LINES (ADSL)

Digital Subscriber Line (DSL) technology is a modem technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. The term xDSL covers a number of similar yet competing forms of DSL technologies, including ADSL, SDSL, HDSL, HDSL-2, G.SHDL, IDSL, and VDSL. xDSL is drawing significant attention from implementers and service providers because it promises to deliver high-bandwidth data rates to dispersed locations with relatively small changes to the existing telco infrastructure.

xDSL services are dedicated, point-to-point, public network access over twisted-pair copper wire on the local loop (last mile) between a network service provider's (NSP) central office and the customer site, or on local loops created either intrabuilding or intracampus. Currently, most DSL deployments are ADSL, mainly delivered to residential customers.

Asymmetric Digital Subscriber Line (ADSL) technology is asymmetric. It allows more bandwidth downstream—from an NSP's central office to the customer site—than upstream from the subscriber to the central office. This asymmetry, combined with always-on access (which eliminates call setup), makes ADSL ideal for Internet/intranet surfing, video-on-demand, and remote LAN access. Users of these applications typically download much more information than they send.

ADSL transmits more than 6 Mbps to a subscriber and as much as 640 kbps more in both directions (shown in Figure 21-1). Such rates expand existing access capacity by a factor of 50 or more without new cabling. ADSL can literally transform the existing public information network from one limited to voice, text, and low-resolution graphics to a powerful, ubiquitous system capable of bringing multimedia, including full-motion video, to every home this century.

ADSL will play a crucial role over the next decade or more as telephone companies enter new markets for delivering information in video and multimedia formats. New broadband cabling will take decades to reach all prospective subscribers. Success of these new services depends on reaching as many subscribers as possible during the first few years. By bringing movies, television, video catalogs, remote CD-ROMs, corporate LANs, and the Internet into homes and small businesses, ADSL will make these markets viable and profitable for telephone companies and application

ADSL Capabilities

An ADSL circuit connects an ADSL modem on each end of a twisted-pair telephone line, creating three information channels: a high-speed downstream channel, a medium-speed duplex channel, and a basic telephone service channel. The basic telephone service channel is split off from the digital modem by filters, thus guaranteeing uninterrupted basic telephone service, even if ADSL fails. The high-speed channel ranges from 1.5 to 9 Mbps, and duplex rates range from 16 to 640 kbps. Each channel can be sub multiplexed to form multiple lower-rate channels.

ADSL modems provide data rates consistent with North American T1 1.544 Mbps and European E1 2.048 Mbps digital hierarchies, and can be purchased with various speed ranges and capabilities. The minimum configuration provides 1.5 or 2.0 Mbps downstream and a 16-kbps duplex channel; others provide rates of 6.1 Mbps and 64 kbps for duplex. Products with downstream rates up to 8 Mbps and duplex rates up to 640 kbps are available today. ADSL modems accommodate Asynchronous Transfer Mode (ATM) transport with variable rates and compensation for ATM overhead, as well as IP protocols.

ADSL Technology

ADSL depends on advanced digital signal processing and creative algorithms to squeeze so much information through twisted-pair telephone lines. In addition, many advances have been required in transformers, analog filters, and analog/digital (A/D) converters. Long telephone lines may attenuate signals at 1 MHz (the outer edge of the band used by ADSL) by as much as 90 dB, forcing analog sections of ADSL modems to work very hard to realize large dynamic ranges, separate channels, and maintain low noise figures. On the outside, ADSL looks simple—transparent synchronous data pipes at various data rates over ordinary telephone lines. The inside, where all the transistors work, is a miracle of modern technology. Figure 6 displays the ADSL transceiver-network end.

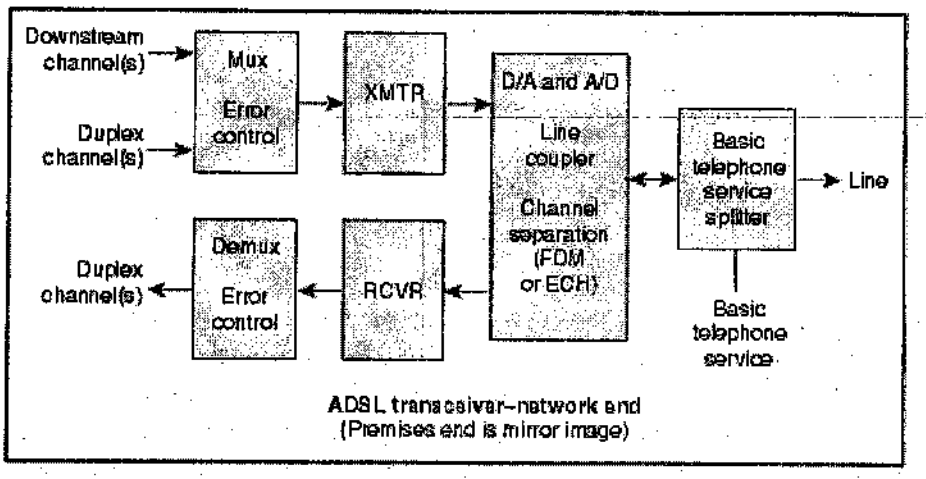


Figure 6: Overview of the Devices That Make Up the ADSL Transceiver-Network End of the Topology

To create multiple channels, ADSL modems divide the available bandwidth of a telephone line in one of two ways: frequency-division multiplexing (FDM) or echo cancellation. FDM assigns one band for upstream data and another band for downstream data. The downstream path is then divided by time-division multiplexing into one or more high-speed channels and one or more low-speed channels. The upstream path is also multiplexed into corresponding low-speed channels. Echo cancellation assigns the upstream band to overlap the downstream, and separates the two by means of local echo cancellation, a technique well known in V.32 and V.34 modems. With either technique, ADSL splits off a 4-kHz region for basic telephone service at the DC end of the band.

6.4 VOICE MAIL

Voicemail (or voice mail, vmail or VMS, sometimes called message bank) is a centralized system of managing telephone messages for a large group of people. In its simplest form it mimics the

functions of an answering machine, uses a standard telephone handset for the user interface, and uses a centralized, computerized system rather than equipment at the individual telephone. Voicemail systems are much more sophisticated than answering machines in that they can:

- answer many phones at the same time
- store incoming voice messages in personalized mailboxes associated with the user's phone number
- enable users to forward received messages to another voice mailbox
- send messages to one or more other user voice mailboxes
- add a voice introduction to a forwarded message
- store voice messages for future delivery
- make calls to a telephone or paging service to notify the user a message has arrived in his/her mailbox
- transfer callers to another phone number for personal assistance
- play different message greetings to different callers.

Voicemail messages are stored on hard disk drives, media generally used by computers to store other forms of data. Messages are recorded in digitized natural human voice similar to how music is stored on a CD. To retrieve messages, a user calls the system from any phone, logs on using Touch-tones (clearing security), and his/her messages can be retrieved immediately. Many users can retrieve or store messages at the same time on the same voicemail system.

Many voicemail systems also offer an automated attendant facility. Automated attendants enable callers to a "main" business number to access directory service or self-route the call to various places such as a specific department, an extension number, or to an informational recording in a voice mailbox, etc.

Voicemail systems contain following elements:

- A central processor (CPU) which runs the operating system and a program (software) that gives the system the look-and-feel of a voicemail system. This software includes thousands of pre-recorded prompts that "speak" to the users as they interact with the system;
- Disk controller and multiple disk drives for message storage;
- System disks which not only include the software above, but also contain a complete directory of all users with pertinent data about each (name, extension number, voicemail preferences, and pointers to each of the messages stored on the message disk that belong to them);
- Telephone interface system that enables many phone lines to be connected to it.

Voicemail systems are often associated with office telephone systems or PBXs. They may also be associated with public telephone network services such as residential phones or cellular phones. Mobile phones generally have voicemail as a standard network feature. The most modern implementations of voicemail support fax delivery to personal voice mailboxes and retrieval via printers, are integrated into e-mail systems for shared directories and shared message storage (also called Unified Messaging), and use touch tone telephony user interfaces (TUI), speech technologies, and/or visual, screen-based graphical user interfaces (GUI) user interfaces.

6.5 VIDEO CONFERENCING

A videoconference (also known as a video teleconference) is a set of interactive telecommunication technologies which allow two or more locations to interact via two-way video and audio transmissions simultaneously. It has also been called visual collaboration and is a type of groupware

Simple analog videoconferences could be established as early as the invention of the television. Such videoconferencing systems consisted of two closed-circuit television systems connected via cable. During the first manned space flights, NASA used two radiofrequency (UHF or VHF) links, one in each direction. TV channels routinely use this kind of videoconferencing when reporting from distant locations, for instance. Then mobile links to satellites using special trucks became rather common.

This technique was very expensive, though, and could not be used for more mundane applications, such as telemedicine, distance education, business meetings, and so on, particularly in long-distance applications. Attempts at using normal telephony networks to transmit slow-scan video, such as the first systems developed by AT&T, failed mostly due to the poor picture quality and the lack of efficient video compression techniques. The greater 1 MHz bandwidth of Picturephone in the 1970s also did not cause the service to prosper.

It was only in the 1980s that digital telephony transmission networks became possible, such as ISDN, assuring a minimum bandwidth (usually 128 kilobits/sec) for compressed video and audio transmission. The first dedicated systems, such as those manufactured by pioneering VTC firms, like PictureTel, started to appear in the market as ISDN networks were expanding throughout the world. Video teleconference systems throughout the 1990's rapidly evolved from highly expensive proprietary equipment, software and network requirements to standards based technology that is readily available to the general public at a reasonable cost. Finally, in the 1990s, IP (Internet Protocol) based videoconferencing became possible and more efficient video compression technologies were developed, permitting desktop, or personal computer (PC)-based videoconferencing. In 1992 CU-SeeMe was developed at Cornell by Tim Dorcey et al. VTC arrived to the masses and free services and software, such as NetMeeting, MSN Messenger, Yahoo Messenger, Skype and others brought cheap, albeit low-quality, VTC.

The core technology used in a video teleconference (VTC) system is digital compression of audio and video streams in real time. The hardware or software that performs compression is called a codec (coder/decoder). Compression rates of up to 1:500 can be achieved. The resulting digital stream of 1's and 0's is subdivided into labeled packets, which are then transmitted through a digital network of some kind (usually ISDN or IP). The use of audio modems in the transmission line allow for the use of POTS, or the Plain Old Telephone System, in some low-speed applications, such as video telephony, because they convert the digital pulses to/from analog waves in the audio spectrum range.

The other components required for a VTC system include:

- **Video input**: video camera or web cam
- **Video output**: computer monitor, television or projector
- **Audio input**: microphones
- **Audio output**: usually loudspeakers associated with the dis play device or telephone
- **Data transfer**: analog or digital telephone network, LAN or Internet

There are basically two kinds of VTC systems:

Dedicated systems have all required components packaged into a single piece of equipment, usually a console with a high quality remote controlled video camera. These cameras can be controlled at a distance to pan left and right, tilt up and down, and zoom. They became known as PTZ cameras. The console contains all electrical interfaces, the control computer, and the software or hardware-based codec. Omni directional microphones are connected to the console, as well as a TV monitor with loudspeakers and/or a video projector. There are several types of dedicated VTC devices:

Large group VTC are non-portable, large, more expensive devices used for large rooms and auditoriums.

Small group VTC are non-portable or portable, smaller, less expensive devices used for small meeting rooms.

Individual VTC are usually portable devices, meant for single users, have fixed cameras, microphones and loudspeakers integrated into the console.

Desktop systems are add-ons (hardware boards, usually) to normal PC's, transforming them into VTC devices. A range of different cameras and microphones can be used with the board, which contains the necessary codec and transmission interfaces. Most of the desktops systems work with the H.323 standard. Video conferences carried out via dispersed PCs are also known as e-meetings.

Simultaneous videoconferencing among three or more remote points is possible by means of a Multipoint Control Unit (MCU). This is a bridge that interconnects calls from several sources (in a similar way to the audio conference call). All parties call the MCU unit, or the MCU unit can also call the parties which are going to participate, in sequence. There are MCU bridges for IP and ISDN-based videoconferencing. There are MCUs which are pure software, and others which are a combination of hardware and software. An MCU is characterized according to the number of simultaneous calls it can handle, its ability to conduct transposing of data rates and protocols, and features such as Continuous Presence, in which multiple parties can be seen onscreen at once.

MCUs can be stand-alone hardware devices, or they can be embedded into dedicated VTC units.

Some systems are capable of multipoint conferencing with no MCU, stand-alone, embedded or otherwise. These use a standards-based H.323 technique known as "decentralized multipoint", where each station in a multipoint call exchanges video and audio directly with the other stations with no central "manager" or other bottleneck. The advantages of this technique are that the video and audio will generally be of higher quality because they don't have to be relayed through a central point. Also, users can make ad-hoc multipoint calls without any concern for the availability or control of an MCU. This added convenience and quality comes at the expense of some increased network bandwidth, because every station must transmit to every other station directly.

In recent years, IP based videoconferencing has emerged as a common communications interface and standard provided by VTC manufacturers in their traditional ISDN-based systems. Business, government and military organizations still predominantly use H.320 and ISDN VTC. Though, due to the price point and proliferation of the Internet, and broadband in particular, there has been a strong spurt of growth and use of H.323, IP VTC. H.323 has the advantage that it is accessible to anyone with a high speed Internet connection, such as DSL.

In addition, an attractive factor for IP VTC is that it is easier to set-up for use with a live VTC call along with web conferencing for use in data collaboration. These combined technologies enable users to have a much richer multimedia environment for live meetings, collaboration and presentations.

High speed Internet connectivity has become more widely available at a reasonable cost and the cost of video capture and display technology has decreased. Consequently personal video teleconference systems based on a web cam, personal computer system, software compression and broadband Internet connectivity have become affordable for the general public. Also, the hardware used for this technology has continued to improve in quality, and prices have dropped dramatically. The availability of free software (often as part of chat programs such as msn messenger) has made software based videoconferencing accessible to many.

For many years, futurists have envisioned a future where telephone conversations will take place as actual face-to-face encounters with video as well as audio. Desktop PC videoconferencing promises to make this a reality, although it remains to be seen whether there is widespread enthusiasm for video calling.

Videoconferencing provides students with the opportunity to learn by participating in a 2-way communication platform. Furthermore, teachers and lecturers from all over the world can be brought to classes in remote or otherwise isolated places. Students from diverse communities and backgrounds can come together to learn about one another. Students are able to explore, communicate, analyze and share information and ideas with one another. Through video conferencing students can visit another part of the world to speak with others, visit a zoo, a museum and so on, to learn. These "virtual field trips" can bring opportunities to children, especially those in geographically isolated or the economically disadvantaged. Small schools can use this technology to pool resources and teach courses (such as foreign languages) which otherwise couldn't be offered. Teachers can use this technology to acquire additional college credits for recertification without driving to classes

Videoconferencing is a very useful technology for telemedicine and telenursing applications, such as diagnosis, consulting, transmission of medical images, etc., in real time. Using VTC, patients may contact nurses and physicians in emergency or routine situations, physicians and other paramedical professionals can discuss cases across large distances. Rural areas can use this technology for diagnostic purposes, thus saving lives and making more efficient use of health care dollars.

Special peripherals such as microscopes fitted with digital cameras, video endoscopes, medical ultrasound imaging devices, otoscopes, etc., can be used in conjunction with VTC equipment to transmit data about a patient.

Videoconferencing can enable individuals in faraway places to have meetings on short notice. Time and money that used to be spent in traveling can be used to have short meetings. Technology such as VOIP can be used in conjunction with desktop videoconferencing to enable face-to-face business meetings without leaving the desktop, especially for businesses with wide-spread offices. The technology is also used for telecommuting, in which employees work from home.

6.6 INTERNET PRIVACY

Internet privacy consists of privacy over the media of the Internet: the ability to control what information one reveals about oneself over the Internet, and to control who can access that information. Many people use the term to mean universal Internet privacy: every user of the Internet possessing Internet privacy.

Internet privacy forms a subset of computer privacy. Experts in the field of Internet privacy have a consensus that Internet privacy does not really exist. Privacy advocates believe that it should exist.

People with only a casual interest in Internet privacy need not achieve total anonymity. Regular Internet users with an eye to privacy may succeed in achieving a desirable level of privacy through careful disclosure of personal information and by avoiding spyware. The revelation of IP addresses, non-personally-identifiable profiling, and so on might become acceptable trade-offs for the convenience that such users would otherwise lose in using the workarounds needed to suppress such details rigorously. On the other hand, some people desire much stronger privacy. In that case, they may use Internet anonymity to ensure privacy - use of the Internet without giving any third parties the ability to link the Internet activities to personally-identifiable information of the Internet user.

Those concerned about Internet privacy often cite a number of privacy risks - events that can compromise privacy — which one may encounter through Internet use. Unfortunately, given the complexity of Internet privacy, many people do not understand the issues. Therefore this section covers not only "real" privacy risks, but also risks perceived as overemphasized.

6.6.1 COOKIES

Cookies are a very important method for maintaining state on the Web. "State" in this case refers to an application's ability to work interactively with a user, remembering all data since the application started, and differentiating between users and their individual data sets.

An analogy I like to use is a laundry cleaner's shop. You drop something off, and get a ticket. When you return with the ticket, you get your clothes back. If you don't have the ticket, then the laundry man doesn't know which clothes are yours. In fact, he won't be able to tell whether you are there to pick up clothes, or a brand new customer. As such, the ticket is critical to maintaining state between you and the laundry man.

Unfortunately, HTTP is a "stateless" protocol. This means that each visit to a site (or even clicks within a site) is seen by the server as the first visit by the user. In essence, the server "forgets" everything after each request, unless it can somehow mark a visitor (that is, hand him a "laundry ticket") to help it remember. Cookies can accomplish this.

A cookie is a text-only string that gets entered into the memory of your browser. This value of a variable that a website sets. If the lifetime of this value is set to be longer than the time you spend at that site, then this string is saved to file for future reference.

Technically, cookies are arbitrary pieces of data chosen by the Web server and sent to the browser. The browser returns them unchanged to the server, introducing a state (memory of previous events) into otherwise stateless HTTP transactions. Without cookies, each retrieval of a Web page or component of a Web page is an isolated event, mostly unrelated to all other views of the pages of the same site. By returning a cookie to a web server, the browser provides the server a means of connecting the current page view with prior page views. Other than being set by a web server, cookies can also be set by a script in a language such as JavaScript, if supported and enabled by the Web browser.

Cookie specifications suggest that browsers should support a minimal number of cookies or amount of memory for storing them. In particular, an internet browser is expected to be able to store at least 300 cookies of 4 kilobytes each, and at least 20 cookies per server or domain. Cookies names are case insensitive.

The cookie setter can specify a deletion date, in which case the cookie will be removed on that date. If the cookie setter does not specify a date, the cookie is removed once the user quits his or her browser. As a result, specifying a date is a way for making a cookie survive across sessions. For this reason, cookies with an expiration date are called *persistent*. As an example application, a shopping site can use persistent cookies to store the items users have placed in their basket. This way, if users quit their browser without making a purchase and return later, they don't have to find the products they previously placed in the shopping cart over again.

Cookies are in fact only data, not program code: they cannot erase or read information from the user's computer. However, cookies allow for detecting the Web pages viewed by a user on a given site or set of sites. This information can be collected in a *profile* of the user. Such profiles are often anonymous, that is, they do not contain personal information of the user (name, address, etc.) More precisely, they cannot contain personal information unless the user has made it available to some sites. Even if anonymous, these profiles have been the subject of some privacy concerns.

According to the same survey, a large percentage of Internet users do not know how to delete cookies.

Most modern browsers support cookies. However, a user can usually also choose whether cookies should be used or not. The following are common options: (1) cookies are never accepted, (2) the browser asks the user whether to accept every individual cookie, or (3) cookies are always accepted.

The browser may also include the possibility of better specifying which cookies have to be accepted or not. In particular, the user can typically choose one or more of the following options: reject cookies from specific domains; disallow third-party cookies; accept cookies as non-persistent (expiring when the browser is closed); and allow a server to set cookies for a different domain. Additionally, browsers may also allow users to view and delete individual cookies.

Most browsers supporting JavaScript allow the user to see the cookies that are active with respect to a given page by typing javascript:alert ("Cookies: "+document.cookie) in the browser URL field. Some browsers incorporate a cookie manager for the user to see and selectively delete the cookies currently stored in the browser.

The P3P specification includes the possibility for a server to state a privacy policy, which specifies which kind of information it collects and for which purpose. These policies include (but are not limited to) the use of information gathered using cookies. According to the P3P specification, a browser can accept or reject cookies by comparing the privacy policy with the stored user preferences or ask the user, presenting them the privacy policy as declared by the server.

Cookies have some important implications on the privacy and anonymity of Web users. While cookies are only sent to the server setting them or one in the same Internet domain, a Web page may contain images or other components stored on servers in other domains. Cookies that are set during retrieval of these components are called *third-party cookies*.

Advertising companies use third-party cookies to track a user across multiple sites. In particular, an advertising company can track a user across all pages where it has placed advertising images or web bugs. Knowledge of the pages visited by a user allows the advertisement company to target advertisement to the user's presumed preferences.

The possibility of building a profile of users has been considered by some a potential privacy threat, even when the tracking is done on a single domain but especially when tracking is done

across multiple domains using third-party cookies. For this reason, some countries have legislation about cookies.

Besides privacy concerns, cookies also have some technical drawbacks. In particular, they do not always accurately identify users, they can be used for security attacks, and they are at odds with the Representational State Transfer (REST) software architectural style.

If more than one browser is used on a computer, each has a separate storage area for cookies. Hence cookies do not identify a person, but a combination of a user account, a computer, and a Web browser. Thus, anyone who uses multiple accounts, computers, or browsers has multiple sets of cookies.

Likewise, cookies do not differentiate between multiple users who share a computer and browser, if they do not use different user accounts.

6.7 INTERNET SECURITY

Internet security is the practice of protecting and preserving private resources and information on the Internet. Computer and network security are challenging topics among executives and managers of computer corporations. Even discussing security policies may seem to create a potential liability. As a result, enterprise management teams are often not aware of the many advances and innovations in Internet and intranet security technology. Without this knowledge, corporations are not able to take full advantage of the benefits and capabilities of the network. Together, network security and a well-implemented security policy can provide a highly secure solution. Employees can then confidently use secure data transmission channels and reduce or eliminate less secure methods, such as photocopying proprietary information, sending purchase orders and other sensitive financial information by fax, and placing orders by phone.

6.7.1 ANTI VIRUS

A computer virus is probably the best known and most dangerous threat to computer security. Just like an organic virus, a computer virus attaches itself to healthy computer programs (body cells). With over 1000 different types of viruses, there is a variety of different parts of the computer they can attack e.g. boot sector. A computer virus is a piece of code someone inserts into an otherwise legitimate computer program for the purpose of causing mischief. Some viruses are just annoying. For example, one may cause a political message or animation display to pop up on your screen, and that's all it does. Other viruses can do considerable damage. A particularly malicious one might erase every file on your hard drive. Viruses are also designed to spread from one machine to another through shared files. A user can unknowingly infect his or her own computer and then spread that virus to others without realizing it. Some viruses are visible and obvious, while others are subtle and devious. A virus that quietly operates behind the scenes might cause a gradual slowdown in the performance of your computer over a long period of time. You would not notice anything right away, and you may never figure out what happened to your computer.

If you plan to download software from the Internet, you need to know how to protect yourself. You never have to be heart by a computer virus if you take some simple precautions. The most common symptoms that indicate your computer has been infected,

- files and data is deleted
- the computer takes longer to load programs/applications
- items and images on your screen are distorted and unusual images and text appears
- unusual noises come from your keyboard, hard disk

- hard disk operates excessively or is inaccessible
- disk space and filenames change for no reason
- system tools such as Scandisk return incorrect values

The only way to know if a virus is present on your computer is with special software designed to detect viruses hiding in your file. These software also provide remedy from these viruses, and called antivirus software. Antivirus software locates the known viruses by watching for identifying signatures that give them away. A good antivirus software will look for thousands of viruses, and periodically software updates are released to keep up with new viruses. The best way to protect yourself against viruses is to buy a good anti-virus software package such as Norton or McAfee and keep installing the latest updates. Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware). Antivirus software typically uses two different techniques to accomplish this:

(i) Examining (scanning) files to look for known viruses matching definitions in a virus dictionary.

(ii) Identifying suspicious behavior from any computer program which might indicate infection. Such analysis may include data captures, port monitoring and other methods.

In the virus dictionary approach, when the antivirus software examines a file, it refers to a dictionary of known viruses that the authors of the antivirus software have identified. If a piece of code in the file matches any virus identified in the dictionary, then the antivirus software can take one of the following actions:

- attempt to repair the file by removing the virus itself from the file
- quarantine the file (such that the file remains inaccessible to other programs and its virus can no longer spread)
- delete the infected file

To achieve consistent success in the medium and long term, the virus dictionary approach requires periodic (generally online) downloads of updated virus dictionary entries. As civically minded and technically inclined users identify new viruses "in the wild", they can send their infected files to the authors of antivirus software, who then include information about the new viruses in their dictionaries.

Dictionary-based antivirus software typically examines files when the computer's operating system creates, opens, closes or e-mails them. In this way it can detect a known virus immediately upon receipt. Note too that a System Administrator can typically schedule the antivirus software to examine (scan) all files on the computer's hard disk on a regular basis.

Although the dictionary approach can effectively contain virus outbreaks in the right circumstances, virus authors have tried to stay a step ahead of such software by writing "oligomorphic", "polymorphic" and more recently "metamorphic" viruses, which encrypt parts of themselves or otherwise modify themselves as a method of disguise, so as to not match the virus's signature in the dictionary.

The suspicious behavior approach, by contrast, doesn't attempt to identify known viruses, but instead monitors the behavior of all programs. If one program tries to write data to an executable program, for example, the antivirus software can flag this suspicious behavior, alert a user and ask what to do.

Unlike the dictionary approach, the suspicious behavior approach therefore provides protection against brand-new viruses that do not yet exist in any virus dictionaries. However, it can also sound a large number of false positives, and users probably become desensitized to all the warn-

ings. If the user clicks "Accept" on every such warning, then the antivirus software obviously gives no benefit to that user. This problem has worsened since 1997, since many more nonmalicious program designs came to modify other .exe files without regard to this false positive issue. Thus, most modern antivirus software uses this technique less and less.

Some antivirus-software uses of other types of heuristic analysis. For example, it could try to emulate the beginning of the code of each new executable that the system invokes before transferring control to that executable. If the program seems to use self-modifying code or otherwise appears as a virus (if it immediately tries to find other executables, for example), one could assume that a virus has infected the executable. However, this method could result in a lot of false positives.

Yet another detection method involves using a sandbox. A sandbox emulates the operating system and runs the executable in this simulation. After the program has terminated, software analyzes the sandbox for any changes which might indicate a virus. Because of performance issues, this type of detection normally only takes place during on-demand scans. Also this method may fail as virus can be nondeterministic and result in different actions or no actions at all done then run - so it will be impossible to detect it from one run.

Most commercial antivirus software uses both of these approaches, with an emphasis on the virus dictionary approach. These software may not always protect you against the latest virus, but offer the best solution possible. You should always try the following

Install anti-virus software.

Keep your anti-virus software up-to-date.

Install a personal firewall

Use Windows / Apple / Linux updates to patch security holes.

Don't open email messages that look suspicious

Don't click on email attachments you were not expecting

6.7.2 FIREWALLS

A web server usually hosts many web sites and offers many services on the Internet, or it network is an organization, it has many valuable and confidential information on line - trade secrets, product development plan, marketing strategies, financial analysis, etc. Disclosure of this information to a competitor could have dire consequences. In addition to danger of information leaking out, there is also a danger of information leaking in. In particular, viruses, worms, and other digital pests can breach the security, destroy valuable data, and waste large amount of administrators' time trying to clean up the mess they leave.

A firewall is a mechanism for protecting a local network from external, untrusted networks. Like the physical firewall used in some buildings to limit the spread of fire, a network firewall protects user's site from purposeful and inadvertent attacks from the outside. The firewall is placed as an interface between the server or network and the Internet or other external systems. Firewall can exist between different intra-networks to prevent security breaches from internal sources.

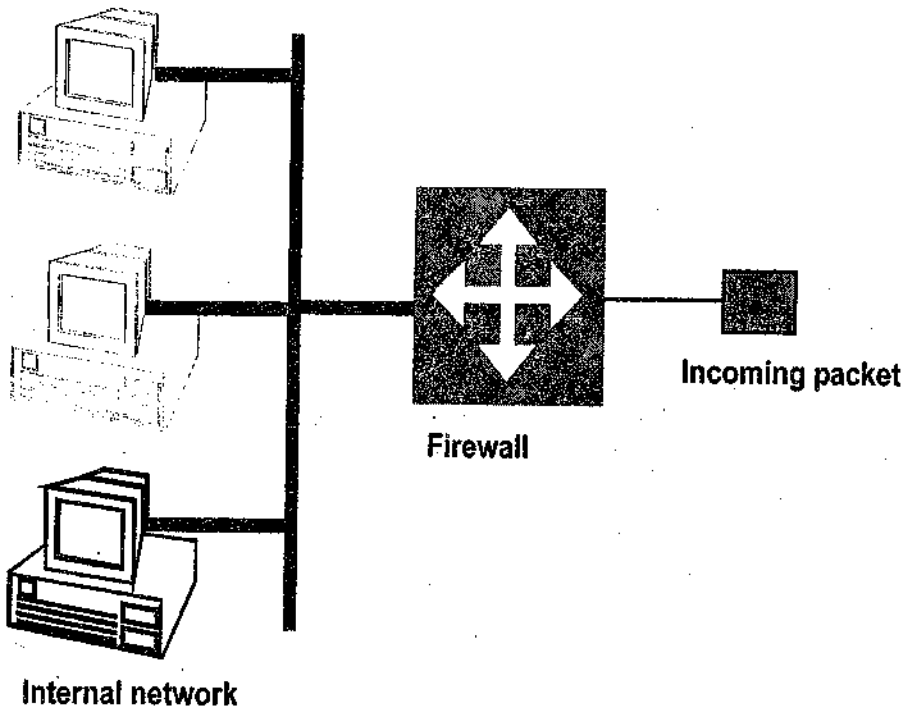


Figure 7: A Firewall in operation.

Firewall enforces the security policy that each site adopts. The sophistication of the firewall depends on the individual's security philosophy. There is a wide variety of firewall packages available such as the BlackICE Defender and software available from Norton and McAfee. Firewall's can protect networks and personal computers from attacks on packet traffic, ftp and telnet applications and use technologies such as a proxy server which hides the IP address of a network or personal computer.

The characteristics of a good firewall implementation are as follows:

- All traffic from inside to outside, and vice versa, must pass through the firewall. To achieve this, all the outside access to the local network must be physically blocked, and access only via the firewall should be permitted.
- Only the traffic authorized as per the local security policy should be allowed to pass through the firewall.
- The firewall itself must be strong enough, so as to render attacks on it useless.

Firewalls can be classified into three generic types, which might be employed in combination.

6.7.2.1 Packet filters

Packet filters block or permit packets based on a set of rules that specifies characteristics such as those listed here:

- State of the connection (new or already established)
- Direction the packet is traveling (inbound or outbound)
- Communications protocol used (such as IP, IPX, ICMP, TCP, UDP)
- Source and/or destination addresses

- Protocol port number
- physical interface

A network administrator usually configures these rules ahead of time. The header part of each packet is examined, rules are applied consecutively and all packets are subject to a pass/fail decision. If the packet header passes all requirements, the packet is forwarded on to the public network. If the packet fails any rule test, it is discarded. An audit trail is maintained in this case for future reference. A packet filter is standard router which has some additional functionality which allows the packet filters to examine every incoming or outgoing packet.

Packet filters are the most easily accessible form of protection in the environments and provide an excellent start. Given that most routers today have packet filter capabilities, and routers are required to connect to the Internet, every organization should at least implement this basic type of security.

6.7.2.2 Higher Layer Inspection Firewalls

It is similar to packet filters but are more sophisticated due to their awareness of all layers in the protocol stack. The device can be software, hardware, or a combination of both. Many higher layer inspection firewalls are just software that runs on a server, although some routers have these capabilities as well. These firewalls typically maintain state tables to enable the scanning of packets within the context of the overall data stream. The most popular example of a higher-layer inspection firewall is CheckPoint's Firewall-1 product.

While ordinary packet filters can also operate on some fields of the TCP/UDP headers, a higher layer inspection firewall makes this feature its main purpose and adds many more inspection capabilities to simple TCP/IP "pseudo-header" packet filtering. The higher layer inspection firewall gives the network an additional level of protection. Because these firewalls maintain state information and understand the typical behavior of protocols and applications, they are more effective at stopping some kinds of attacks.

6.7.2.3 Proxy Servers

Proxy server is an intermediate device that acts in place of one of the end-communicating devices. These servers provide a set of services to the outside, but actually act as a proxy for the real server. An external client does not connect directly to an internal server, but instead attaches to the proxy, which in turn, attached to the internal server. Proxy servers can be in circuit-level or application-level forms.

Application-level proxies are hardware or software specific to a given application. They operate at the Application Layer of TCP/IP. When the internal client attempts to establish a connection to a WWW server on the Internet, the proxy intervenes- it acts like the server from the perspective of the client and acts like a client from the perspective of the server.

A Circuit-level proxy differs in that it is application-independent. It operates at the Transport Layer of TCP/IP. When the WWW client attempts to make connection to the WWW server, the proxy intervenes, but this time at the TCP level. The circuit level proxy has no knowledge of the higher layer protocols. Furthermore, if this client were to attempt to establish an FTP connection to this server, the same proxy host would intervene to create a new TCP connection; in the case of application-level hosts, a different proxy agent would be needed for the WWW and FTP processes.

6.8 SUMMARY

This unit discussed some of the most popular Internet browsers like Lynx, Netscape Navigator, Internet Explorer, Opera and Mozilla. Some of the common features required in these browsers are discussed. we also introduced various types of Internet access methods like dial-up, leased line, ISDN, cable, DSL etc. Features of Voicemail and videoconferencing, two major applications of Internet, are also discussed in this unit. Some aspects of Internet privacy and concept of cookies are also described in this section. Internet security features like anti virus and firewalls are also covered.

Check Your Progress 2

1. What are the advantages of using leased line over dial-up line?
2. Whar are the disadvantages of cable Internet access?
3. What are the options availavle in browsers for cookies?
4. What do you understand by a Firewall?
5. What is Proxy server? What does it do?

6.9 SOLUTIONS/ANSWERS

Check Your Progress 1

1. Connect on the Internet for the addressed domain name and display the page retrieved.
2. Connect on the Internet for the addressed domain name and if modified since last retrieval download and display the page retrieved.
3. Back - Displays the previous page in the history list. A history list references a hierarchy of pages you have already viewed. This tool lights up making it easy to navigate from one page to the previous page.

   Forward - Displays the next page in the history list. When you use Back or a history menu item to retrieve a page, using Forward gets the proceeding page. Forward is only available after you use Back or a history item.

   History - provides a log of all pages accessed, in chronological order, starting with the most recent.
4. Title Bar: It is the top most bar displayed on screen. It displays the name of current application or document.

   Menu Bar: Below the title bar is the menu bar which shows following buttons/options from left to right: File, Edit, View, Do, Communicator, and Help. On a click of mouse at each, a menu is displayed for selecting appropriate command.

   Navigation Tool Bar: It is next to the menu bar. This bar contains several tool buttons like Back, Forward, Home Reload etc.

   Address Bar: It has a picture labeled 'address' on the left and a field for address (URL). This field shows address of current URL. On the right hand side there is a button 'Go'. If you enter a new address in address field, it can be executed using "Go' button. If arrow on the right side of address field is clicked, then the recently visited pages pop up from the history.

   Personal Tool Bar: Using this tool, buttons can be created for various menus. The menus are for URLs of interest. This is done by dragging and dropping the URLs using mouse. Three menus which are already available are Internet, New and Cool, and Lookup.

Status Bar: Located at the bottom of the screen, this bar is used to show the status of mouse action. When content is being loaded, it shows the progress of loading. When loading is completed, it shows status 'done'.

Check Your Progress 2

1. No dialing required in leased line. It provides fast and reliable Internet connection and suitable for large organizations.
2. There are two disadvantages to cable Internet:
   Users in a neighborhood share the available bandwidth provided by a single coaxial cable line. Therefore, connection speed varies depending on how many people are using the service at the same time. In most areas this has been eliminated due to redundant and fiber networks. From a technical point of view, all networks, including DSL services, are sharing a fixed amount of bandwidth between a multitude of users but because cable networks tend to be spread over larger areas than DSL services, more care must be taken to ensure good network performance.
3. Most modern browsers have following settings for cookies: (1) cookies are never accepted, (2) the browser asks the user whether to accept every individual cookie, or (3) cookies are always accepted.
4. A firewall is a mechanism for protecting a local network from external, untrusted networks. Like the physical firewall used in some buildings to limit the spread of fire, a network firewall protects user's site from purposeful and inadvertent attacks from the outside. The firewall is placed as an interface between the server or network and the Internet or other external systems. Firewall can exist between different intra-networks to prevent security breaches from internal sources.
5. Proxy server is an intermediate device that acts in place of one of the end-communicating devices. These servers provide a set of services to the outside, but actually act as a proxy for the real server. An external client does not connect directly to an internal server, but instead attaches to the proxy, which in turn, attached to the internal server. Proxy servers can be in circuit-level or application-level forms.

6.10 UNIT END QUESTIONS

1. What is Firewall? Explain.
2. What is ADSL?
3. Compare LYNX with Internet Explorer.
4. What are cookies?
5. Explain the set up of dial-up connection.

UNIT - VII

WORLD WIDE WEB

STRUCTURE OF THE UNIT

7.0 Objectives
7.1 Introduction to www
7.2 Elements of web
7.3 Web browser
7.4 Using a browser
7.5 Viewing page with a browsers
7.6 Using a browser for mails
7.7 Security and privacy issue (Executable applets and scripts, blocking system)
7.8 Tips for effective browsing downloading / copying files from the web.
7.9 Summary
7.10 Unit end questions

7.0 OBJECTIVES

After going through this unit sudent will be able to :

- Describe elements of www,web browser, web server.
- Describe various types of web browser ,search engine.
- Describe Email uses how to email etc.
- Describe various Security and privacy issue.
- Various tip of browsing and downloading.

7.1 INTRODUCTION TO WWW

World wide web is a part of internet that stores information on pages of various web sites. The web site in the world wide web (www) that stores information on pages on various commercial , business, educational and entertainment topics. www sites may be hosted by individual ,Organizations, Departments, Banks, Suppliers, Service providers, marketing firms, publisher, Doctors , Authors etc.

7.2 ELEMENTS OF WEB

There are lot of elements of web some of them are :-

(1) Gopher

Gopher is a communications method or protocol for retrieving text and file-based information from the Internet. Designed at the University of Minnesota, gopher quickly became an Internet standard. When gopher was first developed, the programs that used this method for accessing Internet information were also called Gopher. Today, programs that use this method of retrieval are referred to as Gopher Clients. The program called Gopher is also considered a Gopher client.

The Gopher protocol is designed to allow easy access to text and file-based information that is distributed across different machines on the Internet.

Gopher allows you to connect to remote computers known as Gopher Servers and browse the information that has been made available on them. Typically, you use Gopher by starting at a local machine, and following connections from that machine out to other sources of data. At each new machine, there are often connections to other computers. This interconnection of data and machines, was the precursor to what has come to be called the World Wide Web

(2) World Wide Web

The World Wide Web (also known as the Web, WWW, and sometimes W3) is the area of the Internet that has received tremendous focus in the last few years. Many people new to the Internet, think that the Web *is* the Internet. However, the Web is just part of the Internet, albeit a very major part.

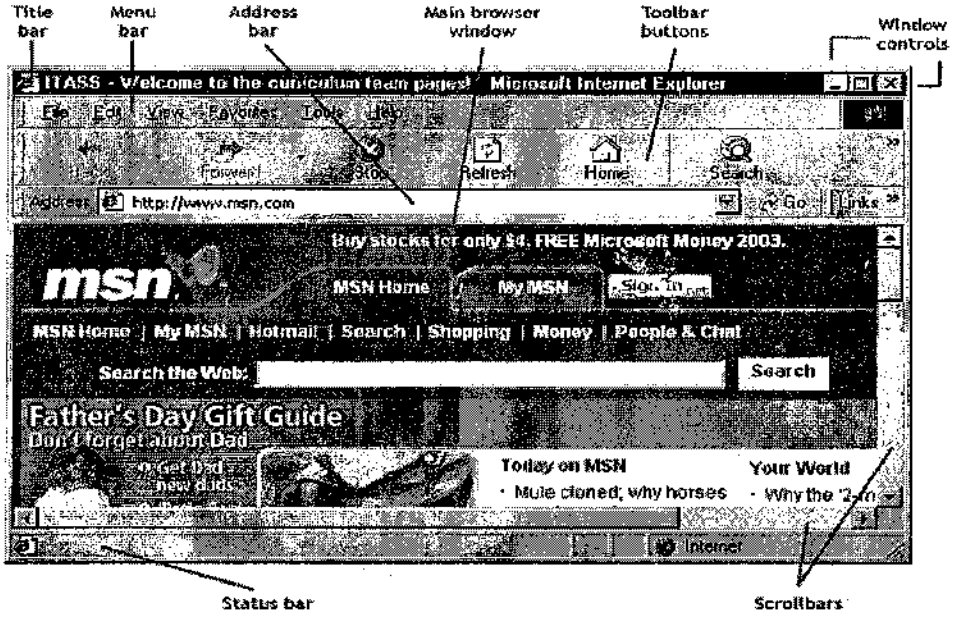
The Web is made up of "sites" - a site being where someone has placed files that can be accessed by those connected to the Internet. The files are of all different types - text, graphic, video, sound, etc. - and they are on computers around the world. They constitute a vast amount of information on several subjects.

The files are accessed by using IP addressing and a specific protocol called http, which stands for Hypertext Transfer Protocol. The Web works on the client/server model. You use a client program which passes your request for information to a server. The server obtains the information and passes it back to your client. The client software that you use to access the Web is called a browser. Popular browsers are Netscape Navigator and Microsoft Internet Explorer. With all of these browsers, you can see graphic files on the Web. There are some text-only browsers, such as Lynx.

(3) Web Browser

A Web browser is a program that you can use to view files on the Internet, including images,text, sound and video.

A graphical Web browser is a browser that enables you to view Multimedia content such as images, audio, and video, on the Internet. The first graphical Web browser was "Mosaic" that was developed in 1993 by the National Center for Supercomputing Application at the University of Illinois. Mac Andreessen and six fellow students developed the program for creating the Mosaic browser while working on a university-sponsored computer project. This program has contributed immensely to developing and propagating the World Wide Web to the forefront of Internet tools. Mosaic converted the text only WWW into an environment that is similar to Microsoft Windows. With the introduction of Mosaic, the total amount of data transported through the Web increased by a factor of 10,000 within six months

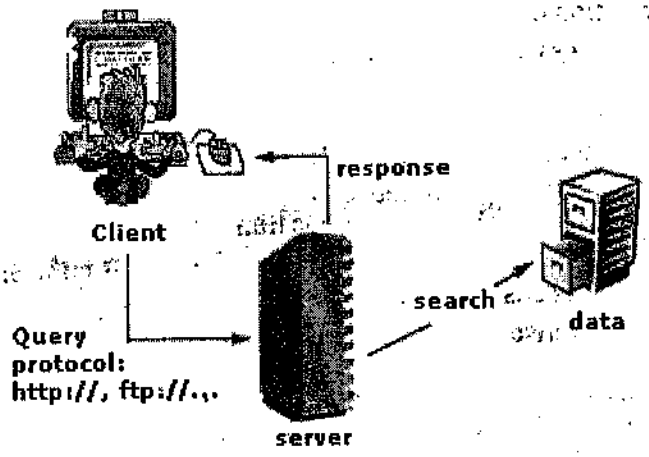


(4) Web Server

A web server is the computer that stores web pages or an application that resides on the server. The computer and the server refer to the hardware components while the application is the software component. The server transmits graphics, audio, and video to web browsers. Web servers are also called HTTP servers because they use the HyperText Transfer Protocol (HTTP) to serve web pages to web browsers.

A connection between the web browser and the web server is called 'stateless'. This is because when you send a request for a web page to a web server by using the browser, the server checks for the validity of the request for an HTML document. Then the server sends the requested web page to your web browser and the connection is closed. The web browser connects to the web server only when a request for the web page to be reloaded or refreshed is submitted.

we can avail of Web servers by paying for them, known as commercial Web servers. Alternatively, you can use the free Web servers that are called Freeware. Microsoft Internet Information Server (IIS)® and Netscape web server are among the most popular commercial web servers. Apache® is a popular Freeware



(5) HTTP

HTTP, the Hypertext Transfer Protocol, is the application-level protocol that is used to transfer data on the Web. HTTP comprises the rules by which Web browsers and servers exchange information over a TCP/IP connection. An HTTP server is a program that listens on a machine's port for HTTP requests. An HTTP client or web client opens a TCP/IP connection to the server via a socket, transmits a request for a document, and waits for a reply from the server. After the request-reply sequence is completed, the socket is closed. So the HTTP protocol is a transactional one. The lifetime of a connection corresponds to a single request-reply sequence that is known as a transaction.

How Does HTTP Work?

HTTP is a request-response protocol.

The request comprises

- a request line
- a set of request headers
- an entity

The server sends a response that comprises

- a status line,
- a set of response headers, and
- an entity.

The entity in the request or response can be thought of simply as the payload, which may be binary data. The other items are readable ASCII characters. When the response has been completed, the browser or the server may terminate the TCP/IP connection, or the browser can send another request.

(6) URL

URL is the abbreviation of Uniform Resource Locator. A URL is the global address of documents and other resources on the World Wide Web.

The first part of the address indicates the protocol and the second part specifies the IP address or the domain name where the resource is located.

http://oracle.com/certification/documents.asp

here

http:// : This part of the address is always at the start of a web page address and most of the time we don't need to use it

oracle.com : This part is the name of computer which have the pages on them and is known as domain name

/certification/documents.asp: This part indicates the location of the page on the computer

(7) Search Engine

A Search Engine is used to find information on the Internet when you don't know where to start.

Search engines allow users to enter keywords to find Internet sites. Search Engines use "robots" or "crawlers" to find and index words that appear on web sites. The Search Engine then matches the keywords in the search to the words in its index. The different search engines that are available are www.google.com, www.altavista.com, www.hotbot.com, www.yahoo.com, www.askjeeves.com etc.

7.3 WEB BROWSER

Web browser is a program that you can use to view files on the Internet, including images, text, sound and video .

History

The first graphical Web browser, a program that lets Internet users page through the Web, was "Mosaic". This program was developed in 1993 by the National Center for Supercomputing Application at the University of Illinois. Mac Andreessen and six fellow students developed the program while working on a university-sponsored computer project. This program has provided much of the forward push that has brought the World Wide Web to the forefront of Internet tools. Mosaic turned the then text only WWW into a point-and-click environment much like Microsoft Windows by using only a mouse. With the introduction of Mosaic, the total amount of data transported through the Web increased by a factor of 10,000 within six months.

Bookmarks

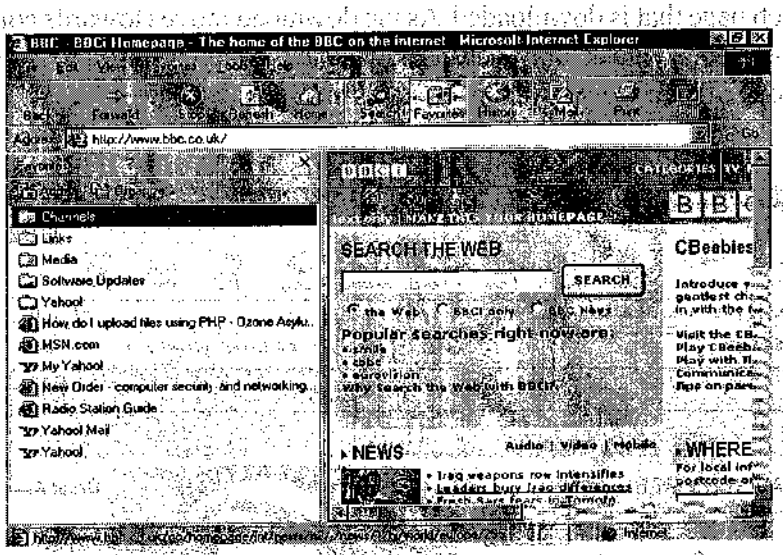
You can use bookmarks to save the locations of Web sites that you can revisit. Bookmarks are stored as a list on your computer. The browser can access this list when you want to revisit the Web site.

7.4 USING A BROWSER

How to use bookmarks?

To view a Web site from the list of bookmarks, select the item that represents the Web site from the list. The browser will display the page.

Please note : The bookmark feature is referred to as favorites in Internet Explorer and bookmark in Netscape Navigator

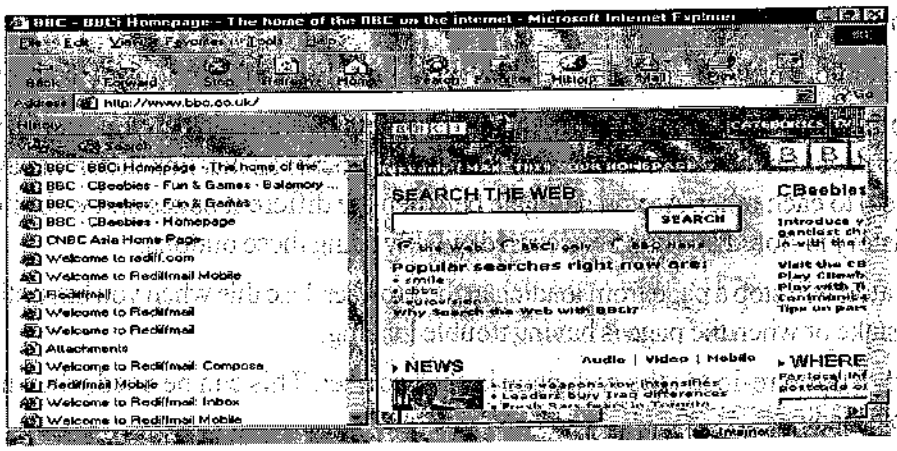


Browser History

A built in feature of the browser which keeps a record of the pages visited by the user with help of the browser.

How to use History

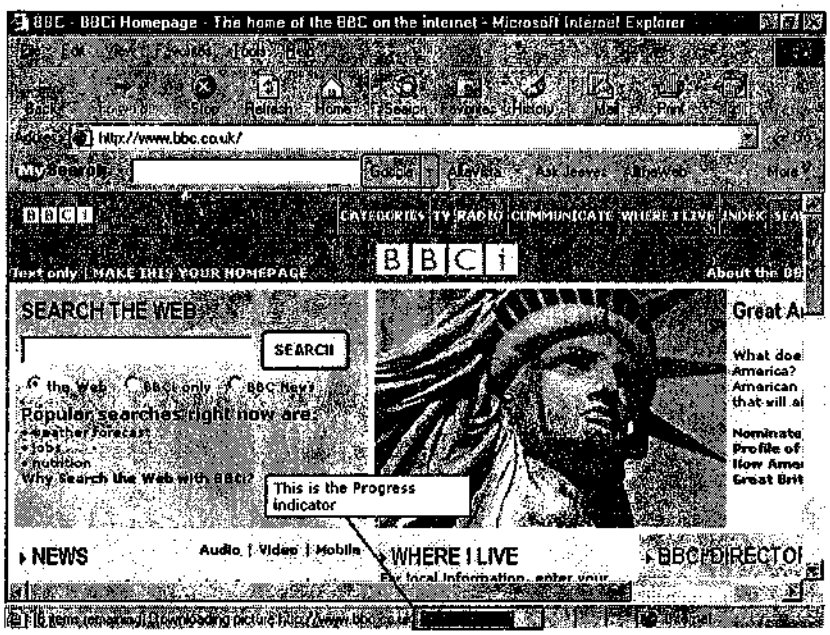
To view a Web site from the list of History, select the item that represents the Web site from the list. The browser will display the page.



Progress Indicator

We have seen that a series of events are fired when we enter the address of a web page or click on a link. These events are shown in the status message field in the lower-left corner of the IE. Examples of messages are connecting to server, web site found waiting for reply, and download-

ing page. Next to the status message field is the progress bar. The progress bar shows the amount of the web page that is downloaded. As the download moves towards completion the progress indicator is filled with color. When the download is completed the progress indicator is empty and a message **Done** is displayed in the status message field.



7.5 VIEWING PAGE WITH A BROWSERS

Using the browser toolbar

The browser toolbar provides quick access to the commonly-used functions of the browser.

The **Back button** and the **Forward Button** are quick navigation aids as you "surf" between different web pages on the internet. Web pages contain Hyperlinks that link different pages (and different sites) to each other. As you navigate between the different pages and web sites, your browsing history is stored and can be accessed quickly using these buttons.

The **Stop** Button will stop a page from loading in the browser. Use this when you have clicked on a link by mistake or when the page is having trouble loading.

The **Refresh** Button re-loads the web page in the browser. This can be used when a page is having trouble loading.

The **Home** Button will take you to your home page (for information on how to set this up, see setting your home page below).

The **Search** Button will give you quick access to the search facility in the browser. This is usually set to the Microsoft search site, which will appear in a pane on the right-hand side of the screen.

The **Favorites** Button opens your favorites in a pane on the right-hand side of the screen

The **History** Button opens your browsing history in a pane on the right-hand side of the screen.

The **Print** Button will print out a page (without you having to specify printing settings).

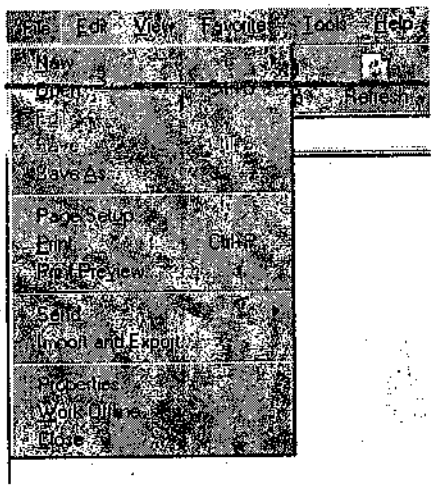
The **Mail** Button will start up an email program on your computer (if one is installed).

The **Edit** Button will start up a web page editing program, and load the page which is currently being displayed into it.

File Menu

Using this menu one can perform the following jobs on the basis of the options provided.

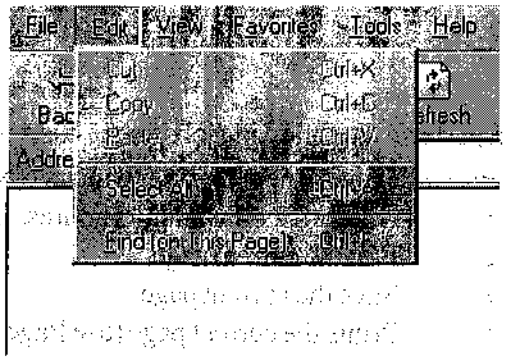
New : Opens a new browser window (New >window).
Open : Open a specific Internet address or a local file.
Edit : Edit the current page.
Save : Save the current page
Print : Prints the current page (use Page Setup to change printing settings).
Send : Send the page to someone via email.
Import and Export : Allows to import and export browser settings such as Favorites.
Properties : List The properties of the current displayed page, like page size, date created, Address of the page
Close : Closes the browser window



Edit Menu

Using this menu one can perform the following jobs on the basis of the options provided.

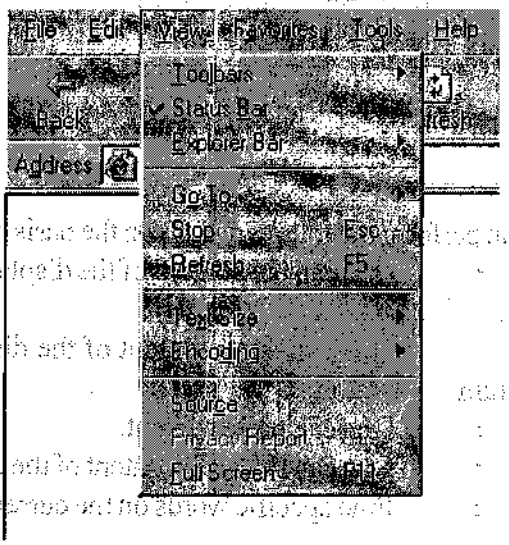
Cut : One can cut content of the displayed page so they can be copied to another program.
Copy : One can copy content of the displayed page so they can be copied to another program
Paste : One can paste content.
Select All : One can select all content of the displayed page.
Find : Find specific words on the current web page.



View Menu

Using this menu one can perform the following jobs on the basis of the options provided.

Toolbar	:	One can view the toolbars that are available in Internet Explorer
Status Bar	:	One can view the status of the web page being accessed
Explorer bar	:	One can change the icons on the Explorer bar
Go To	:	One can access (back and forward, home page, history)
Stop	:	One can stop the current downloading page
Refresh	:	One can reload the current displayed page
Text Size	:	One can manually change the text Size
Encoding	:	One can manually change the encoding of the page
Full Screen	:	One can view the browser in Full Screen mode (all the browser controls will disappear apart from a small toolbar).

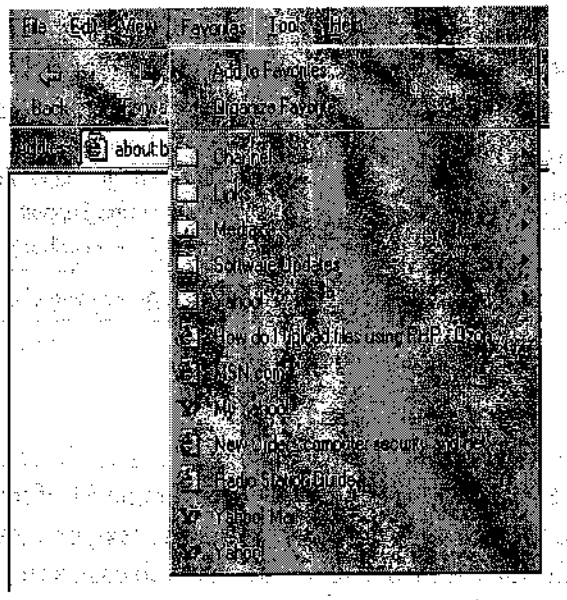


Favorites Menu

Using this menu one can perform the following jobs on the basis of the options provided.

Add : Add sites to your favorites list.

Organise : Organise your list of favorites by placing them in folders etc.



Tools Menu

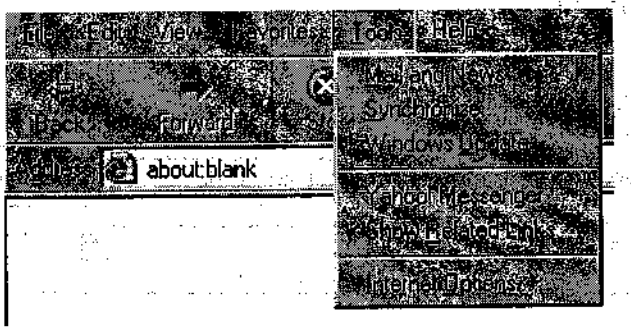
Using this menu one can perform the following jobs on the basis of the options provided.

Mail and news : Access any email or news reading programs you have on your computer.

Synchronise : Synchronies' the emails to outlook express if configured.

Windows Update : Downloads any updates if available for the browser

Internet Options : One can configure proxy, clear caches, browser security options



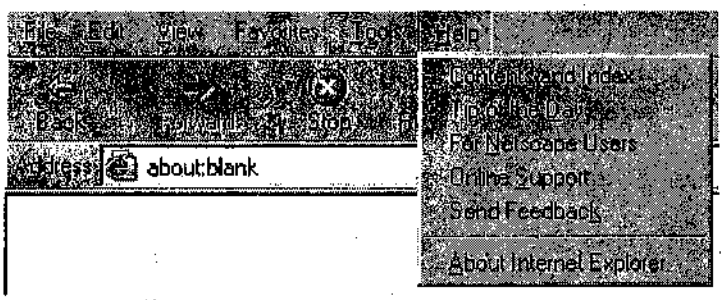
Help Menu

Using this menu one can

access the Help for the program.

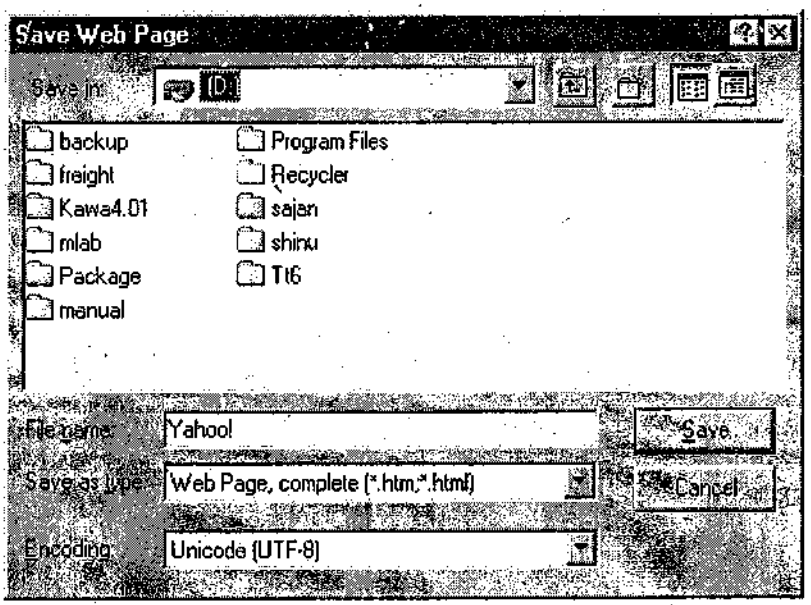
access online tours of the Internet and support site for Microsoft products

get information about the browser (version etc.)



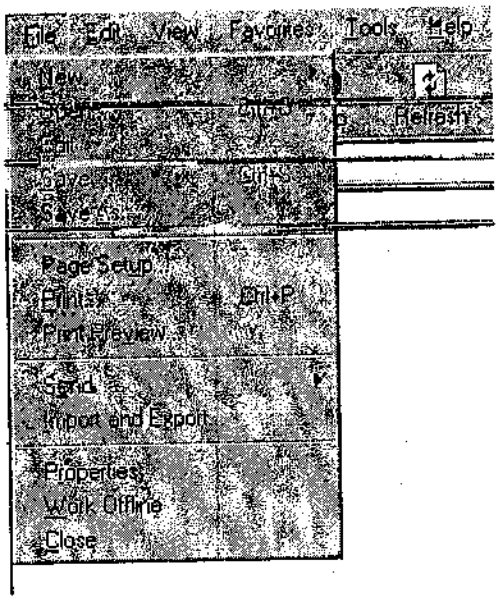
Saving web pages

Saving files from the web Saving web pages so they can be viewed when you are "offline" or stored on a local drive is quite simple if one is using version 5+ of Internet Explorer. Web pages are usually made up of a lot of different elements such as text, images, sound and video. Internet Explorer 5 saves all the files needed to reproduce the web page as it appears online in a folder so things like images will still be present in your local copy of the file. Internet Explorer 4, on the other hand, will only save the HTML file that brings all these elements together and formats them on the web page. This means that if one is using version 4, one will find that any images, sound, video, and even some of the functionality and formatting of a saved page is lost.



Printing web pages

To print a web page one either click on the print icon or choose the file menu and choose print. On click this option the current page will be printed on the default configured printer (To change print setting one needs to Page Setup).



7.6 USING A BROWSER FOR MAILS

Electronic Mail

Electronic-mail or Email is the process of sending messages anywhere electronically using the computer and a modem. Emails can be sent and received according to the convenience of the user. Any number of Emails can be sent at a time to any number of designated locations.

Email is delivered almost instantaneously. Email is cheap and easy to use especially for international messages. The cost of an Email is only the price of the telephone connection to the Internet Service Provider.

Use of E-mail

1. It is much cheaper to send an E-mail than a letter.
2. It is much cheaper than a long distance phone call.
3. It saves paper and raises productivity within the office environment.
4. Replies can be formulated at leisure and are easily sent (no searching for addresses).
5. Messages are usually delivered within minutes of being sent.

Email address

An email address is composed of two parts the user name and the domain in the format username@domain. Each email address uniquely identifies an Internet user.

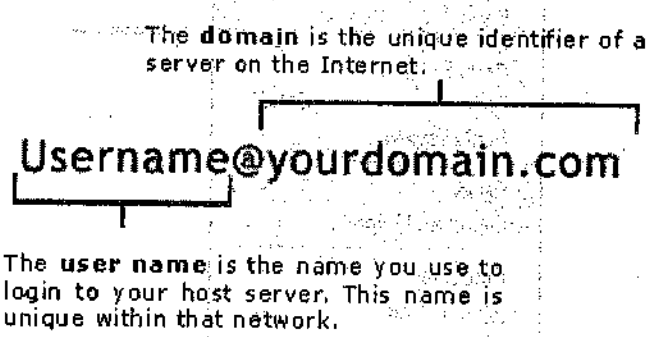
The user name is the name you use to login to your host server. This name is unique within that network. The domain is the unique identifier of a server on the Internet. Usually, an email address is not case sensitive.

Email Networks

Email Networks are nothing but a group of users who share common information with the help of emails. One can become a part of network by signing on to the network. After which one will receive or post queries or information to the user group or the email network.

Mail server

The mail server is a software residing on the server that acts as a collection point for incoming and outgoing E-mail for the users that it services. While the mail server will route outgoing E-mail upon receiving it from the user, it will store incoming E-mail till the user's mail client requests it to be downloaded and then deleted.



Email Headers.

Email have headers that provide information on the origin of a message and enable you to track and stop junk e-mail. Most e-mail clients only show the To: and From: headers, which can be easily forged. The complete message headers will look something like this:

Return-Path : [fake@address.com]

Received : from some.host.com (hostname [xx.xx.xx.xx])

by mydomain.com (8.9.3/8.9.3) with ESMTP id NAA123456;

Thu, 11 May 2002 10:15:30 +0530 (EDT)

Date: 11 May 2002 10:15:30 +0530

From : Spammer [junk@mydomain.com]

To : user@mydomain.com

Subject : My junk message!!

Netscape Mail (ver 4)

Click View from the pull-down menu bar. Then click Headers and Select All.

Outlook Express

Open the message. Then click File from the pull-down menu bar and select Properties. Another window with two tabs is displayed. To view the details, click the Details tab. Cut and paste the headers into the message that you want to forward.

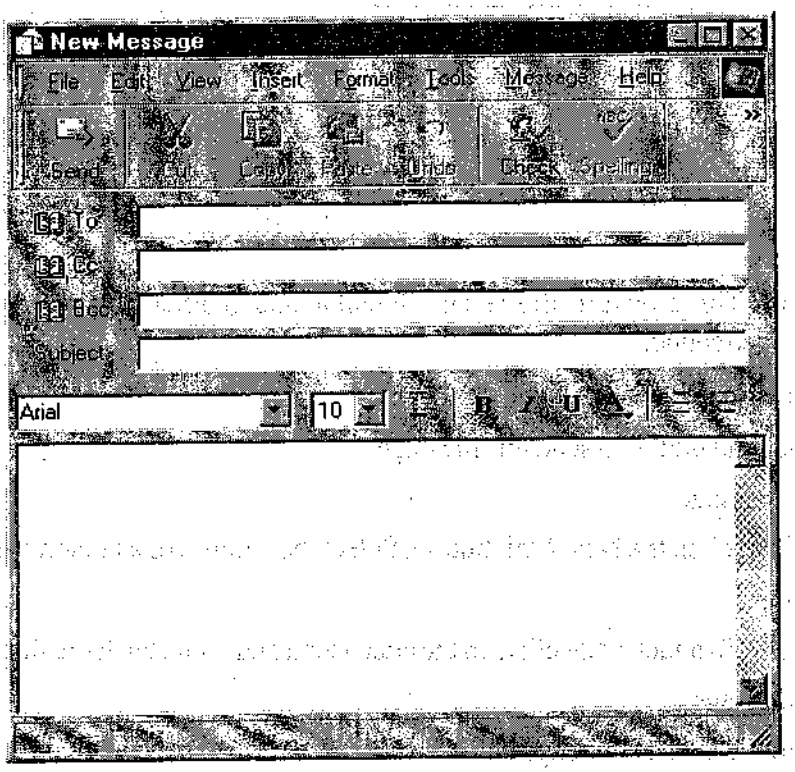
Email Structure

To: In this field you can type an address (or several addresses separating names with a comma or semicolon) to whom one would like to send a email to.

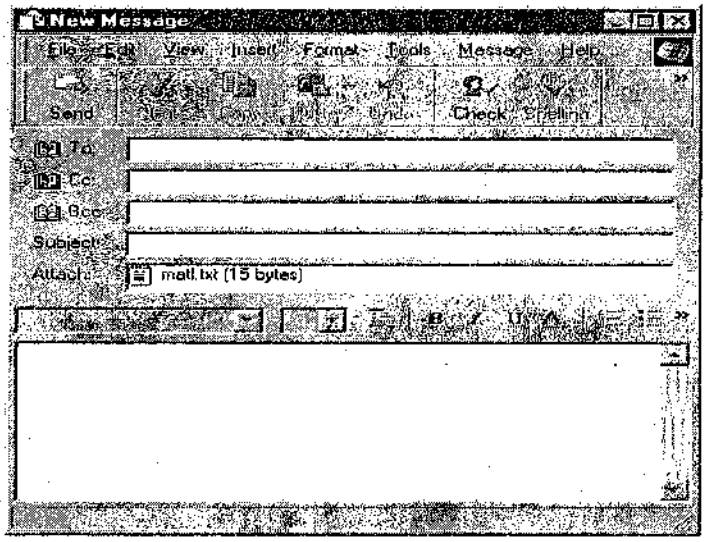
CC (carbon Copy): This will send a copy of the message to the address placed in this field and other recipients can see that the copy was sent.

BCC (Blind carbon Copy): This will send a copy of the message to the address placed in the field but other recipients do NOT see that the copy was sent.

Subject line: The subject should be short but descriptive. Some people filter their mail by subject so the subject line should be reflective of the contents of the message or the message may not be read by the recipient



(Body): You can type your message in the message field, copy text from another program and paste in the message field or embed a document in the message field. Notice that the font options (color, size, style) become active at this point. REMEMBER the recipients of your message using a different email program may not see text the same way you wrote it.



Attachment: This a feature allowed in a email to attach other files and documents such as text,audio,video sound.

Sending messages:

Click on the send button to send this message.

Start a new message:

On the toolbar, click the New Mail button. Select the address of a person to send to.

Type the subject

Attachments: To attach a file click on the attach icon and then attach the file.

Type your message.

Click on **send** icon. The message will be sent

7.7 SECURITY AND PRIVACY ISSUE

It very important to have the network secure. A list of the major challenges of Internet security and simple explanations of how they affect a network are explained below.

Protection from hackers on the Internet.

Hacker attacks can cause irrepairable damage to sensitive and confidential information. Critical data resides on a company's private network and businesses must actively prevent the theft, destruction and corruption of this information. For some companies, the confidential information residing on the business network belongs to corporate clients, raising issues of legal liability as well as financial loss.

Filter Inappropriate Materials.

The valuable information so readily available online also includes material inappropriate for the workplace, classroom, and home. Companies can face losses in productivity due to the vast array of non-work related material available at the click of a mouse. Objectionable content can create an uncomfortable work environment, creating a vulnerability to harassment lawsuits. Schools, libraries and home offices risk children accessing pornography or racially intolerant sites.

Protection Against Viruses.

Virus attacks are the greatest threat to Internet security today. The outbreak of viruses has increased in the past several years and statistics indicate that the number will continue to rise.

Protection from Active Content, such as ActiveX and Java.

ActiveX is a programming language that is used to embed small programs in Web pages. It is generally considered an insecure protocol to allow into a network since it is possible for malicious programmers to write controls that can delete files, compromise security, or cause other damage. Java is also used to embed small programs known as applets, in Web pages. It is generally considered safer than ActiveX, but some administrators may want to filter out Java since there have been instances of bugs in these safety mechanisms.

Following tool and application can use for security and privacy.

Firewall

A firewall protects a computers that are stand-alone's or a part of the local area network (LAN) against outside intrusion. Firewall's work as filters between the outside world and a private network. A firewall approves some types of traffic and blocks unauthorized users who attempt to access your network.

The term "firewall" is borrowed from architecture, but it doesn't actually refer to any one particular device. A firewall could be either a piece of hardware or software, and a network may use more that one type of firewall in order to provide extra security.

There are two common types of firewall:

A packet-filtering firewall applies predefined rules to filter the chunks of data, or packets, that pass through it. The filter accepts or rejects packets based upon the originating computer's network address or other characteristics. The packet filter may be a computer, or it may be part of a separate piece of hardware, such as a router.

A proxy server, also known as a gateway, acts as a middleman that relays data between the network and the outside world. The proxy prevents outsiders from gathering information about computers inside the network. The proxy can also screen packets based on their application type, such as Web access or email, or other identifying traits.

Anti virus

Anti virus software protect your computer from a variety of malicious software programs which are referred as virus. The anti virus companies is always on a lookout for these viruses and provide an immediate cure for the same.

These can include:

Viruses - They are small programs that attach themselves to other programs or documents and replicate with the potential to cause damage.

Worms - They are viruses that are specifically engineered to make extensive use of email to spread themselves rapidly.

Trojans - They are programs that appear harmless but have a damaging intent.

Zombies - They are programs that install themselves on computers and remain dormant until some external event triggers them into action. The actions could include corrupting, truncating, or stealing your information and sending it to a predefined email account or opening up remote control access portals to your machines.

SSL (Secure Socket Layer)

Customers visiting web sites may want to maintain their privacy when they register for a service online and in particular want to be assured that their credit card details are kept well away from crooks and fraudsters.

The most common means of achieving this privacy is through the use of SSL or Secure Socket Layer technology. When you connect to secure web space the data passing between your browser and the web site in question is encrypted which makes it virtually impossible for any third party to intercept the data that is being transferred. So whether your address or your credit card number that is being recorded it is strictly between you and the web site in question.

To gain certification for the security of your domain is a costly, complicated and time-consuming procedure.

This is where shared SSL is beneficial. It is seldom desirable to host the whole of your site on secure SSL servers as the extra complexity results in slower performance than you would get on "standard" hosting. So you can host the bulk of your site on normal shared hosting and use SSL secure hosting only for the sensitive functions such as customer registration and online payment.

Proxy server

A proxy server is an interface between the browser and the destination server. The proxy server receives the page request and handles the connection of the browser to the destination. These proxy servers are also able to cache pages. If such a proxy is configured to cache then it will first check the cache to see if the requested page exists. If the page is not found then the proxy server searches other caching proxy servers or makes a direct request to the destination. This process depends on the configuration for the proxy. The advantage of using a common caching proxy server is given by the probability to find a page in the local cache. The probability is in general expressed by the hit rate. A cache with several GB size and a lot of users can reach a hit rate of 30 to 40 percent. Frequently requested pages such as the help pages of your browser may be in the cache every time. In case the page is not in the local cache there is no difference in the elapsed time of a direct request or a request handled by a proxy server

7.8 TIPS FOR EFFECTIVE BROWSING/ DOWNLOADING/ COPYING FILES

There are a number of basic ways to access correct information on the Internet:

1. Go directly to a site if you have the address
2. Browse
3. Explore a subject directory
4. Conduct a search using a Web search engine
5. Query a service devoted to digitized scholarly materials or books
6. Explore the information stored in live databases on the Web, known as the "deep Web"
7. Join an e-mail discussion group or Usenet newsgroup
8. Subscribe to RSS feeds

TIPS ON CONDUCTING SEARCHES

1. Read the directions at each search site. The technique for formulating a search depends on the search engine you are using. There is a wide variety of options available among the different search engines.
2. If you have a multi-term search, be sure to determine which type of Boolean logic you should use. For example, a search about the relationship between latitude and temperature can be formulated as: +latitude + temperature on many Web search engines in order for AND logic to apply.
3. Include synonyms or alternate spellings in your search statements and connect these terms with OR logic.
4. Check your spelling.
5. Take advantage of capitalization if the search engine is case sensitive.
6. If your results are not satisfactory, repeat the search using alternative terms.
7. Try different sources to diversify your results. Sources can include other search engines and large directories.
8. Experiment with different search engines. No two search engines work from the same index.
9. Try search engines which allow you to search multiple search engines simultaneously. Be aware that you will lose access to advanced query options since not all engines offer them.
10. If you have too many results, or results that are not relevant:
11. Field search
12. Add concept words to your original search.
13. Use vocabulary that is specific to your topic; avoid words with large concepts unless you intend to field search.
14. Link appropriate terms with the Boolean AND (+) so that each term is required to appear in the record. While many search engines do not require this, it doesn't hurt to be on the safe side.
15. If one of your search terms is a phrase, enclose it within quotations.

7.9 SUMMARY

- World wide web is a part of internet that stores pages on website. Persons, Organizations can host websites. Other in the world can visit the site and read/download those pages.
- A Web browser is a program that you can use to view files on the Internet, including images,text, sound and video.
- The mail server is a software residing on the server that acts as a collection point for incoming and outgoing E-mail for the users that it services.
- URL is the abbreviation of Uniform Resource Locator. A URL is the global address of documents and other resources on the World Wide Web.
- HTTP, the Hypertext Transfer Protocol, is the application-level protocol that is used to transfer data on the Web.

- HTTP comprises the rules by which Web browsers and servers exchange information over a TCP/IP connection. An HTTP server is a program that listens on a machine's port for HTTP requests.
- Browser s a software in user's computer that helps in locating the website.
- A Search Engine is used to find information on the Internet when you don't know where to start. Search engines allow users to enter keywords to find Internet sites.
- Anti virus software protect your computer from a variety of malicious software programs which are referred as virus.
- A proxy server is an interface between the browser and the destination server. The proxy server receives the page request and handles the connection of the browser to the destination.

7.10 UNIT END QUESTIONS

1. What is world wide web?
2. What are the function of web browser?
3. What is URL?
4. What is Search Engine?
5. What is Email?
6. How would you get information using search engine?
7. What is the use of PROXY Server?
8. How would you copy data from web page?
9. What is the work of SSL?
10. What is the use of anti virus?

UNIT - VIII

APPLICATION OF INTERNET

STRUCTURE OF THE UNIT

8.0 Objectives
8.1 Finding and installing players
8.2 Plug-ins and activeX controls
8.3 Dealing with web pages that contain activeX,java,java Script
8.4 Playing streaming audio and video
8.5 Playing MP3 music
8.6 Using search engines
8.7 Making use of web resources
8.8 Summary
8.9 Unit end questions

8.0 OBJECTIVES

After going through this unit , you will be able to :

- Describe various internet application.
- To find and install players.
- Able to define the work of plug-ins and ActiveX controls.
- Defining streaming of audio and video.
- Plying mp3 music on audio players.
- Working of search engine .
- Working with various web resources like portal, news weather, sports, personal financing and investing, entertainment shopping, computers and internet, travels, health and medicine, communities and clubs.

8.1 FINDING AND INSTALLING PLAYERS

There are various audio and video plug-ins and ActiveX controls that can play various types of audio and video file formats which can be downloaded from the internet. We can find them on the internet by using search engine by putting the name of the player the in the text box of search engine.

Some Audio and video player

Real Player : It is also known as Real player. It can play most of the popular audio formats and video files, including streaming audio and video. Real player also supports burning of audio files on CDs, so a users can create their own music CDs. User can download real player from www.real.com .

Quick Time : It plays audio and video file stored in the QuickTime format . we can download windows or any other version of the quick time player from www.apple.com/quicktime.

Windows media player : It plays both regular and streaming audio and video files , including most audio file on CDs. It supports burning to CDs or copying files to portable media players that support WMA format. It is available with windows OS . we can also download it from www.microsoft.com .

VB Script can also set the attributes or properties of ActiveX Controls, Java applets, and other objects present in the browser. This way, you can change the behavior of plug-ins or other objects without having to rewrite them. For example, your VB Script code could automatically set the text of an ActiveX label control based on what time the page is viewed.

JavaScript

JavaScript is a script language from Netscape that is supported in Netscape Navigator from Version 2.0. It is easier to use than Java, but not as powerful. JavaScript uses the HTML page as its user interface, whereas Java can generate a completely custom interface. On the client, JavaScript applets are maintained in source code. On the server, they are compiled into byte code, similar to Java programs. A JavaScript applet can be used to display a data entry form and validate the input, while a Java program processes the information. JavaScript is also used to tie Java applets together.

JavaScript evolved from Netscape's Live Script language and was made more compatible with Java. Although it shares many of the features and structures of the full Java language, it was developed independently. JavaScript is endorsed by a number of software companies and is an open language that anyone can use without purchasing a license. It is supported by recent browsers from Netscape and Microsoft, though Internet Explorer supports only a subset, which Microsoft calls Jscript.

Java

Java is a language developed by Sun Microsystems which allows World Wide Web pages to contain code that is executed on the browser. Because Java is based on a single "virtual machine" that all implementations of java emulate, it is possible for Java programs to run on any system which has a version of Java. It is also possible for the "virtual machine" emulator to make sure that Java programs downloaded through the web do not attempt to do unauthorized things. Java is a full-blown object-oriented programming language developed by Sun Microsystems Inc. Java is an interpreted language. This means that in order for a Java program to run on a computer, a run-time system (interpreter) will need to have been installed on the computer.

The dynamism and interactivity is achieved by including links within an HTML page to Java programs called applets. When the link is clicked on, the Java applet is transferred to your computer and executed locally by the browser. Java will therefore eliminate the need for a client computer on the Internet to depend on the host computer for the execution of dynamic content.

Not only is Java poised to make the end user's life more interesting, but it also provides a powerful programming environment for the software developer and Internet content provider.

The Internet is a highly heterogeneous networked environment encompassing dozens of operating systems (Windows, Unix, Macintosh, OS/2, etc.) running on a wide variety of microprocessors. A Java program once developed is capable of running on EVERY platform which has the Java interpreter.

The implication of this portability is quite profound to the Internet programmer. The programmer no longer has to worry about developing different versions of an application to cater for the different computer platforms in use across the Internet. By programming in Java, only one application will need to be developed; it will then run on ALL platforms to which the Java interpreter is ported.

In order to use Java applets, you need to have associate files, which are compiled applet programs usually ending with .class. One applet may need one or more .class files to make it work. You can check with the sources where you obtain the applets and what .class files you need.

The default scripting language used for writing ASP is VBScript, although you can use other scripting languages like JScript which is Microsoft's version of JavaScript. ASP pages have the extension .asp instead of .htm. When a page with the extension .asp is requested by a browser the web server interprets any ASP contained within the web page before sending the HTML produced to the browser. In this way all the ASP runs on the web server and no ASP will ever be passed to the web browser.

Any web pages containing ASP cannot be run by just simply opening the page in a web browser. Web pages that contain ASP must be requested through a web server that supports ASP. If there is no Web server, then ASP pages cannot be displayed.

ASP was first introduced by Microsoft on it's web server Internet Information Server (IIS), that runs on Windows 2000/XP Pro/NT4. ASP pages run best on this Web server. The micro version of this server is called Personal Web Server (PWS). Both IIS and PWS are available free of cost with Windows.

We can locate these Web servers in the following places:

Windows 2000/XP Pro	- IIS can be found in 'Add/Remove Programs' in the 'Control Panel'.
Windows 98	- PWS can be found under 'add-ons' on the Windows 98 CD.
Windows NT4/95	- You can get hold of IIS by downloading the NT4 Option Pack from Microsoft (don't be fooled by the name as it also runs on Windows 95).
Windows ME	- IIS and PWS are not supported on this operating system.
Windows XP Home Edition	- IIS and PWS are not supported on this operating system.

VB Script

Like JavaScript, VB Script allows you to embed commands into an HTML document. When a user of a compatible Web browser downloads your page, your VB Script commands are loaded by the Web browser along with the rest of the document. The commands runs in response to a series of events. VB Script is an interpreted language. The browser interprets the VB Script commands when they are loaded and run. They do not need to be compiled into an executable form by the Web author who uses them.

VB Script is a fast and flexible subset of Microsoft's Visual Basic and Visual Basic for Applications languages. VB Script is designed to be easy to program in and quick in adding active content to HTML documents. The language elements are mainly ones that will be familiar to anyone who has programmed in just about any language, such as If...Then...Else blocks and Do, While, and For...Next loops, and a typical assortment of operators and built-in functions.

What VB Script Can Do

VB Script provides a fairly complete set of built-in functions and commands. These functions and commands allow you to perform math calculations, manipulate strings, play sounds, open up new windows and new URLs, and access and verify user input to your Web forms.

The code to perform these actions can be embedded in a page and executed when the page is loaded. You can also write functions that contain code that is triggered by events you specify. For example, you can write a VB Script method that is called when the user clicks the Submit button of a form, or one that is activated when the user clicks a hyperlink on the active page.

Winamp : It plays MP3 windows media files , as well as many other music formats, CD, and steaming audio and video. Winamp can be downloaded from www.winamp.com/download.

8.2 PLUG–INS AND ACTIVEX CONTROLS

A Plug-in is a program that can "plug into" your browser to give the browser a new capability. Plug-ins were invented for navigator browser, but most plug-ins work with the internet explorer too.

Internet Explorer stores all activeX controls and plug-ins in a single folder. In windows this folder is called C:\windows\downloaded program files or C:\winnt\downloaded.

Finding and installing plug-ins and ActiveX controls

All the web browsers are used to display text and graphics, but many web pages have non text information like audio files and video files animated graphics. Plug-ins or ActiveX controls developed to support all new type of information to play and display on the web page.

Many plug-ins and activeX controls are available for download from the web if a page contains information that requires a plug-in or activeX controls, the page usually also contains a link that leads to a page from which we can download what we need.

Various plug-in and ActiveX controls are available for windows and other operating system on the internet.

Some important Plug-ins and ActiveX Controls are below.

(1) **Adobe Acrobat Reader** : It displays portable document format files, documents that are saved with all of their formatting for uploading to the web.

(2) **Apple Quick Time** : Quick time is a standard audio and video it plays audio and video file .

(3) **Real One Player** : This plug-in plays Real Networks streaming audio and video files.

(4) **Shockwave and Flash** : These are the animation system from macromedia. Both widely used on the web. They display animated graphics, play sound, and interact with the web page.

Uninstalling Plug-ins and ActiveX Controls

Some times it is not easy to uninstall plug-ins and activeX controls or it is not possible to uninstall it. Some plug-ins come with uninstall programs but most do not have uninstall . To uninstall the plug-in and or ActiveX controls, select the control panel option in start button and then select the add/remove program icon and see whether the plug–in or activeX control is listed there or not.

8.3 DEALING WITH WEB PAGES THAT CONTAIN ACTIVEX,JAVA,JAVA SCRIPT

ASP(Active Server Pages)

Active Server Pages or ASP, as it is more commonly known, is a technology that enables you to make dynamic and interactive Web pages. ASP uses server-side scripting to dynamically produce web pages that are not affected by the type of browser the web site visitor is using.

8.4 PLAYING STREAMING AUDIO AND VIDEO

Streaming is a technology for playing audio and video files (either live or pre-recorded) from a Web page. A user can view the audio or video files directly from the Web server for immediate playback. This avoids time consuming downloads of large files.

When audio or video is streamed, a small buffer space is created on the user's computer, and data starts downloading into it. As soon as the buffer is full (usually just a matter of seconds), the file starts to play. As the file plays, it uses up information in the buffer, but while it is playing, more data is being downloaded. As long as the data can be downloaded as fast as it is used up in playback, the file will play smoothly.

8.5 PLAYING MP3 MUSIC

Mp3 is a compressed audio format that is used for storing audio data. Many music files are available on the internet in MP3 format, which has extension .mp3.

To play an MP3 format file, MP3 players are used , windows media player , winamp, real player etc are famous MP3 players used for playing mp3 file.

Finding MP3 music on the Web

In many players option is available to help in finding music on the internet. We can also find the MP3 sites using Search engine. There are so many site where user can file his favorite audio, video, music, song by paying some amount or free.

8.6 USING SEARCH ENGINES

Search Engine

A Search Engine is used to find information on the Internet when you don't know where to start.

A search engine is a program that can search the Web on a specific topic for you. By typing in a word or phrase (known as a keyword), the search engine will produce pages of links on that topic. Theoretically, the more relevant links are at the top of the list, but that is not always true.

- To find a Web site or Web page, the user just enters a word or phrase, called the keywords or search text, in the search engine's text box, and press enter, the search engine then displays a list of all the Web sites or Web pages that matches the keywords or search text entered.
- The URLs of several Internet search engines are listed below:

Search Engine	URL
AltaVista	www.altavista.com
Excite	www.excite.com
Google	www.google.com
HotBot	www.hotbot.com
Lycos	www.lycos.com
WebCrawler	www.webcrawler.com
Yahoo!	www.yahoo.com

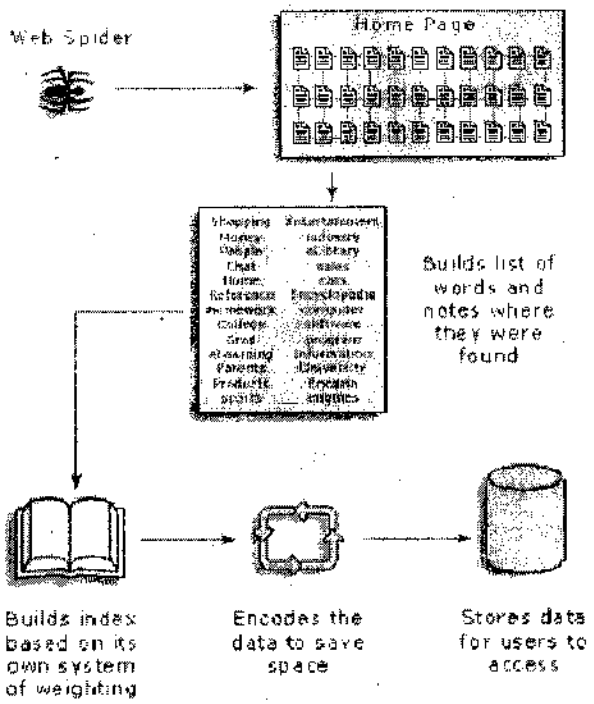
Metasearchers or Crawlers

Metasearchers or crawlers offer the possibility to do a search without having to consult every search robot separately. They function as an intermediary, by passing on the query to the search robots and afterwards order the results.

This happens in two ways:

The first type presents the various search robots together on one page, each with their own text box. The user subsequently chooses a particular search robot. The advantage of such a page is that you can immediately go back to the Metasearch page and choose another search robot.

The second type offers the possibility to type in a query once and then indicate in which database of which robot(s), the search is to be carried out. The query is then simultaneously submitted to the chosen search robots. The results are presented either in a long list, sorted according to the relevance or as a list per search robot that is then sorted according to relevance.



Search result Ranking

How does the search engine determine which query results to list first. Search engine have formulas they use to rank each page they index, and their ranking methods.

What are the Web Directories

A web directory is a web site that categorizes web pages so a user can browse link to web pages by topic for example , the yahoo web directory (WWW.yahoo.com) include category for arts and Humanities, Business and Economy ,Computers and internet ,Education and dozen other. Each of these major categories contains many subcategories : for example if you click the recreation and sports category , you find Sports, Games , Travel , Fitness ,Outdoors and many

more keep clicking categories to see subdirectory until you find the specific type of web page you are looking for.

The advantage of web directory over a search engine is that human being have categorized the web pages , so all the links in a category usually belong there.

Searching tips

Quotes

Placing words within quotation marks (") creates a phrase. The search engine returns a match only when the engine finds the exact word sequence. Example: "oracle India pvt. Ltd."

Asterisk

An asterisk (*) is also known as a wild card; it must be placed on the right-hand side of a word or embedded within a word. Normally sites require at least three characters to the left. You can use an asterisk to find various spellings or related words. Example: export* would return matches of export, exports, exporter,and exporting.

AND operator

Search results must contain all words joined by the AND statement. Example: commercial AND service.

AND NOT operator

Search results cannot contain the word that follows the AND NOT statement.

Example: software AND NOT integrator will find sites about software itself but eliminate sites about software integrator

OR operator

Search results must contain at least one of the words joined by the OR statement. Example: distributor OR agent lists sites that contain either word.

Plus

Adding a plus sign (+) directly in front of a word requires that the word be included in all search results. Place the plus sign between two words in a multiple wordsearch.

Example: export+assistance

Minus

Adding a minus sign (-) directly in front of a word indicates that the word should not be found in search results. Example: commerce -chamber

Parentheses

Use parentheses to build complex search queries that incorporate other special words and characters. Example: NAFTA AND (Canada OR Mexico) lists sites about either country pertaining to NAFTA.

8.7 MAKING USE OF WEB RESOURCES

Portal is a term, generally synonymous with gateway, for a World Wide Web site that is or proposes to be a major starting site for users when they get connected to the Web or that users tend to visit as an anchor site. To attract you, a portal site tries to have every thing , and all for free : Web guides, Search Engines, Chat rooms, e-mail accounts , Customizable Weather, and news Services etc. Some major general portals include Yahoo, Excite, Netscape, Lycos, CNET,

Microsoft Network, and America Online's AOL.com. Examples of portals include Garden.com (for gardeners), and SearchNetworking.com (for network administrators).

A number of large access providers offer portals to the Web for their own users. Most portals have adopted the Yahoo style of content categories with a text-intensive, faster loading page that visitors will find easy to use and to return to. Companies with portal sites have attracted much stock market investor interest because portals are viewed as able to command large audiences and numbers of advertising viewers.

Typical services offered by portal sites include a directory of Web sites, a facility to search for other sites, news, weather information, e-mail, stock quotes, phone and map information, and sometimes a community forum. Excite is among the first portals to offer users the ability to create a site that is personalized for individual interests.

8.8 SUMMARY

- A Plug-ins is a program that can "plug into " your browser to give the browser a new capability.
- Active Server Pages or ASP, as it is more commonly known, is a technology that enables you to make dynamic and interactive Web pages.
- A search engine is a program that can search the Web on a specific topic for you. By typing in a word or phrase (known as a keyword), the search engine will produce pages of links on that topic
- A portal site tries to have every thing , and all for free : Web guides, Search Engines, Chat rooms, e-mail accounts, Customizable Weather, and news Services etc.
- A web directory is a web site that categorizes web pages so a user can browse link to web pages by topic.
- Streaming is a technology for playing audio and video files (either live or pre-recorded) from a Web page. A user can view the audio or video files directly from the Web server for immediate playback.

Finding and installing players, plug ins and activeX controls dealing with web pages that contain activeX,java,java Script, playing streaming audio and video, playing MP3 music, using search engines, making use of web resources " portal , news weather, sports, personal financing and investing , entertainment shopping , computers and internet, travels, health and medicine, communities and clubs.

8.9 UNIT END QUESTIONS

1. What are plug-ins, how they are important?
2. What is ASP? Why it is important.
3. What is java? How it is important in web programming?
4. What is the use of Java Script and VB Script?
5. What is Search Engine?
6. What is the use of Portal?
7. What do you mean by Streaming? Explain.

UNIT - IX

E-COMMERCE

STRUCTURE OF THE UNIT

9.0 Objectives
9.1 Introduction to electronic commerce
9.2 Scope Applications, Feasibility and various constraints
9.3 Introduction to cyber laws, ethics & intellectual property rights.
9.4 Intellectual property rights
9.4 Summary
9.5 Hot Sites
9.6 Glossary
9.7 Unit end questions

9.0 OBJECTIVES

After going through this unit, you will be able to :

- Define Electronic commerce
- Define Scope of electronic commerce.
- Describe the trade cycle electronic market , and
- Electronic data interchange , internet commerce.
- Understand intellectual property rights.

9.1 INTRODUCTION TO ELECTRONIC COMMERCE

Electronic commerce or 'eCommerce' is the use of the internet for a range of business purposes, including:

- marketing and publicity
- online sales via the web
- communication
- business to business transactions

Marketing and publicity

The web is an ideal media for marketing and publicity because of it's potential reach to a global audience and it's capacity to support the use of images, animation, and audio/video. Many websites will carry advertisements for the web sites of sponsoring companies, which through the hyperlink system can be accessed simply by clicking on the advertisement.

Online sales through web

Improvements in security are leading to an increasing number of web-based services now being available for the buying and selling of goods. Most major high-street brands now have a website with facilities for ordering goods online. In addition, a number of companies have been established to trade solely via the web.

Communication

Many companies now rely on the internet for communication, both within the company and with customers. While this is typically through email, other facilities such as chat, instant messaging, web telephony and audio/video conferencing are also being used.

Business to Business transactions

Business to Business (B2B) transactions involves the direct trade between two companies, rather than between a company and a customer, for example exchanging information or transactions with a supplier. This may be through the use of an "extranet" (area of a website restricted to authorised people who logon with a password) which allows access to ordering product or accounting information specific to that company.

Concepts

Electronic commerce (e-commerce) is the use of telecommunications and data processing technology to improve the quality of transactions between business partners. It existed in some form since the invention of the telegraph and early automated data processing equipment but its use has greatly increased. E-Commerce improves organizational efficiencies by leveraging data processing, database storage, and data communications technologies. Existing network facilities can be utilized to achieve great savings in labour costs and the reduction of paper storage and handling facilities. It has enabled firms to be more effective in improving the quality of standard goods and services and to offer a variety of new services. The global marketplace has become larger and wider than ever because of the expansion of the e-commerce activity.

The growth of electronic commerce has been fueled by the availability of world wide telecommunication networks along with enhanced information delivery techniques utilizing the various multimedia technologies Client-server architecture allows systems with different hardware and software platforms to interact in an open system computing environment.

Technology in E-Commerce

Introduction

In any E-Commerce systems implementation, integration between business processes within a company and across companies is very important for a successful implementation. Within a company integration needs include interfacing with legacy systems, communicating with third party products, and integrating business processes across distributed E-Commerce systems. The two most commonly deployed technologies for this type of integration are ALE (Application Link and Enabling) and EDI (Electronic Data Interchange) technologies, which make use of the popular Idoc (Intermediate Document) interface for exchanging data.

EDI provides business process integration across companies by exchanging business documents such as purchase order. Invoices, and shipment notices in electronic form using industry standard formats such as ANSI X.12 (American National Standard's Institute) and EDIFACT (Electronic Data Interchange For Administration, Commerce, and Transport).

Electronic Data Interchange

EDI refers to electronic interchange of structured data via computer network . EDI is the transfer of information for processing between computer to computer.

The two aspects of EDI are :

- The information transmitted is directly used by recipient computer without the need for human intervention.
- EDI refer to interchange between 1. Two or more departments of the same Organization or two or more independent Organization.
- Business information is exchanged with each other without human intervention, using agreed formats and protocols.

Internet & E-business

Electronic commerce can be viewed from two business application perspectives. One perspective e-commerce in business is to look at those businesses engaged in providing electronic commerce technology to help enable other businesses. Internet Service Providers (ISP) and Private Commercial Network Providers help the companies into wide area networks (WAN) for use in e-commerce activity. They may offer additional features such as protocol conversion and are they described as Value- Added Network (VAN). Other types of firms specialize in helping organization build electronic commercial sites. Software firms sell data encryption and other types of security-related technologies, user interface programs and other types of software used to implement e-commerce. Other firms specialize in consulting and designing e-commerce applications such as World Wide web sites.

Another perspective on e-commerce is to examine the application uses to which a business uses such technologies. Linkages between business partners may be tightened through improvements in Just In Time (JIT) supply logistics overall improvement in supply chain management. Consumer marketing and sales techniques like shopping kiosks and home shopping techniques have removed barriers of distance and increased product awareness. Electronic publishing services, financial news and remote banking services are now available over networks. Commercial databases and library services provide general information resources. On line job placement services are numerous, and distance education and job training services can assist in career development. A wide variety of recreational and entertainment services are currently available and such services will expand dramatically in the near future.

Advantages of E-Commerce

The increased computerization of our society is triggering major changes in the organization of work. Paper driven processes are being reengineered to capture the benefits of doing business electronically. Businesses are implementing electronic commerce to meet the imperatives of an increasingly competitive world.

Electronic Commerce is the business environment in which information for the buying selling, and transportation of goods and services moves electronically. Electronic Commerce (EC) includes any technology that enables a company to do business electronically. Some of the direct benefits of Electronic Commerce are:

- Improved Productivity
- Cost Savings
- Streamlined Business Processes
- Better Customer Service
- Opportunities for New Businesses

Improved Productivity: Using electronic commerce, the time required to create transfer and process a business transaction between trading partners is significantly reduced. Furthermore, human errors and other problems like duplications of records are largely eliminated with the reduction of data-entry and re-entry in the process. This improvement in speed and accuracy plus the easier access to document and information, will result in increase in productivity.

Cost Savings: Based on the experience of a wide variety of early adopters of electronic commerce. Forrester Research has estimated that doing business on the Internet can result in cost savings of about 5% to 10% of sales. This cost savings steam from efficient communication quicker turnaround time and closer access to markets.

Streamlined Business Processes: Cost savings are amplified when business go a step further and adapt their internal processes and back-end legacy systems to take advantage of electronic commerce. Inventories can be shaved if businesses use the Internet to share such information as promotional plans, point-of-sale data, and sales forecasts. Business processes can also be made more efficient with automation.

Better Customer Service: With electronic commerce, there is better and more efficient communication with customers. In addition, customers can also enjoy the convenience of shopping at any hour, anywhere in the world.

Opportunities for New Business: Business over the Internet has a global customer reach. There are endless possibilities for business to exploit and expand their customer base.

9.2 SCOPE, APPLICATIONS, FEASIBILITY & VARIOUS CONSTRAINTS

The explosion in the use of the Internet/Intranet and its accessibility to individuals, corporations, and educational institutions. This revolution has dramatically changed the way of organizations conduct business with its consumers and with each other. The geographic boundaries, that offer limited access to goods and services, are crumbling and companies of all sizes are busy building commerce solutions and adapting to new ways of doing business. The internet/Intranet with inherent features like easy access, real-time information, and low cost, is a natural driver for commerce solutions. Further, companies enticed with the promise of the following competitive advantages are undertaking electronic commerce projects.

- Broader market reach
- Increased efficiency and accuracy through automated order-processing, inventory control billing, shipping, and so forth.
- Better customer service and support
- Instant communication with consumers and trading partners.
- Improved profit margins through automated supply chain management.
- Better forecasting of customer needs for goods and services
- Reduced labour costs
- Lower overall costs

Electronic commerce is often misunderstood to be limited to buying and selling of goods and services over the Internet. Actually, commerce solutions are a lot more than just the handling of business transactions and fund transfers over the Internet. It defines new forms of doing business. In addition To provid buying and selling services, commerce solutions can provide a complete system of services built into an organization's digital nervous system so it supports the sales processes and provides total account management.

9.3 INTRODUCTION TO CYBER LAWS AND ETHICS

Cyber Law

Cyber law encompasses a wide variety of legal issues related to the use of communications technology. It includes use of Internet as well as any other form of Computer or Digital Processing Devices. It includes intellectual property, privacy, freedom of expression, and jurisdiction.

Cyber Law addresses the issues of Virtual Property and Virtual Persons. It covers rights of Netizens who are the citizens of Cyber Space and regulation of the Cyber Space for a peaceful and harmonious existence of Netizens. The biggest challenge before Cyber Law is its integration with the legacy system of laws applicable to the physical world.

Since Cyber Space has no geographical boundaries, nor the Netizens have physical characteristics of Sex, Age etc, several conflicts surface when the rights of Netizens are viewed in the eyes of Citizens of a physical space. This is well reflected in the conflict between the Trade mark Laws and system of Domain Names.

There are several countries which have enacted special laws for regulating Cyber Space Transactions of Citizens within their Physical Jurisdiction and these are recognized as the Cyber Laws of the Physical Jurisdiction.

Computer ethics are the moral guidelines that govern the use of computers and information systems. Frequently concerned areas of computer ethics are

- Unauthorized access and use of computer systems
- Software piracy
- Information privacy
- Information accuracy
- Intellectual property rights
- Codes of conduct

9.4 INTELLECTUAL PROPERTY RIGHTS.

Intellectual property (IP) refers to work created by inventors, authors, and artists.

Intellectual property rights are the rights to which creators are entitled for their work.

A copyright gives authors and artists exclusive rights to duplicate, publish, and sell their materials. A common infringement of copyright is software piracy.

Copyright law usually gives the public fair use to copyrighted material (e.g., for educational purposes). However, this vague definition is always subject to widespread interpretation.

A trademark protects a company's logos and brand names. The controversy with trademarks often relates to domain names, when some people or smaller companies purposely acquire a domain name that uses the exact trademarked name of their competition.

9.5 Summary

- Electronic commerce or 'eCommerce' is the use of the internet for a range of business purposes, including:
    1. marketing and publicity
    2. online sales via the web
    3. communication
- Business to Business (B2B) transactions involves the direct trade between two companies, rather than between a company and a customer.
- Electronic commerce (E-commerce) is the use of telecommunications and data processing technology to improve the quality of transactions between business partners.
- In any E-Commerce systems implementation, integration between business processes within a company and across companies is very important for a successful implementation.
- EDI provides business process integration across companies by exchanging business documents such as purchase order.
- EDI refers to electronic interchange of structured data via computer network. EDI is the transfer of information for processing between computer to computer.

- Some of the direct benefits of Electronic Commerce are:
  1. Improved Productivity
  2. Cost Savings
  3. Streamlined Business Processes
  4. Better Customer Service
  5. Opportunities for New Businesses
- Cyber law encompasses a wide variety of legal issues related to the use of communications technology. It includes use of Internet as well as any other form of Computer or Digital Processing Devices. It includes intellectual property, privacy, freedom of expression, and jurisdiction.
- Intellectual property (IP) refers to the work created by inventors, authors, and artists.
- Intellectual property rights are the rights to which creators are entitled for their work.

9.6 Hot Sites

These sites take you to some of the major producers of computers, computer systems, and related hardware and software.

COMPUTER SYSTEMS

IBM

http://www.ibm.com

Apple Computer

http://www.apple.com

Sun Microsystems, Inc.

http://www.sun.com

Digital Equipment Corporation (DEC)

http://www.dec.com

Compaq

http://www.compaq.com

Printers

Hewlett-Packard

http://www.hp.com

Modems

US Robotics

http://www.usr.com

Hayes

http://www.hayes.com

Practical Peripherals

http://www.practinet.com

MAJOR SOFTWARE CORPORATIONS

Microsoft

http://www.microsoft.com

Adobe Systems Incorporated

http://www.adobe.com

INTERNET SITES

This section contains Internet-related World Wide Web sites.

Browsers and Plug-Ins

Netscape Communications

http://www.netscape.com

Microsoft Internet Explorer

http://www.microsoft.com/ie/

Search Engines

Yahoo!

http://www.yahoo.com

Infoseek

http://www.infoseek.com/

AltaVista

http://www.altavista.digital.com/

WebCrawler

http://www.webcrawler.com/

Google

http://www.google.com/

People Finders

InfoSpace

http://www.infospace.com

WhoWhere?

http://www.whowhere.com

America Directory Assistance

http://www.lookupusa.com/lookupusa/adp/peopsrch.htm

Broadcast Media

This list of sites covers everything from network TV to cable to the movies.

Network TV

ABC

http://www.abc.com

Fox

http://www.foxworld.com

Cable TV

Cinemax

http://www.cinemax.com

The Disney Channel

http://www.disney.com/DisneyChannel/

ESPN

http://www.espn.com

Movie Studios

MCA/Universal

http://www.mca.com

Sony Pictures

http://www.spe.sony.com/Pictures/SonyMovies/index.html

20th Century Fox

http://www.tcfhe.com

Walt Disney Studios

http://www.disney.com/DisneyPictures/

9.7 Glossary

Advanced Research Projects Agency Network (ARPANET)

A pioneering long-haul network funded by what's now-called DARPA (formerly known as ARPA). It was the foundation on which the Internet was built.

Application

Sometimes known as a client or an "app," it's a program that performs a specific function. FTP, Mail, Gopher, Mosaic, and Telnet clients are the most common examples of Internet applications.

Archie

You'll usually hear this term referred to in the phrase "archie search." Archie is a way of automatically gathering, indexing and sometimes even retrieving files on the Internet. Most good archie clients are able to FTP files once you've found the information you're looking for.

Archive

A collection of files stored on an Internet machine. FTP sites are known as archives.

Arpanet

See Advanced Research Projects Agency Network.

Asynchronous Transfer Mode (ATM)

A transfer method that dynamically allocates bandwidth using a fixed-size "packet," or "cell." Also known as "fast packet."

Authentication

Any process that ensures that users are who they say they are. When you type your name and password, you are authenticated and allowed access.

Bandwidth

This refers to the difference (measured in Hz), between the highest and lowest frequencies of a transmission. Most people loosely refer to bandwidth as the amount of data that can be transferred over a network connection.

Bitmap

A representation, consisting of rows and columns of dots, of a graphics image in computer memory. The value of each dot (whether it is filled in or not) is stored in one or more bits of data. For simple monochrome images, one bit is sufficient to represent each dot, but for colors and shades of gray, each dot requires more than one bit of data.

Browser

A software program that allows users to access the Internet.

Chat

Another term for IRC . Also, an acronym meaning "Conversational Hypertext Access Technology."

Corporation for Research and Educational Networking (CREN)

An organization formed in October 1989, when Bitnet and CSNET were combined. CSNET is no longer around, but CREN still operates Bitnet.

Cyberspace

The "world of computers and the society that gathers around them," as referred to by William Gibson in his fantasy novel "Neuromancer." It now loosely refers to the online world and even more loosely to the Internet.

Datagram

A block of data that is "smart" enough (actually, which carries enough information) to travel from one Internet site to another without having to rely on earlier exchanges between the source and destination computers.

Dialup

A widely-used method of accessing the Internet. A dialup connection uses regular phone lines to connect one computer to another via modem.

Domain

A "logical" region of the Internet. People sometimes refer to them loosely as "sites." Generally, a domain corresponds to an IP address or an area on a host.

Domain Name System (DNS)

The DNS is a static, hierarchical name service used with TCP/IP hosts, and is housed on a number of servers on the Internet. Basically, it maintains a database for figuring out and finding (or resolving) host names and IP addresses on the Internet. This allows users to specify remote computers by host names rather than numerical IP addresses (if you've used UNIX, you may have heard the DNS referred to as the BSD UNIX BIND service). For example, go to a DOS prompt in Windows 95, the % prompt in UNIX, or use a ping client for Windows 3.1 or Mac, and type "PING UTW.COM". This will check the DNS server you have configured, look up the numerical IP address for UTW.COM, and then ping UTW's IP address. The advantage of the DNS is that you don't have to remember numerical IP addresses for all the Internet sites you want to access.

Electronic Mail (Email)

A method by which computer users can exchange messages with each other over a network. Email is probably the most widely-used communications tool on the Internet. There are many quirky conventions to Email, but most entail a "To:", "From:", and "Subject:" line. One of Email's

advantages is its ability to be forwarded and replied to easily. If an email is badly received by a group or user, the sender is likely to get "flamed."

Encryption

The basis of network security. Encryption encodes network packets to prevent anyone except the intended recipient from accessing the data.

FAQ

Acronym for "Frequently Asked Questions." FAQs are widely available on the Internet and usually take the form of large, instructional text files. They are written on a wide variety of topics, and are usually the most up-to-date source for specialized information.

File Transfer Protocol (FTP)

The most widely-used way of downloading and uploading (getting and putting) files across an Internet connection. The File Transfer Protocol is a standardized way to connect computers so that files can be shared between them easily. There is a set of commands in FTP for making and changing directories, transferring, copying, moving, and deleting files. Formerly, all FTP connections were text based, but graphical applications are now available that make FTP commands as easy as dragging and dropping. Numerous FTP clients exist for a number of platforms.

Firewall

The name "firewall" derives from the term for a barrier that prevents fires from spreading. A computer "firewall" is a barrier between your computer and the outside world. Just like a fire is most likely to spread through open doors in a building, your computer is most vulnerable at its ports (the doors). Without ports you could not go on the Internet or let Internet traffic enter your computer.

An effective software firewall isolates your computer from the Internet using a code that sets up a blockade to inspect each packet of data, from or to your computer to determine whether it should be allowed to pass or be blocked.

Firewall software operates in various ways: Packet filters block traffic from IP addresses and/or port numbers. Proxy servers can break the connection between two networks. NATs (Network Address Translators) hides the IP addresses of client stations by presenting one IP address to the "outside" world. Stateful inspection verifies inbound and outbound traffic to be sure the destination and the source are correct. Firewall software can allow your computer to operate in stealth mode, so that its IP address is not visible.

Gateway

A kind of "go-between" device or program that passes information between networks that normally couldn't communicate. What used to be called a gateway is now called a router. Not to be confused with a protocol converter.

Gopher

An information search and retrieval tool used widely for research. Gopher information is stored hierarchically on computers across the Internet. It uses a simple protocol that allows a client to access information from a multitude of numerous Gopher servers at one time, creating what's known as "gopher space." The most common search tools in gopher are Veronica and Jughead. Gopher clients exist for most platforms.

Hacker

A computer user who works to understand the "ins and outs" of computers, networks, and the Internet in general. Hackers are generally benign, and are not to be confused with crackers.

Host

A computer that is attached to a network or the Internet. Hosts allow users on client machines to connect and share files or transfer information. Individual users communicate with hosts by using client application programs.

Host Address

The address of a host computer on the Internet.

Hostname

The name given to a host computer connected to the Internet.

HTML

HyperText Markup Language.

Hypermedia

The combination of hypertext and multimedia in an online document.

Hypertext

A type of text that allows embedded "links" to other documents. Clicking on or selecting a hypertext link displays another document or section of a document. Most World Wide Web documents contain hypertext.

Hypertext Markup Language (HTML)

The standard way to mark text documents for publishing on the World Wide Web. HTML is marked-up using "tags" surrounded by brackets. To see what tagged HTML text looks like, select the View Source feature from the menus in the program you are using to view this document now, and you'll see a display of the HTML text used to create this page.

Integrated Services Digital Network (ISDN)

A relatively new technology which combines voice and digital network services in a single medium. ISDN makes it possible for communications carriers to offer their customers digital data services as well as voice connections through a single line. CCITT defines the standards relating to ISDN.

International Organization for Standardization (ISO)

An organization of 89 member countries (founded in 1946) responsible for setting world standards in many electronics areas. Members of the ISO are the national standards organizations of the member countries.

Internet

A large, uncontrolled, unadministered, anarchic cyber-state that will soon take over the world! Basically, it's just everyone's computers hooked together. It's not a corporation, organization, or entity in itself. When you connect to the Internet, you actually become part of it. Always capitalized, the word Internet can also be referred to colloquially as the "Net."

Internet Protocol (IP)

An industry standard, connectionless, best-effort packet switching protocol used as the network layer in the TCP/IP Protocol Suite.

Internet Protocol Address (IP Address)

The 32-bit address defined by the Internet Protocol. Every resource on the Internet has a unique numerical IP address, represented in dotted decimal notation. IP addresses are the closest thing the Internet has to phone numbers. When you "call" that number (using any number of connection methods such as FTP, HTTP, Gopher, etc.) you get connected to the computer that "owns" that IP address.

Internet Service Provider (ISP)

An ISP is a company that maintains a network that is linked to the Internet via a dedicated communication line, usually a high-speed link known as a T1. An ISP offers use of its dedicated communication lines to companies or individuals (like me) who can't afford 1,300 a month for a direct connection. Using a modem, you can dial up to a service provider whose computers will connect you to the Internet, typically for a fee.

IRC

The world-wide "party line" of the '90s. IRC allows multiple users to converse in real time on different "channels." Channels (which have a "#" sign preceding their name) vary in traffic and content. Channel operators (or Ops) moderate the conversation, and have the ability to "kick" people from channels, or even ban them if their actions warrant it. IRC clients are available for nearly all platforms.

LAN

Acronym for "Local Area Network." LANs are now commonplace in most businesses, allowing users to send email and share resources such as files, printers, modems, etc. Currently, most larger companies are connection their LANs to the Internet, allowing users to connect to resources within or outside the LAN.

Leased Line

A dedicated, full-time connection used to link a user or network to an Internet Service Provider or another network.

Mailing List

A list of email addresses used to forward messages to groups of people. When you subscribe to a mailing list, you receive all mail sent to that list.

Mosaic

A graphical browser for the World Wide Web that supports hypermedia. The NCSA (National SuperComputer Association) invented the Mosaic browser, which quickly became the industry standard. Recently, however, Netscape Communications has stormed the market with its freeware release of their Netscape Browser, which has radically redefined the Web. The term "Mosaic" is sometimes used incorrectly as a synonym for the World Wide Web.

Multipurpose Internet Mail Extensions Encoding (MIME Encoding)

MIME is a standardized method for organizing divergent file formats. The method organizes file formats according to the file's MIME type. When Internet (usually email) software retrieves a file from a server, the server provides the MIME type of the file, and the file is decoded correctly when transferred to your machine.

Network File System (NFS)

A protocol developed by Sun Microsystems. NFS allows a computer to access and use files over a network as if they were local. This protocol has been incorporated into the products of more than two-hundred companies, and is now a de facto Internet standard.

Open Systems Interconnection (OSI)

A suite of protocols, designed by ISO committees to be the international standard computer network architecture.

Packet Internet Gopher (PING)

The simplest way to test or time the response of an Internet connection. PING sends a request to an Internet host and waits for a reply (called a...yep.. you guessed it: PONG). When you PING an address, you get a response telling you the number of seconds it took to make the connection. PING clients exist for a number of platforms, or you can use a UNIX or Windows 95 prompt to issue a PING command directly.

Point-to-Point Protocol (PPP)

A protocol that provides a method for transmitting packets over serial point-to-point links. PPP is one of the most popular methods for dialup connections to the Internet, since it allows you to use other standard protocols (such as IPX, TCP/IP, and Netbeui) over a standard telephone connection, but it can also be used for LAN connections.

Portal

A Web site "gateway" that provides multiple services, which could include Web searching capability, news, free-email, discussion groups, online shopping, references and other services. A more recent trend is to use the same term for sites that offer services to customers of particular industries, such as a Web-based bank "portal," on which customers can access their checking, savings and investment accounts.

Post Office Protocol (POP)

A protocol designed to allow single users to read mail from a server. There are three versions: POP, POP2, and POP3. When email is sent to you, it is stored on the server until accessed by you. Once you are authenticated, the POP is used to transmit the stored mail from the server to your local mailbox on your client machine.

Protocol

Simply, the "language" spoken between computers to help them exchange information. More technically, it's a formal description of message formats and the rules that two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces (like the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (the way in which two programs transfer a file across the Internet).

Router

A device that forwards traffic between networks. Forwarding decisions are made based on network layer information and routing tables, often constructed by routing protocols.

Search Engine

specialized software, such as AltaVista and Yahoo, that lets WWW browser users search for information on the Web by using keywords, phrases, and boolean logic. Different search engines

have different ways of categorizing and indexing information. Search engines are accessed by typing in the URL of that engine or using a browser's compilation of search engines in its Internet search function.

Serial Line Internet Protocol (SLIP)

Similar to PPP, SLIP is another standard protocol used to run TCP/IP over serial lines, such as telephone circuits or RS-232 cables. Unlike PPP, however, SLIP does not work on a LAN connections. SLIP is probably the most popular way for dialup users to access the Internet.

Server

Simply, a computer that provides resources, such as files or other information. Common Internet servers include file servers and name servers Domain Name Service.

Simple Mail Transfer Protocol (SMTP)

A protocol used to transfer email. SMTP transfers mail from server to server, and the end user must use POP (see also Post Office Protocol) to transfer the messages to their machine.

Simple Network Management Protocol (SNMP)

Developed to manage nodes on an IP network, SNMP is an Internet standard protocol. It can be used to manage wiring hubs, video toasters, CD ROM jukeboxes, and many other devices.

Smiley

The use of punctuation marks and other symbols or characters to portray moods when typing, especially in email messages and IRC. Here's an example of a simple smiley :) . If you don't see it, tilt your head to the left and look at it. The colon makes the eyes and the parenthesis makes the smiley mouth. The smile means happiness (like if someone says something funny) or it often denotes sarcasm. Other combinations of characters can express many other emotions. You may also hear them referred to as "emoticons".

Telnet

The Internet standard protocol to connect to remote terminals. Telnet clients are available for most platforms. When you Telnet to a UNIX site, for example, you can issue commands at the prompt as if the machine were local.

Topology

The "layout" of all the computers on a network and the links that join them.

Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP is the standard communications protocol required for Internet computers. To communicate using TCP/IP, PCs need a set of software components called a TCP/IP stack. Macintoshes typically use a proprietary software called MacTCP. Most UNIX systems are built with TCP/IP capabilities.

Usenet

Usenet groups are more commonly known as "newsgroups." There are thousands of groups hosted on hundreds of servers around the world, dealing with various topics. Newsreader software is required to properly download and view "articles" in the groups, but you can usually "post" and article to a group simply by emailing to it.

Veronica

A search engine (not unlike Archie) that is built into Gopher. It allows searches of all gopher sites for files, directories and other resources.

Universal Resource Locator (URL)

More commonly referred to as the URL, the Universal Resource Locator refers to the entire address that is recognized "universally" as the address for an Internet resource. Each resource on the Internet has a unique URL. URLs begin with letters that identify the resource type, such as http, ftp, gopher, etc. These types are followed by a colon and two slashes. Next, the computer's name is listed, followed by the directory and filename of the remote resource. For example, the URL for this glossary is http://www.windows95.com/glossary.html.

World Wide Web (WWW)

The "Web" is a collection of online documents housed on Internet servers around the world. The concept of the Web was created by researchers at CERN in Switzerland. Web documents are written or "coded" in HTML. To access these documents, you have to use a Web browser, such as Netscape or Mosaic. When these browsers access (or hit) a page, the server uses the HyperText Transfer Protocol (HTTP) to send the document to your computer.

9.8 Unit end questions

1. Define and explain E-Ccommerce.
2. Describe Electronic Data Interchange (EDI.).
3. Describe Typical business transaction using internet.
4. How E-Business support the internet?
5. What are the advantages of E-Commerce?
6. What is Cyber law?
7. What do you mean by Intellectual Property Rights?

UNIT - X

CREATING AND MAINTAINING WEB SITES

STRUCTURE OF THE UNIT

10.0 Objectives
10.1 Development Tools
10.2 Planning
10.3 Elements of a web Page and creation of web pages
10.4 Summary
10.5 Unit end questions

10.0 OBJECTIVES:

This unit will explain how to develop a Basic HTML Web page and how to run the web page, it covers all the basic elements that are to put on to a web page. It also explains the different advanced tags that are to be placed on web page to make it attractive and simple for the user. This unit will cover the different parts of web page i.e. body section, head section etc. It also explains the tags and their attributes. This unit will also helps you to get the knowledge of frames and forms which are very useful for web page presentation. At the end you will be able to design a web page of your own using different HTML tags. So,have a nice tour to this unit.

10.1 Development Tools

Many Tools are available for the development of websites. We have to choose from them any one method for making websites but for that we have to plan the development process and then choose the language or tool for making web sites.Different tools available are Front page, Dreamweaver for fast development of web pages and HTML is used in all these tools.

10.2 Planning

The process of choosing among competing opportunities for communication so that overall goals for the web can be set. These goals include anticipating and deciding on the targets for the audience, purpose and objective for the information. Planning also is done for domain information through a process of defining and specifying the supporting information that must be collected, how it will be collected and how the information will be updated. If a specification for a design calls for using a form interface. For example, the web planner must identify the need for web implementation to have these skills

HTML is the basic tool for designing a web page. HTML is the acronym for Hyper Text Markup Language. It is a documentation language to mark the headings, title, table and forms.

10.3 Elements of a Web Page

HTML TAGS

When a web page is to be developed, the following are to be planned:

- Content of the page
- Appearance of the page

The appearance of the page is coded in HTML language using HTML tags.

HTML Tags and their Attributes

An HTML tag is a word specifying the appearance of the content. The following are the sailent features of an HTML tag:

- A tag is enclosed between the < and > symbols. Examples are <head>, <h1>, <ol>.
- Most of the tags have end tag, which begin with </. For example </h1> is the end tag for <h1>.

A tag may have some attributes. Attributes are the properties of the tag. This tag contains the following attributes:

1. Size(thickness of the line)
2. Width
3. Alignment

These are represented as follows:
<hr size=10 width=25% align = LEFT>

HTML Documents

Every html documents begins with the <html> tag and ends with the corresponding end tag </ html>. A document has the following two sections:

1. Head
2. Body

Header Section

Every HTML document must have head section which begins with the tag <head> and ends with </head>. The following are some important components of the head section.

1. Title
2. Prologue
3. Links

Title Tag

The title is the heading that appears as the title of the window. It is enclosed between the tags <title> and </title>.

Prologue

Prologue is only a comment, which can tell about the HTML version that is adopted for preparing the document. A prologue is given as shown below:

<! Doctype HTML 4.0 >

LINKS

The link tag can be used for the following purposes:

- To inform the browser the previous document
- To inform the browser the next document
- To link the banner
- To inform the location of the base document location

Previous and Next Attributes

The HTML document can be placed in between two HTML document using link tag. Suppose we want to assign a HTML document nov2002. html as the previous document and jan2003. html as the next document. We define as follows:

<head>

<title>travel in december 2002 </title>

<link rel = previous href = "nov2002. html">

<link rel = next href = "jan2003. html">

</head>

Banner attribute

A banner is a fixed part of the page that will stay on the screen when we scroll the text of the page. The emblem of the company, or the title of the company can be a banner. For example, Suppose logo.html is a HTML document which shows the emblem of the college.

<head>

<title> travel in December 2002 </title>

<link rel = banner href = "logo.html">

</head>

Body section

The body begins with <body> and ends with </body>. The following is a simple template for creating a HTML document.

<html>

<head>

<title>

The title appears here

</title>

</head>

<body>

.....

.....

</body>

</Head>

</HTML>

The <body> tag has several attributes. The following is a partial list.

- Background design (background)
- Background color (bgcolor)
- Text color (text)
- Link color (link)
- Active link color (alink)
- Visited link color (vlink)

Use of Link Documents using Anchor Tag

When a page is shown, some of its words may need further explanations. Such words are called hot text or link and they appear in a different color. when we click it, another HTML file will be opened and that will have the required explanation. A hot text is created with anchor tag <a>. For example, if a hot text United States of America is to be created with a html document us.html, we must type as

 United States of America

Here the anchor tag <a> has an attribute href. This attribute specifies the name of the document to be opened.

For example, a HTML file travel.html is shown below. It contains details about the travel made.

<html>

<head>

<title>Travel in December 2002 </title>

</head>

<h1>Travel Details </h1>

<hr>

<h3>December 28, 2002 United States of America </h3>Quartely Meeting with Bank of America

<h3> December 29, 2002 Canada </h3> Meeting with Branch Officers Managers

</body>

</HTML>

FORMATTING CHARACTERS

In a web page the characters can be bold, italics, underline etc. by using some HTML tags. There are two methods of formatting characters. They are,

1. Logical styles
2. Physical styles

Logical styles

The logical styles inform the browser what kind of text to present. The browser takes care of how to present it. For example, consider the tag. This tag tells that emphasis must be given. Table lists the logical styles tags.

Logical Styles Tags

Tag	Meaning
....	Basic emphasis. Normally rendered in italics style.
..	Strong emphasis. Normally rendered in bold style.
<dfn>... .</dfn>	Defining instance of the enclosed team.
<code> </code>	Extracts of program code.
<samp>. .</samp>	Sample outputs from Program, scripts etc.
<kbd>... .</kbd>	Text to be typed by the user.

<var>... .</var>	Variables or arguments to command.
<cite>... .</cite>	Citation or reference to other sources.

Physical Styles Format

The physical styles format tags explicitly informs the browser how the characters must be shown, bold, italics etc. the physical styles tags are shown in Table

Physical Styles Tags

Tag	Meaning
.....	**Bold face**
<I>.....</I>	*Italics*
<tt>.....</tt>	Teletype
<u>..... .</u>	Underline
<strike>..... ..</strike>	Strike through
_{..... .}	subscript
^{..... .}	Superscript
<big>.....</big>	Larger font
.....	Smaller font

Font Tag

The tag is used to set a specific font and size. It usually has two attributes, namely face and size.

For example, consider the following:

Web Technology book by Dr. C. Xavier

Images and Pictures

A picture or an image in the web page can be inserted using the <img>tag. The <img>tag has several attributes to inform the source, height of the picture, width of the picture alignment etc. the following are of its important attributes:

- Citation or reference to other sources. src
- Height
- Width
- Align
- Alt

The src attribute specifies the source of the picture. It gives the file name of the picture file. The height and the width may be expressed in terms of either pixels or percentage or in units. The default is the pixels. For example consider the following:

<img src="companylogo.gif" height="100" width="120">

The align attribute can be used to align the picture.

Listing

This section introduces two more tags <ol> and <ul> that lists a set of items either with serial numbers or with bullets. They are called Ordered and Unordered lists.

Unordered Lists

The unordered list is represented by tag and tag. is given at the beginning and tag is given at the end. Each list item is given <li> tag. In the unordered list, every list has a circle or square as its bullet. The bullet can be any one of the following symbols:

- Disc
- Circle
- Square

The symbols that we want to include can be chosen using type attribute of <UL> tag. For example suppose we use <ul type = square> we shall get square symbol. If we use <ul type = circle> we shall get the circle. We shall get a disc as the bullet if we give the <ul> tag as <ul type = disc>.

The following is an example:

```
<html>
<head>
<title>
Unordered List
</title>
</head>
<body>
<h1>Places Visited</h1>
<ul>
<li>United States of America
<li>Canada
<li>Brazil
<li>United Kingdom
</ul>
</body>
</html>
```

Ordered Listing

The ordered list is represented by <ol> in the place of <ul>. Consider the following:

```
<html>
<head>
<title>
Unordered List
</title>
</head>
<body>
<h1>Places Visited</h1>
```

```
<ol>
<li>United States of America
<li>Canada
<li>Brazil
<li>United Kingdom
</ol>
</body>
</html>
```

Inserting Tables in HTML

In HTML the beginning of a table is marked by <table> tag and the end is marked by </table> tag. If we want a border for our table, we must give the beginning tag as

<table border>

If we want a bigger border we can also give numbers to represent the size of the border. For example,

<table border = 5> will give a bigger border.

The following is an example.

```
<html>
<head>
<title>
Table showing the Places visited
</title>
</head>
<body>
<table border=5>
<caption><b>Places Visited</b></caption>
<tr>
<th>Date <th>Country <th>Purpose
<tr>
<td>Dec 28,2002<td>USA <td>Quarterly Review Meeting
<tr>
<td>Dec 29,2002<td>Canada <td>Branch Managers Meeting
</table>
</body>
</html>
```

Check Your Progress:

1.1 Design a HTML page describing your Profile in one paragraph. Design in such a way that it has a heading, a horizontal rule, three links and your photo. Also, write three HTML documents for the links.

1.2 Design a HTML page describing your academic career. The page will tell about the degrees, institutions and your hobbies. Add some lists also.

1.3 Design a HTML page on your native place?

1.4 Design a HTML page on your friends. List your friends. Each friend's name is a link. Prepare separate HTML documents on each friend and call them in the appropriate link?

1.5 Prepare a HTML page listing popular cars companies. For each company prepare a sub-list showing various brands of cars it offers.

Adding Frames and Forms:

The browser window is called the container. It is possible to divide the container into several frames and use each frame for displaying a different html document. Frames have the following characteristics.

1. Each frame is given a name.
2. Each frame will be targeted by an html document.
3. Each frame resizes itself dynamically in response to the changes in the size of visible client area.

Frameset Definition

A set of frames are defined using the <frameset>tag which ends with </frameset> tag. The <frameset> tag has two attributes.

1. Row or column frame.
2. Size of each frame.

The size of the frames is mentioned in any one of the followings units:

1. Pixel unit
2. Percentage unit
3. Fraction unit

Pixel Unit

The pixel unit simply represents the number of pixels in each frame. Commas must separate the numbers. For example, consider the following:

<frameset cols="150, 70, 70">

.....

</frameset>

This definition creates three column-wise frames with the first frame of 150 pixels width, second of 70-pixel with and the third also of 70 pixels width.

Percentage Unit

The percentage unit divides the window according to the specified percentages. For example, consider the frame set definition,

<frameset rows=70%, 30%>

.....

.....

</frameset>

In the above definition two row wise frames are defined in the container.

If the total of the percentages is greater than 100 all percentages are scaled down. If the sum of the percentages is less than 100, the extra spaces are left out.

Fraction Unit

Instead of using percentage unit, we can use fraction unit to represent the relative size of the frames. Suppose we give the following:

<frameset cols="4*, 4*, *,*">

.....

.....

</frameset>

This defines four column wise frames. The first two frames have 4 unit size, and the third and fourth ones have one unit each. So, the frame sizes are 4/104/10, 1/10 and 1/10 of the overall container size.

Frame Definition

The definition of the frame is given using the <frames>tag. The <frame> tag may have any of the following attributes:

- Source html address (src)
- Name of the frame (name)
- Margin width (marginwidth)
- Scrolling button (scrolling)
- Can it be resized (noresize)

Example Banking Self Help Page

Consider the following frameset definition. Two row wise frames are defined

<html>

<head>

<title>

Welcome to commercial bank of Singapore

</title>

</head>

<frameset rows ="45,55">

<frame name="f1" src="D:\servlets\banking\bank1.html">

<frame name="f2" src=http://localhost:8080\servlet\Bankselfhelpservlet>

</frameset>

</html>

Nested Framesets

In this section we deal with nested framesets. In the example shown here, first the windows is row wise divided into two frames. The bottom frame is column wise divided further into two frames. The <no frame> tag is also used to communicate suitable message when the browser doesn't support frames.

```
<html>
<head>
<title>tutorial on web Technology</title>
</head>
<frameset rows="152,*">
<frameheader.html">
<frameset cols="150,*">
<frame name="contents" target="main" src="contents.html">
<frame name="main" src="body.html">
<frame name="main" src="body.html">
</frameset>
<no frames>
<body>
<p>This page uses frames, but your browser doesn't support them.</p>
</body>
</frames>
</frameset>
</html>
```

HTML Forms

Using forms we can design a web page on which a user can communicate his/her wisher ,opinion, suggestion etc.

A form is defined with <form> tag and </form> tag. The form tag has three attributes. They are

- Action
- Method
- Enctype

Action Attribute

The forms are used to get the input from the user. The user input is submitted to the server. The action attribute informs the browser the location of the server program to which the form input has to be submitted The server program may be a cgi-perl script ,a java applet or any other server program like JSP,ASP etc.

Method Attribute

The method attribute has only two choices of values. They are

Method = "get"

Method="post"

This denotes the protocol the server uses in implementing the forms features. Usually the value used for method attribute is

Method="post"

This is the recommended protocol. With the post method, the information from user is put into the data stream of the HTTP, and the back end program can read the data as input through the "standard input" data stream.

In the case of method = "get", the data received in the form are placed at the end of URL. If the form is very big and gets a number of inputs, the get method causes the URL to be very long. So, the method = "get" option is often discouraged.

ENCTYPE Attribute

This attribute is used to inform the server the way to handle the encryption process. Usually it is set to

Application/x-www-form-urlencoded. That is, the value is given as

enctype = "application/ x-www-form-unrecorded"

Elements of a Form

In a form there can be several elements to get the input form the use. They are

1. Selection List Box
2. Input Box
1. Text Area

Selection List Box

A selection list presents a list of options to the user. The user can select his choice from the list. The selection list box is created with <select> tag. The definition ends with </select> tag.

The < select> tag has three attributes. They are

1. Name attribute
2. Size attribute
3. Multiple attribute

The name attribute assigns a name for the variable, which will hold the selected choice. For example consider the following:

```
<select name="name box">
<option>Aparna</option>
option>Nithya</option>
<option>Priya</option>
</select>
```

This creates a selection box with three choices, Aparna, Nithya and Priya. It is possible to assign a value for each option using value attribute in the option tag. This is illustrated below:

```
<select name="nameBox">
<option value ="1">Aparna></option>
<option value="2">Nithya</option>
<option value="3">Priya</option>
</select>
```

In the dropdown list we normally select one of the items. There are certain cases in which the user can be given a freedom to select more than one of the options. This is provided by the

multiple attribute in the select tag.

<select name = townsvisited multiple ="multiple >

Input Elements

The input of the user can be given in any of the following GUI elements.

- Checkbox
- Radio button
- Text field
- Password field
- Hidden field
- Button
- Submit button
- Reset button

The input box is defined using the <input> tag. The type attribute defines whether it is a check box, radio button etc.

Text Field and Submit Button

Consider the following HTML document

```
<html>
<head>
</head>
<body>
<form name="biodata_form">
<h3>Enter your age please...</h3>
<input type="text" name="age">
<input type="submit" value="Submit Age">
</form>
</body>
</html>
```

Checkbox

The following is a HTML document that shows a form with several checkboxes.

```
<html>
<head>
</head>
<body>
<h3>Please select your computer configuration <br></h3>
<h4>
<input type="checkbox" name="computer" value="CPU Intel P4 1.8GHz">Intel P4 1.8GHz
<br>
```

<input type="checkbox" name="computer value="HDD 40 GB">Width 40 GB HDD

<input type="checkbox" name="computer" value="15 inch color monitor">Width Monitor

<input type="checkbox" name= "computer" value="1:44MD FDD">With FDD

<input type="checkbox" name= "computer" value= "CD ROM Drive"> With CD ROM Drive

<input type="checkbox" name= "computer" value= "Printer">With Printer

<input type= "text" name= "Order" size "50">

<input type= "button" name= "test" value= "Order Please">

</h3>

</body>

</html>

Password Field

The following HTML document shows a password field. Notice that when a user types the password, the characters are no displayed. The asterisk symbol will be displayed.

<html>

<html>

<title>Authorization Page</title>

</head>

<body>

<form name ="my form">

User Id :<input type=text name=id

Password :<input type=password name password>

<input type=submit value=Go>

</form>

</body>

</html>

Radio Button and Text Field

Consider the following HTML document

<html>

<head><title>Foreign Exchange</title>

</head>

<body>

<form name="fore form">

<pre>

Enter the value in rupees

<input type=text name="rupees">

```
<input type=radio name=currency> USDollar
<input type=radio name=currency> UKPound
</form>
</body>
</html>
```

Example Factorial of a Number

The following HTML document shows two text fields and a button

```
<html>
<head><title>Factorial</title>
</head>
<body>

<form>
<hr><br>
<h1 align="center"><marquee>Factorial </marquee></h1\>
<pre>
<center>
Enter the number: <input type=text name=a>
<br>
The factorial is:<input type=text name=b>
<br><br>
<input type= button value="Find the factorial">
</pre>
</form>
</body>
</html>
```

Text Area

The Text Area is a multi-line area in which the user can type the input. For example, the experience of a user with a product the suggestion for improvement of a course etc can be got using text area .A text area can be created using<text area>tag. The <text area> tag has three attributes. They are,

1. Number of rows in the text area
2. Number of columns in the text area
3. Name of the variable which will attain the content typed in the text area and submit it to the server

The rows and the columns attribute tell the number of rows and the number of columns of the text field visible at any instant .Notice that this is not a restriction for the text typed.The text area will have scroll bars for viewing the entire text typed.For example

<textarea name ="remark' rows ="5" columns ="25">

</textarea>

<h2>type your remarks here and press Proceed button</h2>

<textarea name = "remark" rows ="5" columns ="25"

</textarea><input type=button value="proceed">

Image maps: In this tag we placed a image on web page which consists of many spots and when we click on a part of a graphics that has spots on it, and depending on which hot spot youclick you'll go to a different page. For e.g. If you have map of the united states, each state could have its own hot spot. Clicking on a state brings you to a page with detailed information about that state.

Syntax:<map name="demo"><area href="url"></map>

Meta Tag gives us the information about the data with this tag the user is able to get the knowledge of what kind of material is present of website or on web page.

10.4 SUMMARY

HTML is the mother language of design web pages. it is tag oriented language and simple to learn. It consists tags like <h1>,<b>, etc.

It also consists of some advanced tags like meta tag which gives data about data.HTML also provides the facility of creating frames and forms through which the user can interacts.HTML file can easily prepared in any editor and its display can be displayed on any browser.HTML forms can also be prepared using different tags like button,textarea,radio button etc..Framesets are used for displaying many web pages on single web window by dividing it.

10.5 UNIT END QUESTIONS

1 Design a HTML form for reserving a room in a Hotel.

2 Design a HTML form to reserve a Railway Ticket.

3 Design a HTML form to see the result for a candidate when the results are published on the Web.

4 Design a HTML form to find the railway fare from one place to another.

5 Design a HTML form to find out the balance for a mobile phone customer as on today.

6 Design a HTML form to update the address of an insurance policy holder.

7. Design a web page for maruti udyog showing all the models which it prepares a using listing tags and the information of each using linking the document with each other.

8. Prepare a examination form for your university which consists of attributes name,rollno,exam-fees,father name etc and display the contents as web page.

9. Design a HTML web page for a departmental store showing all the products which it contains and information related with each product.

Reference Books:

1. G. Robertson: Hands on HTML,BPB Publications.

2. Harley Hahn: The Intenet,Tata McGraw Hill.

3. Javascript for the world wide web: Tom Negrino,Person Education.

4. Complete Javascript,Ivan Bayross

evaluate the effectiveness of online library instructions and can understand how to create a more useable interface.

The components require making a webpage are described below:

- **Text** : A text consisting of an HTML file and related files for scripts and graphics are often hyperlinked to other documents on the web.
- **Pictures** : Pictures can be still images or video images which can be put up in a web page. A picture is a visual representation or image painted, drawn, photographed or other wise rendered on a flat surface.
- **Animated Graphics** : The term "animated graphics" means text or images that do not remain static but they move when viewed in a web browser. A simulation of movement created by displaying a series of pictures or frames. Cartoon on television is an example of animation.

Audio Files : Sound file has been digitalized and stored on a computer. All performance characteristics and sound or voices are included in the file and sounds will sound the same on any computer, except for differences in speaker quality. Audio files are very large. One minute of CD quality stereo takes about 10 mb.

We need the following tools for creating a webpage:

- A text editor.
- A supply of clip art.
- Sound video equipment.

Method of Linking using HTML

The most important capability of HTML is it's ability to create hyperlinks to documents elsewhere on the server and on different servers and thereby make possible a world wide network of linked documents and information. For example,

 yahoo:

http://www.yahoo.com

Links are inserted using the (anchor) element. The anchor element is unlike the elements that require certain attributes inside it's opening tag in order to activate the hyperlink the most important attribute is a location to which you would like the anchoring object to be linked. Anchors can also be linked to email addresses when someone clicks on this type of anchored link, the default email program initiates an email message to be linked to the address.

11.3 WebSite Publishing

Publishing means putting HTML documents on the web server. Deciding where to store your pages is one of the final steps in creating your web site plan. To make your web pages available to every one on the web, you need to publish the site on the web server. You can either set up your own server or post your files to some one else's Web server.

Web pages are coded using Hyper Text Markup Language (HTML) tags to specify the way text and graphics are displayed. When you own Web page, you can either type the tags manually in a text editor or use a Webpage editor to do the coding for you. These editors are also called

Web page publishing tools. There are number of Web page editors available for making Web pages. Some popular editors are Netscape Composer, FrontPage and FrontPage Express, Page Mill and Hotdog.

Publicizing Your Site

After your site is published on the Web and have joined the global on-line community, how are you going to publicize the Site? The first step is to register your site with some search engines, so that people doing on-line searches can find the site. Apart from advertising your site by the word or mouth, here are some ways to let people know your Site on Web.

- Get the URL of your site printed on your business cards.
- Add your URL to your signature block in email.
- Include the URL in your return addresses whenever you send greeting cards.
- Have some bumpers stickers printed showing your group.
- Print the URL in your church bulletin each week.
- Post the URL on all school bulletin boards.

11.4 Maintenance of site

The management and maintenance of a site is as important as the original production. Web sites evolve, whether it's in style, contents, purpose or functionality. As a site establishes itself, unforeseen changes are made within the site so that it may better serve its purpose. This is done through the use of Web statistics management, a system in which different areas, specific pages and / or functions of a site monitored and if needed, changed to increase efficiency and productivity.

Business web sites should not only welcome new visitors to browse the site but also entire users to re-visit the site, in search of updated information. To accomplish this, web sites must have periodical changes made in both contents and graphics design.

The general purpose of any site is to produce revenue, by reaching more people, informing them, opening a new line of communication and in the end, selling a product or service.

11.5 Planning and Process Development of Web

Developing information for the web requires a focus on meeting users needs. To accomplish this methodology involves the following:

- **Planning** : Define target audience, purpose, objective and policies for information development and use.
- **Analysis** : Check technical construction of web with validation tools, evaluate information consistency and verify correctness of domain information.
- **Design** : Separate information page sized chunks, connect pages al-ong routes of use and user thinking, provide information, context and navigation cues, create a consistent look and feel.
- **Implementation:** Create an extendible directory and file structure, use HTML tools were helpful, use templates for supporting consistent look and feel, check implementation in various browsers.
- **Promotion** : Target publicity release for general Web audience, potential users and current users, follow online community norms and practices, innovatively connect with users to meet their needs.

- **Innovation** : Continuously and creatively work for improvement to meet user needs, use testing, evaluation and focus groups to shift and change web's content as users need change.

Planning

The process of choosing among competing opportunities for communication so that overall goals for the web can be set. These goals include anticipating and deciding on the targets for the audience, purpose and objective for the information. Planning also is done for domain information through a process of defining and specifying the supporting information that must be collected, how it will be collected and how the information will be updated. If a specification for a design calls for using a form interface. For example, the web planner must identify the need for web implementation to have these skills.

Analysis

A process of gathering and comparing information about the web and its operation in order to improve the web's overall quality. An important operation is one in which a web analyst examines information gathered about the audience for its relevance to some other elements or processes in web development. Information about the audience's level of technical interest can have a great deal of impact on what information should be provided to a user about a particular product or topic.

For example, analyzing the web's purpose in light of other new developments, such as the contents of a competitors web must be an ongoing process.

Design

The process by which a web design, working within the web's specification, makes decisions how a web's actual components should be constructed. This process involves taking into account the web's purpose, audience, objective and domain information. A good designer knows how to achieve the effect called for by the specification in the most flexible, efficient and elegant way. Because it relies so heavily on the other processes and elements in web development, however, the design process is not more important than any of the others, but it requires a through grounding in implementation possibilities as well as knowledge about how particular web structures affect an audience.

Implementation

The process of actually building the web using Hyper Text MarkUp Language (HTML) or improvements on it. The implementation process is perhaps most like software development because it involves using a specific syntax for encoding web structures in a formal language in computer files. Although automated tools are available to help with the construction of HTML documents, a thorough grounding in HTML as well as an awareness of how design can best be implemented in HTML enriches the web implementer's expertise.

Promotion

The process of handling all the public-relations of a web. These include making the existence of a web known to on-line communities through publicity, as well as forming business or other information relationship with other

webs. Promotion might involve using specific marketing strategies or creating business models.

Innovation

The process of making sure that the other development process continue and improve. This include monitoring technologies for new innovations that might be appropriate for the web, as well as finding creative or unique ways to improve the elements of the web or engage the web's audience in its success. Innovation also involves seeking to continuously improve the usability and quality of the web and exceeds user expectation.

Although the methodology outlined here for developing a web won't work flawless in all situations, it can serve as a basis for looking at many issues of web development. The actual processes and elements used in web development for any particular project might be a variation on these. Being aware of what elements and processes can be involved in web development is key; developers, once aware of what they might face, can most flexibly grow successful webs.

11.6 Components of Web project

The components require making a webpage are described below:

- **Text** : A text consisting of an HTML file and related files for scripts and graphics are often hyperlinked to other documents on the web.
- **Pictures** : Pictures can be still images or video images which can be put up in a web page. A picture is a visual representation or image painted, drawn, photographed or other wise rendered on a flat surface.
- **Animated Graphics** : The term "animated graphics" means text or images that do not remain static but they move when viewed in a web browser. A simulation of movement created by displaying a series of pictures or frames. Cartoon on television is an example of animation.
- **Audio Files** : Sound file has been digitalized and stored on a comp-uter. All performance characteristics and sound or voices are included in the file and sounds will sound the same on any computer, except for differences in speaker quality. Audio files are very large. One minute of CD quality stereo takes about 10 mb.

11.7 Formatting Web Page using Style Sheets

A Web Page can be prepared using Style Sheet. The web pages that are prepared by style sheet can also be called being formatted using style sheet.

Cascading Style Sheets

The mechanism that applies a style across one or more Web pages is termed as Cascading Style Sheets (CSS). The Sheets are files or portions of files on the internet. The style refers to a color scheme, layout, or other strategy of organizing the visual components of a document in a Web Page.

CSS is being used to control all aspects of graphics presentation of a Web Page like fonts, back ground, back ground image formation for Web Page or any tables within the page, page margin and text decoration such as italicizing and underlining to name a few. These designing elements are exposed to scripting, which can modify the document after it is downloaded, thus keeping CSS an integral part of DHTML.

Syntax :

Selector {declarations}

Each declaration is followed by,

Property: Values

H1 {font: Arial}

1) Embedding a style sheet

The <STYLE> tag is used to embed style information within a document. The <STYLE> tag should always include the TYPE declaration, which occurs inside the <HEAD> tag of the document.

2) Class Selector

The <BODY> of the HTML document can contain elements which may have a class associated with it. These classes enable the user to apply styles to specify parts of the document like font family, background color and so on.

3) ID as Selector

The ID selector is used in the same way as the class element. The only difference is that the ID attribute has a unique value over the document. The ID name declaration should proceeded by a#, in the <STYLE> declaration

4) Color

The color property applies to all HTML elements, including text, body back grounds and table back grounds. By default, all headings are in black and back ground of pages, tables to gray (transparent).

Syntax:

Selector { color : value}

Value can be either any color specified as 'RED' or 'GREEN' in hexadecimal value. For example, both the following declarations are valid.

Syntax:

H1 {color : blue}

R{color : #FF0000}

Back ground color can be set for every HTML element – Heading, paragraph and links. It is given as

Background Color – color : white

5) Fonts

CSS defines five font specific properties that can be set : font family, font style, font variant, font weight and font size. This property allows the web page designer to designate the font property on the web page.

The following tables gives the

Properties	Format	Variations
Font-family	P.plain{font-family: Arial}	Generic font families : • Serif (ex, times) • Sans-serif(ex,helvetical) • Cursive (ex, zapf-chauncery) • Fantasy (ex, western) • Monospace(ex, courie)
Font-size	.p{font-size :medium}	Absolute-size, relative-size, percentage, length
Font-Style	H1 {font-style:italic}	Italic, normal, oblique
Font-variant	.p{font-variant:small caps}	-
Font-weight	.p{font-weight : bolder}	Lighter, bolder, normal, bold

Adding Style Sheets

With basic purpose tags like (<H2>), it is not possible to control the text displayed in pure structural HTML pages. Instead, the page relies on the formatting tags in order to make the page more dynamic.

Enhancement of the appearance of the document is achieved using style sheets. The basic appearance of a document is a set to default: black text on a white back ground. After the <style> tags are inserted, the body element is added for overall page defaults.

Example:

```
<HTML>
<HEAD>
<STYLE TYPE = "text / css">
<!- - /* Hide style information from older browser /
P.ss {color : olive}
Span > Highlighted {color : red}
#1caps {text transforms :uppercase background color : MAROON}
H1 {color: purple};
H2 {color: red};
H3 {color: green};
H4 {color: navy};
H5 {color: teal};
H1 {color: arial};
H2 {color: times new roman};
H3 {color: arial black};
H4 {color: garamond};
H5 {color: impact};
// - ->
</STYLE>
</HEAD>
<Body>
```

<H1>Coog – the tiny, gorgeous hill district</h1>

<H2>Coog – the tiny, gorgeous hill district</h2>

<H3>Coog – the tiny, gorgeous hill district</h3>

<H4>Coog – the tiny, gorgeous hill district</h4>

<H5>Coog – the tiny, gorgeous hill district</h5>

< p class = "ss">

Cog is a religious of scattered village and hamlets, with a few townships

standing out.

<Span Class ="Highlighted">

Framed for their hunting skills, the kodavas have now turned ardent conservationists</ BR>

Today if you hear shorts ringing out in Kodagu,

 rest assumed that some Kodavas are testing their marksmanship </Br>

</SPAN>

<P ID =Icaps >People succumb to the lure of this beautiful

 Unsullied Eden and its fun loving, hospitable people </BR></P>

</Boby>

</HTML>

Creating Web Page by using Web Page Editors

In the modern Era there are many editors available for making web pages. The editors like Netscape composer, front page editors are available for making web pages and web sites.

The tags are already there in the web page we just have to write information or data between the tags.

Websites making becomes easier in editors like Front page express editors as it saves lot of time and can be easily prepared.

11.8 SUMMARY

Website is a Collection of web pages. Before making it we have to Plan, Design and many steps to do. A Website consists of pictures, video clips, text as its components. Website also requires the proper maintenance after it is prepared as it should provide the latest information. one of the main aim of website is to produce revenues. There are many tools available which helps us in preparation of websites.

11.9 UNIT END QUESTIONS

1. What are steps in creating a simple web page?
2. Write the various components of a web page?
3. Write short notes on :
   (i) Publishing of a web page
   (ii) Publicity of a web page
4. What are the basic requirements of developing a professional Web Site?
5. How to write Web projects and identification of objects?

6. Explain different tools for creating a Web project?
7. What is a Web site? what main purpose they are designed for?
8. What is the basic difference between a web Designer and a s/w developer.
9. What is the basic use of CSS? Design a web page using CSS tags.

Reference books:

1. Joel Sklar:Principles of Web Design,BPB Publication.
2. G.Robertson:Hands on HTML,BPB Publication.

UNIT - XII

CREATING AND MAINTAINING WEB SITES (CONTD.)

STRUCTURE OF THE UNIT

12.0 Objectives
12.1 Introduction
12.2 Anti-Aliasing
12.3 Image Slicing
12.4 Adding sound to web sites
12.5 Adding sound into a web page
12.6 Optimizing web pages
12.7 File Transfer Protocol (FTP)
12.8 Analyzing Web Traffic
12.9 Creating traffic to your web site
12.10 Summary
12.11 Unit end questions

12.0 OBJECTIVE

This unit will be explaining the advance controls used on web page as in continuation of previous unit. In this unit you will learn how to put animated graphics on web page, put audio files on web page etc.this unit will also explains how to analyze the web traffic, building traffic to web site. This unit will also explain the file transfer protocol, proxy server and web server role. Have a nice trip to this unit.

12.1 INTRODUCTION

Picture

Pictures can be still images or video images which can put up in web page. A picture is visual representation or image painted, drawn, photographed, or otherwise rendered on flat surface.

Animated Graphics

The term "animated graphics" means text or images that do not remain static but that may move when viewed in browser. Animated graphics: a simulation of movement created by displaying a series of pictures, or frames. A cartoon on television is one examples of animation.

Using Gif & JPEG

Gif & JPEG files are used as some a common pictures, that is, both the gif & jpeg files are added on to the website using the img-scr command in HTML & by dragging in front-page etc, the sizes are to set by height and width.

Getting web clip art

Clip art are available on the computers that are also able to added on to a website using different procedures these clip arts act as pictures on images that are predefined, they can be designs, people, automobiles etc.

Optimizing images on the web

Images optimizing refers to the optimization of the images being used i.e. the visual size that must suit the look of the website & also the size (storage size) of the images must also be smaller so as to benefit on the web in websites as these pictures need to be downloaded first when opening any websites, the pictures on the website must be smaller in capacity so as to maintain a fast transfer speed on the net & that alter the website opening speed.

Gif File format - Compuserve Gifs

The GIF file format was developed by **CompuServe** and is sometimes still referred to as *CompuServe Gif*. It uses the LZW (Lempel-Ziv and Welch) compression algorithm for 8-bit color images. It is the only image format supported by all graphical web browsers - even the very first ones.

What are animated GIFs

An animated gif consists of a series of frames that are played one after the other giving a semblance of animation. This is similar to traditional animation technique where frames are displayed in quick succession. Also, in animated gifs you can control the time for which each frame is displayed. In simplest terms, the frames of an animated gif can be considered as individual images. Each frame is displayed for a specific amount of time and is followed by the next. Displaying one frame after the other results in an animated web gif image.

JPEG file format

The JPEG or JPG file format was adopted quite early on the Internet. It's name comes from Joint Photographic Experts Group, the organization that created the format. As evident from the name, JPEG images are used mainly for photographs.

12.2 ANTI-ALIASING

One of the most important techniques in making graphics and text easy to read And pleasing to the eye on-screen is anti-aliasing. Anti-aliasing is a cheaty way of getting round the low 72dpi resolution of the computer monitor and making Objects appear as smooth as if they'd just stepped out of a 1200dpi printer (Nearly).

Anti-aliasing substitutes the shades of grey around the lines which would otherwise be broken across a pixel.

But anti-aliasing is more than just making something slightly fuzzy so that you can't see the jagged edges: it's a way of fooling the eye into seeing straight lines and smooth curves where there are none.

Pixels around an un-anti-aliased line can only be part of the line or not part of it: so the computer draws the line as a jagged set of pixels roughly approximating the course of our original nice smooth line. (Trivia fact: anti-aliasing was invented at MIT's Media Lab. So glad they do something useful there....)

When the computer anti-aliases the line it works out how much of each in-between pixel would be covered by the diagonal line and draws that pixel as an intermediate shade between background and foreground. In our simple-minded example there is shades of grey. This close up the anti-aliasing is obvious and actually looks worse than the un-anti-aliased version, but try taking our glasses off, stepping a few yards back from the screen and screwing up your eyes a bit to emulate the effect of seeing the line on a VGA monitor covered in crud at its right size. Suddenly a nice, smooth line pops into view.

So how does one go about anti-aliasing an image? Just be grateful you don't have to do it by hand. Most screen design programs, including Photoshop and Paintshop Pro include anti-alias options for things like text and line tools. The important thing is simply to remember to do it, and to do it at the appropriate time.

There are far too many graphics out on the Web that are perfectly well-designed, attractive and fitted to their purpose but end up looking amateurish because they haven't been anti-aliased. Equally, there are plenty of graphics that have turned to visual mush because they've been overworked with the anti-alias tool.

Generally, the rules are these:

Always anti-alias text except when the text is very small. This is to taste but I reckon on switching off anti-aliasing in Photoshop below about 12 points. If you're doing a lot with text this size, you really oughtn't to be putting it in a graphic but formatting ASCII instead.

Always anti-alias rasterised EPSs . Except when you don't want to, of course.

If attempting to anti-alias something manually, or semi-manually, such as by putting a grey halo round a block black graphic, then only apply the effect at the last possible stage. And always, always, always bear in mind the target background colour. It's a fat lot of good anti-aliasing a piece of blue text on a white background, if the target page is orange, because the anti-aliased halo is going to be shades of white-orange.

Never confuse blur and anti-aliasing. The former is a great help in making things appear nice and smooth if applied to specific parts of an image, but it'll make your image just look runny if used all over.

12.3 IMAGE SLICING

It's often debated whether or not slicing Web graphics actually makes them load faster. Some people will tell you that slicing an image does not reduce the overall size or load time and it's our human perception that makes it seem like the page is loading faster. Another group will tell you that slicing images can actually increase load time due to the additional simultaneous requests to the Web server. And then there is yet another group that will swear that slicing large images can significantly reduce the time it takes your pages to load.

So, who's right and who's wrong?

Well, there's actually some truth in all of these arguments. It's true that the act of slicing an image will not decrease the file size in and of itself. Simply slicing and saving each section with the same compression settings is pointless; but by optimizing, you can reduce your images by several KB's and you will often get a better looking image too. In this scenario, it's not the act of slicing that reduces the download time; it's the act of compressing each slice to optimal settings.

We'll explore this further with some examples in a bit, but for now here's a brief explanation: You may have an image where some areas compress better as GIF and other areas compress better as JPEG. If large portions of the image have solid colored areas, they can be eliminated completely and replaced with a background color in your table layout. It's extremely important to understand how compression works in order to properly place your slices for the best results.

In addition to optimizing, other reasons for slicing Web graphics are:

when you can repeat or stretch a single small image to fill a larger space,

creating mouse rollovers and clickable image maps

animating portions of a large image.

12.4 ADDING SOUND TO WEB SITES

There are two tags for adding sound to your document, Internet Explorer 3.0's <BGSOUND> tag and Netscape's <EMBED> tag. The <BGSOUND> play the background sound from your page. That is when visitor visit your page, the sound will automatically play. Netscape's <EMBED> tag is slightly different, you can use its attribute to select playing sound when the page is loaded or give the users an option to

click whether they would like to hear the sound. The sound console will appear in their page like this. (Sound console will appear below, if you're using Netscape)

You are exciting to know now how to do it, right? In this example, I use midi file because it give a high quality sound. I will tell you about other format later on this page.

Here is how to use an <EMBED> tag:

<EMBED SRC=your file.mid AUTOSTART=true WIDTH=144 HEIGHT=60 LOOP=1>

AUTOSTART=true means automatically play sound when document is loaded. This way, the sound will play as a background sound. You can also set the value to false. The sound will play when the "play" button is clicked.

LOOP=n This tells browser how many times to play sound. *n* could be an integer, true, or false. Setting LOOP=true, browser will continue playing your sound until the stop button on the console is clicked.

WIDTH and *HEIGHT* This is how the sound control (console) will be displayed. Setting them as the given numbers, browsers will display a full console. Setting the width=0 and height=2, the console will not displayed by the browsers. Other values that too small will cause the browsers display uncompleted image. You might also hide it by placing *HIDDEN=true* like this: <EMBED SRC=your_file.mid AUTOSTART=true HIDDEN=true LOOP=1>

It's a good idea to give an alternative to people who using browsers that do not support the embedded sound. Here is what I did on this page:

<embed src="bgsound.mid" hidden="true" autostart="true" loop="1"> <noembed>Your browser doesn't support EMBED, but you can still listen to the background sound of this page by clicking here.</noembed>

Browsers that do not support EMBED will display the link inside <noembed> tag.

Here is how to use <BGSOUND> tag:

<BGSOUND SRC=your_file.mid LOOP=1>

LOOP can be specified as any positive number, infinite, or -1 which equals infinite.

The differences of two browsers brought headaches to us. I would like to correct what I described here in last version of this page. You'd better use both <EMBED> and <BGSOUND> tags to make sure that visitors get background sound.

Internet Explorer does not support <EMBED> tag directly, but it does support plugins that installed by Netscape. The users of Internet Explorer 3.0 or higher will hear the sound from <EMBED> if they also have Netscape 3.0 installed in their machine. In this case, If there are both tags in the documents, Explorer take <BGSOUND> tag active but will report the error of cannot playing sound that resides in the <EMBED> tag. This is a disadvantage of putting both tags together.

The error tag will be something like:

Anyway, these boxes are not a big deal, users can click "OK" to process to the next step. I recommend using both tags to make sure that your visitors will surely hear background sound. If you're planning for giving the option for users to click from the sound console to hear sound, you only have one alternative — using <EMBED> tag.

Tips for people who installed Netscape 4.0 on the machine that have Internet Explorer installed: Netscape 4.0 will disable your plug-in installed by its previous version. If you have IE installed in your system, IE will no longer be able to play midi file (in case that IE shared

plug-in with Netscape). You'd better back up the plug-in previously installed by Netscape 3.0 and copy them back to plug-in directory. If you have IE installed, you can use those files in IE's plug-in directory.

12.5 ADDING SOUND INTO A WEB PAGE

There are two tags for adding sound to your document, Internet Explorer 3.0's <BGSOUND> tag and Netscape's <EMBED> tag. The <BGSOUND> play the background sound from your page. That is when visitor visit your page, the sound will automatically play. Netscape's <EMBED> tag is slightly different, you can use its attribute to select playing sound when the page is loaded or give the users an option to click whether they would like to hear the sound. The sound console will appear in their page like this. (Sound console will appear below, if you're using Netscape)

LISTEN GO GROOVY	LISTEN TO JAZZY

You are exciting to know now how to do it, right? In this example, I use midi file because it give a high quality sound. I will tell you about other format later on this page.

Here is how to use an <EMBED> tag:

<EMBED SRC=Filename.mid Autostart=true width=144 height=60 Loop=1>

AUTOSTART=true means automatically play sound when document is loaded. This way, the sound will play as a background sound. You can also set the value to false. The sound will play when the "play" button is clicked.

LOOP=n This tells browser how many times to play sound. *n* could be an integer, true, or false. Setting LOOP=true, browser will continue playing your sound until the stop button on the console is clicked.

WIDTH and *HEIGHT* This is how the sound control (console) will be displayed. Setting them as the given numbers, browsers will display a full console. Setting the width=0 and height=2, the console will not displayed by the browsers. Other values that too small will cause the browsers display uncompleted image.

It's a good idea to give an alternative to people who using browsers that do not support the embedded sound. Here is what I did on this page:

Browsers that do not support EMBED will display the link inside <noembed> tag.

Here is how to use <BGSOUND> tag:

<BGSOUND SRC=filename.mid LOOP=1>

LOOP can be specified as any positive number, infinite, or -1 which equals infinite

The differences of two browsers brought headaches to us. I would like to correct what I described here in last version of this page. You'd better use both <EMBED> and <BGSOUND> tags to make sure that visitors get background sound.

Internet Explorer does not support <EMBED> tag directly, but it does support plugins that installed by Netscape. The users of Internet Explorer 3.0 or higher will hear the sound from <EMBED> if they also have Netscape 3.0 installed in their machine. In this case, If there are both tags in the documents, Explorer take <BGSOUND> tag active but will report the error of cannot playing sound that resides in the <EMBED> tag. This is a disadvantage of putting both tags together.

The error tag will be something like:

Anyway, these boxes are not a big deal, users can click "OK" to process to the next step. I recommend using both tags to make sure that your visitors will surely hear background sound. If you're planning for giving the option for users to click from the sound console to hear sound, you only have one alternative — using <EMBED> tag.

Tips for people who installed Netscape 4.0 on the machine that have Internet Explorer installed: Netscape 4.0 will disable your plug-in installed by its previous version. If you have IE installed in your system, IE will no longer be able to play midi file (in case that IE shared plug-in with Netscape). You'd better back up the plug-in previously installed by Netscape 3.0 and copy them back to plug-in directory. If you have IE installed, you can use those files in IE's plug-in directory.

What Formats Does it supports?

The <EMBED> tag plays audio files in WAV, AIFF, AU, and MIDI formats.

MIDI (.mid) format give you a high quality of digital sound.

WAV (.wav) format was developed for used with Microsoft's Window. You can record .wav using Windows. The sound quality is not as good as MIDI, but the file is smaller.

AU (.au) was developed by Sun. The sound quality is poor, but the file is quite small, used for recording short speech.

AIFF (.aiff) was developed by Apple for music and high quality sound.

The most popular is MIDI for music and WAV for short message. If you own a PC running Windows, you are ready to plug a microphone and start recording.

12.6 OPTIMIZING WEB PAGES

One of the important things to remember when designing web pages is their file size. The size of the page determines how fast it loads on the visitor's browser window. Expecting your visitors to wait till your web page loads is wishful thinking. The browser *back* and *Close* buttons are just a click away.So what would you like - a visitor that quickly leaves your web site as it's taking your web page *ages* to load because of all fancy graphics and flash animation or a visitor who

will go through the page and maybe a few more on your web site? Put yourself in the visitors shoes, are you ready to wait more than 10 seconds for a web page to load? Obviously, you cannot control the bandwidth used by the visitor but you ***can*** surely work on optimizing your web pages so they load quickly - right?

12.7 FILE TRANSFER PROTOCOL - FTP

The File Transfer Protocol is an excellent method to transfer (download and send) files from one computer to the other over the Internet. Though you can transfer files using email, it is not a good choice especially when the file size is large or when you need to transfer several files. The objectives of FTP are to:

promote file (programs or data) sharing

Efficiently transfer data from one computer to another

Encourage indirect or implicit use of remote computers

Provide a common platform for file storages among different hosts

FTP sites

FTP sites are storehouses of hundreds to thousands of files - programs, data, music, video etc. In order to upload or download a file from an FTP site, you need to know the login details - the **FTP username** and **FTP password**. Once connected, you can transfer files using the ***binary*** or ***ASCII*** mode. The binary mode is used for *binary files* like executable programs, music, images, video etc. while the *ASCII* mode is employed for plain text files such as those created in Notepad, vi etc.

To connect to your site through FTP:

Start an FTP program such as CuteFTP.

Log in using the appropriate information:

For a name-based site:

<user_name>@<domain_name.com>

or

<user_name>#<domain_name.com>

For an IP-based site:

<user_name>

Note: The default upload directory is /home/<user_name>

FTP Clients versus FTP Servers

FTP is a protocol that involves two systems, one that requests a file transfer (the *client*) and one that then approves the request and does the sending or receiving (the *server*). These two systems have very different roles.

The client side of FTP is basically an interface to make FTP more usable for an end user. It provides an easy way for the end user to specify a transmission mode, from which directory to pull data, or other information pertinent to the FTP session. Every TCP/IP implementation comes with an FTP client program and is executable with the ftp command. Most PC and Macintosh-based TCP/IP packages have a graphical user interface (GUI) front end, so instead of typing the commands discussed earlier, you access FTP commands by using either pull-down menus or buttons the user clicks to invoke a particular FTP command. (An example later in this chapter shows an FTP client GUI and where commands typically may lie in a GUI.)

The server side of FTP does not run like the FTP client program. The FTP server functions in the background where it sleeps until an FTP client attaches to it. After an FTP client attaches to an FTP server program, the FTP server program wakes up, acknowledges that client, and handles

the important task of authentication. The FTP server determines whether the username and password are correct and permits the client to proceed or denies access. (The "FTP Servers" section later in this chapter discusses how users and passwords are handled on a platform-by-platform basis.)

Different types of FTP server processes.

Platform	*Implementation of FTP Server*
UNIX	*Daemon*
MS-DOS	*TSR that can be invoked as an executable*
Windows NT	*Service*
Macintosh	*Extension*

12.8 ANALYZING WEB TRAFFIC

Who is visiting your Web site? What browsers do they use? Where do they go in the site? What pages do they look at? Your Web server log files contain the answers to these questions and more. Once you start using your server log information, you'll wonder how you ever got along without it.

Who Goes There?

Think of your server logs as a virtual visitor sign-in sheet. They record where your visitors came from and where they go on your site.

Server log files tell you:

Which pages get the most traffic - and the least.

What sites are referring visitors to you.

Which pages visitors look at.

What browsers and operating systems are most popular with visitors.

When search engine spiders and directory editors visit.

This data can often help you flag specific problems on your Web site. If you have a lot of visitors, but few sales, check your server logs to see how many visitors actually see your product offerings. Wondering just how effective that expensive ad campaign really is? Your server logs can tell you how much traffic - and sales - it's really generating.

You can also use the data to uncover hidden problems on your site. Suppose you find that 20% of your visitors use the WebTV browser. Since sites display much differently in WebTV than in Explorer or Netscape, you'll probably need to consider optimizing your site for the WebTV browser.

Reading Your Log Files

The server stores visitor information in files with the .log extension - open them as text files if you want to look at the raw log data. Unfortunately, you can't do much useful analysis with the raw data unless you're a math whiz. Here is how the log file records a single request to a Web server:

209.240.221.71 - - [03/Jan/2001:15:20:06 -0800] "GET /Inauguration.htm HTTP/1.0" 200 8788 "http://www.democrats.com/" "Mozilla/3.0 WebTV/1.2 (compatible; MSIE 2.0)"

Here's what it all means!

Server Log Info	Component Name	Meaning
209.240.221.71	remotehost	Name of the computer requesting the Web page.
	rfc931	The name of the remote user. This field is usually blank.
	authuser	Login of the remote user. This is also usually blank.
[03/Jan/2001: 15:20:06 -0800]	date	Date and time of the request.
"GET /Inauguration. htm HTTP/1.0"	request	URL of the file requested. This is noted exactly as the user requested it.
200	status	Error or status code generated by the request.
8788	bytes	Size (in bytes) of the document returned to the client.
http://www.democrats.com/	referrer	The URL the visitor came from immediately before they requested the file.
"Mozilla/3.0 WebTV/1.2 (compatible; MSIE 2.0)"	agent	Records the visitor's browser and operating system.

The server logs provide a lot of important information: the trick is to put that data into an understandable format. If you have a large ecommerce site, then you probably already have a custom system in place. Smaller commercial or personal sites often rely on the Web site statistics programs supplied by their Web hosts.

Log File Analysis Packages

If your Web host doesn't offer site statistics - or charges you for them - consider using some of the Web site analysis packages available for download. Packages vary widely in price and performance. Several like Analog, http-Analyze, and Real Tracker are free for non-commercial sites.

A basic package will organize the log information into several sections. At a minimum, you need to know the following:

Number of computers requesting content: This tells you how many visitors actually came to your site during a certain period - usually 24 hours. It's a much more useful gauge of site traffic than the total number of hits.

Files requested for download: The number of hits to your site. Each hit represents an individual file sent from the server - that includes image files, CGI scripts, and HTML pages. The log data should be broken out by each individual file name so you can tell exactly how many page views you have.

HTML page requests: The number of page views, which is a count of the number of times each individual Web page was requested. Ideally, you want visitors to look at more than just your home page. Divide the page view count by the number of visitors and you can get a rough estimate of how many pages each visitor actually sees.

Browser and operating system: Shows you which browser and operating system your visitors used. Use this information to decide which (if any) browser or operating system-specific elements it's safe to include on your site.

Referrer: A record of what page a visitor was at immediately before they arrived at your site. This information helps you determine which search engines send you the most traffic, the effectiveness of ad campaigns, and which links are the most active.

12.9 CREATING TRAFFIC TO YOUR WEB SITE

The first step towards web promotion is building a web site that is Search Engine friendly and then submitting it to the major search engines and directories on the Internet. Hallmarks of a good web site are a professional design and great content. A professional designed web site stands out from the rest and relevant and detailed content make your online presence strong. You should remember that visitors come to your site for *information*... only when they find it satisfactory would they buy your product or service.

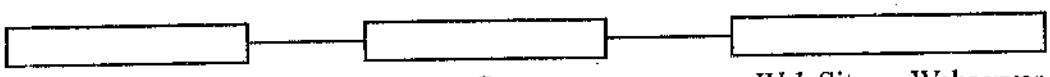
The second step would be to exchange links with other web sites. This helps in increasing your web sites Page Rank also called **PR**. Page Rank is used by Google, the most successful search engine, to rank web sites. It's obvious that sites will good content and a clean nice design will automatically get linked from other sites and you would not have to spend hours trying to convince people to exchange links with your site. Both link exchanging and content writing are time-consuming processes, however, latter is a good option. The reason is simple - when you have good content on your web site, people

would *like* linking to your web site and most will do it without you even knowing about it.

The third step would be to promote your products and services employing web banners and/or text ads.

Proxy Server

Proxy server are very often used to improve the performance of a network traffic by using its capacity to store information's that has been used by many internet users. For example when one person visits an internet site a copy of the information is stored on the proxy server. When another person afterwards visit the same Internet site then he gets information immediately because the data has been previously stored. Such a process of storing of information on proxy server is called cache. The advantage of the proxy server caching method is that the network must less frequently make contact with the original Internet site. The disadvantage is that the shown information is not the most recent available. However old cache that remains on the server are frequently deleted based on the server administrators rules (time, age, size, access....) that says when the information is to be removed from the servers cache.

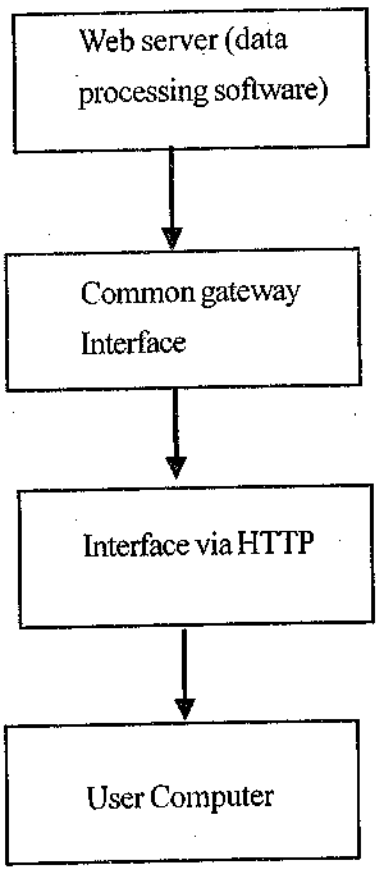


Computer or PC Proxy Server Web Site on Webserver

Proxy servers may also be used to bypass restrictions and limitations that the owner of the internet resource has set for users from specific country, region and users that fall into specific ip address ranges. For example if the website owner (webmaster) for whatever reason blocks access to the visitors from some countries the visitors from blocked country could use an open free proxy server from another countries and override the restriction.

Web Servers:

Web server is computer connected to the internet and running server software. The software lets the computer use the HTTP (Hyper text transfer protocol) to server HTML files to web browser clients. Unless your company or organization has a web server, you must use the services of a web hosting provider. After you choose a server to host your files, you will need to select file transfer software and upload the web sites files from your development machine the web server.



12.10 SUMMARY

The term "animated graphics" means text or images that do not remain static but that may move when viewed in browser. There are two tags for adding sound to your document, Internet Explorer 3.0's <BGSOUND> tag and Netscape's <EMBED> tag. The <BGSOUND> play the background sound from your page. The <EMBED> tag plays audio files in WAV, AIFF, AU, and MIDI formats. MIDI (.mid) format give you a high quality of digital sound. The File Transfer Protocol is an excellent method to transfer (download and send) files from one computer to the

other over the Internet. FTP sites are storehouses of hundreds to thousands of files - programs, data, music, video etc. In order to upload or download a file from an FTP site, you need to know the login details - the FTP username and FTP password. Log files on web server are used to analyze the web traffic. The advantage of the proxy server caching method is that the network must less frequently make contact with the original Internet site. Web server is computer connected to the internet and running server software. The software lets the computer use the HTTP(Hyper text transfer protocol) to server HTML files to web browser clients.

12.11 UNIT END QUESTIONS

1. Write Short notes on:
   a. GIF
   b. JPEG
2. What do you mean by Anti Aliasing? Explain.
3. What is Optimization of web page? How is it done?
4. What is FTP? What are its main Objectives? How we can connect to ftp server.
5 What are Log files? How are they analyzed? Explain with an example.
6. Explain Image Slicing.
7. Explain the concept of Proxy Server.
8. What is the role of Web server in placing a website on web server?
9. How can we place a audio file on a web page?
10. Explain the concept of managing traffic on a web site?

REFERENCE BOOKS

1. Joel Sklar,Principles of Web Design,Web Warror Series.
2. Java and web Technology,G.s Baluja,Dhanpat rai & sons.

UNIT - XIII

JAVASCRIPT

STRUCTURE OF THE UNIT

13.0 Objectives
13.1 Introduction
13.2 How to put a JavaScript code into a HTML page
13.3 JavaScript Variables
13.4 Conditional Statements
13.5 JavaScript Events
13.6 JavaScript - Catching Errors
13.7 Introduction of JavaScript Objects
13.8 Creating your own objects
13.9 HTML DOM objects
13.10 Summary
13.11 Unit end questions

13.0 OBJECTIVES:

In this chapter or unit you will learn the basic as well as advanced concepts of JavaScript. it covers how to put scripts in a HTMLWeb page using JavaScript. it also helps you to make your web page dynamic and interactive. This unit covers all the basic JavaScript commands, loops, objects used in JavaScript's to make a web page interactive. This unit will cover some JavaScript's objects. it also explains with different examples how to declare the variable and other commands in JavaScript. It cover example of Timeout and advanced concepts of HTMLDOM objects. After the end of this unit you will become quiet familiar with JavaScript and also becomes capable of writing your own JavaScript programs. Have a best tour to JavaScript.

13.1 INTRODUCTION

JavaScript is the scripting language of the Web! JavaScript is used in millions of Web pages to improve the design, validate forms, detect browsers, create cookies, and much more. JavaScript is the most popular scripting language on the internet, and works for all major browsers, such as Internet Explorer, Mozilla, Firefox, Netscape, and Opera.

WHAT IS JAVASCRIPT?

- JavaScript was designed to add interactivity to HTML pages
- JavaScript is a scripting language (a scripting language is a lightweight programming language)
- A JavaScript consists of lines of executable computer code
- A JavaScript is usually embedded directly into HTML pages
- JavaScript is an interpreted language (means that scripts execute without preliminary compilation)
- Everyone can use JavaScript without purchasing a license

Are Java and JavaScript the Same?

NO! Java and JavaScript are two completely different languages in both concept and design! Java (developed by Sun Microsystems) is a powerful and much more complex programming language - in the same category as C and C++.

What can a JavaScript Do?

- **JavaScript gives HTML designers a programming tool** - HTML authors are normally not programmers, but JavaScript is a scripting language with a very simple syntax! Almost anyone can put small "snippets" of code into their HTML pages
- **JavaScript can put dynamic text into an HTML page** - A JavaScript statement like this: document.write("<h1>" + name + "</h1>") can write a variable text into an HTML page
- **JavaScript can react to events** - A JavaScript can be set to execute when something happens, like when a page has finished loading or when a user clicks on an HTML element
- **JavaScript can read and write HTML elements** - A JavaScript can read and change the content of an HTML element.
- **JavaScript can be used to validate data** - A JavaScript can be used to validate form data before it is submitted to a server. This saves the server from extra processing.
- **JavaScript can be used to detect the visitor's browser** - A JavaScript can be used to detect the visitor's browser, and - depending on the browser - load another page specifically designed for that browser.
- **JavaScript can be used to create cookies** - A JavaScript can be used to store and retrieve information on the visitor's computer.

13.2 HOW TO PUT A JAVASCRIPT CODE INTO A HTML PAGE

```
<html>
<body>
<script type="text/javascript">
document.write("Hello World!")
</script>
</body>
</html>
```

The code above will produce this output on an HTML page:

Hello World!

Explanation of the above example

To insert a JavaScript into an HTML page, we use the <script> tag (also use the type attribute to define the scripting language). So, the <script type="text/javascript"> and </script> tells where the JavaScript starts and ends:

```
<html>
<body>
<script type="text/javascript">
...
</script>
</body></html>
```

The word **document.write** is a standard JavaScript command for writing output to a page.

By entering the document.write command between the <script type="text/javascript"> and </script> tags, the browser will recognize it as a JavaScript command and execute the code line. In this case the browser will write Hello World! to the page.

Note: If we had not entered the <script> tag, the browser would have treated the document.write("Hello World!") command as pure text, and just write the entire line on the page.

Ending Statements With a Semicolon?

With traditional programming languages, like C++ and Java, each code statement has to end with a semicolon. Many programmers continue this habit when writing JavaScript, but in general, semicolons are **optional!** However, semicolons are required if you want to put more than one statement on a single line.

Where to Put the JavaScript

JavaScripts in a page will be executed immediately while the page loads into the browser. This is not always what we want. Sometimes we want to execute a script when a page loads, other times when a user triggers an event.

Scripts in the head section: Scripts to be executed when they are called, or when an event is triggered, go in the head section. When you place a script in the head section, you will ensure that the script is loaded before anyone uses it.

```
<html>
<head>
<script type="text/javascript">
....
</script></head>
```

Scripts in the body section: Scripts to be executed when the page loads the body section. When you place a script in the body section it generates the content of the page.

```
<html>
<head>
</head>
<body>
<script type="text/javascript">
....
</script>
</body>
```

Scripts in both the body and the head section: You can place an unlimited number of scripts in your document, so you can have scripts in both the body and the head section.

```
<html>
<head>
<script type="text/javascript">
....
</script></head>
<body>
<script type="text/javascript">
```

....
</script> </body>

13.3 JAVASCRIPT VARIABLES

Variables are used to store data .A variable is a "container" for information you want to store. A variable's value can change during the script. Rules for variable names:

- Variable names are case sensitive
- They must begin with a letter or the underscore character

IMPORTANT! JavaScript is case-sensitive! A variable named strname is not the same as a variable named STRNAME.

Declare a Variable

You can create a variable with the var statement:

var strname = some value

You can also create a variable without the var statement:

strname = some value

Assign a Value to a Variable

You can assign a value to a variable like this:

var strname = "Value"

Or like this:

strname = "Value"

The variable name is on the left side of the expression and the value you want to assign to the variable is on the right. Now the variable **strname** has the value "Value".

Lifetime of Variables

When you declare a variable within a function, the variable can only be accessed within that function. When you exit the function, the variable is destroyed. These variables are called local variables. You can have local variables with the same name in different functions, because each is recognized only by the function in which it is declared. If you declare a variable outside a function, all the functions on your page can access it. The lifetime of these variables starts when they are declared, and ends when the page is closed.

13.4 CONDITIONAL STATEMENTS

Very often when you write code, you want to perform different actions for different decisions. You can use conditional statements in your code to do this.

In JavaScript we have the following conditional statements:

- **if statement** - use this statement if you want to execute some code only if a specified condition is true
- **if...else statement** - use this statement if you want to execute some code if the condition is true and another code if the condition is false
- **if...else if....else statement** - use this statement if you want to select one of many blocks of code to be executed
- **switch statement** - use this statement if you want to select one of many blocks of code to be executed

If Statement

You should use the if statement if you want to execute some code only if a specified condition is true.

Syntax

```
if(condition)
{
code to be executed if condition is true
}
```

Note that **if** is written in lowercase letters. Using uppercase letters (**IF**) will generate a **JavaScript error!**

Example

```
<script type="text/javascript">
//Write a "Good morning" greeting if the time is less than 10
var d=new Date()
var time=d.getHours()
if(time<10)
{
document.write("<b>Good morning</b>")
}
</script>
```

Note: When comparing variables you must always use two equals signs next to each other (==). Notice that there is no **..else..** in this syntax. You just tell the code to execute some code only if the specified condition is true.

If...else Statement

If one want to execute some code if a condition is true and another code if the condition is not true, use the if....else statement.

Syntax

```
if(condition)
{
code to be executed if condition is true
}
else
{
code to be executed if condition is not true
}
```

Example

```
<script type="text/javascript">
```

```
//If the time is less than 10,
//you will get a "Good morning" greeting.
//Otherwise you will get a "Good day" greeting.
var d = new Date()
var time = d.getHours()
if (time < 10)
{
document.write("Good morning!")
}
else
{
document.write("Good day!")
}
</script>
```

If...else if...else Statement

You should use the if....else if...else statement if you want to select one of many sets of lines to execute.

Syntax

```
if(condition1)
{
code to be executed if condition1 is true
}
else if(condition2)
{
code to be executed if condition2 is true
}
else
{
code to be executed if condition1 and condition2 are not true
}
```

Example

```
<script type="text/javascript">
var d = new Date()
var time = d.getHours()
if(time<10)
{
document.write("<b>Good morning</b>")
```

```
}
else if (time>10 && time<16)
{
document.write("<b>Good day</b>")
}
else
{
document.write("<b>Hello World!</b>")
}
</script>
```

13.5 JAVASCRIPT EVENTS

Events: By using JavaScript, we have the ability to create dynamic web pages. Events are actions that can be detected by JavaScript. Every element on a web page has certain events which can trigger JavaScript functions. For example, we can use the **on Click** event of a button element to indicate that a function will run when a user clicks on the button. We define the events in the HTML tags.

Examples of events:

- A mouse click
- A web page or an image loading
- Mousing over a hot spot on the web page
- Selecting an input box in an HTML form
- Submitting an HTML form
- A keystroke

Note: Events are normally used in combination with functions, and the function will not be executed before the event occurs.

onload and onUnload

The onload and onUnload events are triggered when the user enters or leaves the page. The onload event is often used to check the visitor's browser type and browser version, and load the proper version of the web page based on the information. Both the onload and onUnload events are also often used to deal with cookies that should be set when a user enters or leaves a page. For example, you could have a popup asking for the user's name upon his first arrival to your page. The name is then stored in a cookie. Next time the visitor arrives at your page, you could have another popup saying something like: "Welcome John Doe!".

onFocus, onBlur and onChange

The onFocus, onBlur and onChange events are often used in combination with validation of form fields.Below is an example of how to use the onChange event. The checkEmail() function will be called whenever the user changes the content of the field:

```
<input type="text" size="30" id="email" onchange="checkEmail()">;
```

onSubmit

The onSubmit event is used to validate ALL form fields before submitting it. Below is an example of how to use the onSubmit event. The checkForm() function will be called when the user clicks

the submit button in the form. If the field values are not accepted, the submit should be cancelled. The function checkForm() returns either true or false. If it returns true the form will be submitted, otherwise the submit will be cancelled:

<form method="post" action="xxx.htm"onsubmit="return checkForm()">

onMouseOver and onMouseOut

onMouseOver and onMouseOut are often used to create "animated" buttons. Below is an example of an onMouseOver event. An alert box appears when an onMouseOver event is detected.

13.6 JAVASCRIPT - CATCHING ERRORS

When browsing Web pages on the internet, a JavaScript alert box appears telling there is a runtime error and asking "Do you wish to debug?". Error message like this may be useful for developers but not for users. When users see errors, they often leave the Web page.

There are two ways of catching errors in a Web page:

- By using the **try...catch** statement (available in IE5+, Mozilla 1.0, and Netscape 6)
- By using the **onerror** event. This is the old standard solution to catch errors (available since Netscape 3)

Try...Catch Statement

The try...catch statement allows you to test a block of code for errors. The try block contains the code to be run, and the catch block contains the code to be executed if an error occurs.

Syntax

```
try
{
//Run some code here
}
catch(err)
{
//Handle errors here
}
```

Note that try...catch is written in lowercase letters. Using uppercase letters will generate a JavaScript error!

Example

The example below contains a script that is supposed to display the message "Welcome guest!" when you click on a button. However, there's a typo in the message() function. alert() is misspelled as **adddlert()**. A JavaScript error occurs:

```
<html>
<head>
<script type="text/javascript">
function message()
{
```

```
adddlert("Welcome guest!")
}
</script>
</head>
<body>
<input type="button" value="View message" onclick="message()" />
</body>
</html>
```

To take more appropriate action when an error occurs, you can add a try...catch statement.

The example below contains the "Welcome guest!" example rewritten to use the try...catch statement. Since alert() is misspelled, a JavaScript error occurs. However, this time, the catch block catches the error and executes a custom code to handle it. The code displays a custom error message informing the user what happened:

```
<html>
<head>
<script type="text/javascript">
var txt=""
function message()
{
try
{
 adddlert("Welcome guest!")
}
catch(err)
{
txt="There was an error on this page.\n\n"
txt+="Error description: " + err.description + "\n\n"
txt+="Click OK to continue.\n\n"
alert(txt)
}
}
</script>
</head>
<body>
<input type="button" value="View message" onclick="message()" />
</body>
</html>
```

JavaScript Throw Statement

The throw statement allows you to create an exception. If you use this statement together with the try...catch statement, you can control program flow and generate accurate error messages.

Syntax

```
throw(exception)
```

The exception can be a string, integer, Boolean or an object.

Note that throw is written in lowercase letters. Using uppercase letters will generate a JavaScript error!

Example

The example below determines the value of a variable called x. If the value of x is higher than 10 or lower than 0 we are going to throw an error. The error is then caught by the catch argument and the proper error message is displayed:

```
<html>
<body>
<script type="text/javascript">
var x=prompt("Enter a number between 0 and 10:","")
try
{
if(x>10)
throw "Err1"
else if(x<0)
throw "Err2"
}
catch(er)
{
if(er=="Err1")
alert("Error! The value is too high")
if(er == "Err2")
alert("Error! The value is too low")
}
</script></body>
</html>
```

JavaScript Special Characters

The table below lists special characters that can be added to a text string with the backslash sign:

Code	Outputs
\'	single quote
\"	double quote
\&	ampersand
\\	backslash
\n	new line
\r	carriage return
\t	tab
\b	backspace
\f	form feed

13.7 INTRODUCTION OF JAVASCRIPT OBJECTS

Object Oriented Programming

JavaScript is an Object Oriented Programming (OOP) language. An OOP language allows you to define your own objects and make your own variable types. Note that an object is just a special kind of data. An object has properties and methods.

Properties

Properties are the values associated with an object. In the following example we are using the length property of the String object to return the number of characters in a string:

```
<script type="text/javascript">
var txt="Hello World!"
document.write(txt.length)
</script>
```

The output of the code above will be: 12

Methods

Methods are the actions that can be performed on objects.

In the following example we are using the toUpperCase() method of the String object to display a text in uppercase letters:

```
<script type="text/javascript">
var str="Hello world!"
document.write(str.toUpperCase())
</script>
```

The output of the code above will be: HELLO WORLD!

JavaScript Form Validation

JavaScript can be used to validate input data in HTML forms before sending off the content to a server.

Form data that typically are checked by a JavaScript could be:

- has the user left required fields empty?
- has the user entered a valid e-mail address?
- has the user entered a valid date?
- has the user entered text in a numeric field?

Required Fields

The function below checks if a required field has been left empty. If the required field is blank, an alert box alerts a message and the function returns false. If a value is entered, the function returns true (means that data is OK):

```
function validate_required(field,alerttxt)
{
with (field)
{
if (value==null||value=="")
 {alert(alerttxt);return false}
else {return true}
}
}
```

E-mail Validation

The function below checks if the content has the general syntax of an email.

This means that the input data must contain at least an @ sign and a dot (.). Also, the @ must not be the first character of the email address, and the last dot must at least be one character after the @ sign:

```
function validate_email(field,alerttxt)
{
with (field)
{
apos=value.indexOf("@")
dotpos=value.lastIndexOf(".")
if (apos<1||dotpos-apos<2)
 {alert(alerttxt);return false}
else {return true}
}
}
```

JavaScript Timing Events

With JavaScript, it is possible to execute some code NOT immediately after a function is called, but after a specified time interval. This is called timing events. It's very easy to time events in JavaScript. The two key methods that are used are:

- setTimeout() - executes a code some time in the future
- clearTimeout() - cancels the setTimeout()

Note: The setTimeout() and clearTimeout() are both methods of the HTML DOM Window object.

setTimeout()

Syntax: var t=setTimeout("javascript statement",milliseconds)

The setTimeout() method returns a value - In the statement above, the value is stored in a variable called t. If you want to cancel this setTimeout(), you can refer to it using the variable name. The first parameter of setTimeout() is a string that contains a JavaScript statement. This statement could be a statement like "alert('5 seconds!')" or a call to a function, like "alertMsg()". The second parameter indicates how many milliseconds from now you want to execute the first parameter.

Example: When the button is clicked in the example below, an alert box will be displayed after 5 seconds.

```
<html>
<head>
<script type="text/javascript">
function timedMsg()
{
var t=setTimeout("alert('5 seconds!')",5000)
}
</script>
</head>
<body>
<form>
<input type="button" value="Display timed alertbox!" onClick="timedMsg()">
</form>
</body>
</html>
```

clearTimeout()

Syntax: clearTimeout(setTimeout_variable)

Example:

```
<html>
<head>
<script type="text/javascript">
var c=0
var t
function timedCount()
{
document.getElementById('txt').value=c
c=c+1
t=setTimeout("timedCount()",1000)
```

```
}
function stopCount()
{
clearTimeout(t)
}
</script>
</head>
<body>
<form>
<input type="button" value="Start count!"
onClick="timedCount()">
<input type="text" id="txt">
<input type="button" value="Stop count!"
onClick="stopCount()">
</form>
</body>
</html>
```

JAVASCRIPT OBJECTS

Earlier we have seen that JavaScript has several built-in objects, like String, Date, Array, and more. In addition to these built-in objects, you can also create your own. An object is just a special kind of data, with a collection of properties and methods. Let's illustrate with an example: A person is an object. Properties are the values associated with the object. The persons' properties include name, height, weight, age, skin tone, eye color, etc. All persons have these properties, but the values of those properties will differ from person to person. Objects also have methods. Methods are the actions that can be performed on objects. The persons' methods could be eat(), sleep(), work(), play(), etc.

Properties

The syntax for accessing a property of an object is:

objName.propName

You can add properties to an object by simply giving it a value. Assume that the personObj already exists - you can give it properties named firstname, lastname, age, and eyecolor as follows:

```
personObj.firstname="John"
personObj.age=30
personObj.eyecolor="blue"
document.write(personObj.firstname)
```

The code above will generate the following output: John

Methods

An object can also contain methods. You can call a method with the following **Syntax**:-
objName.methodName()

Note: Parameters required for the method can be passed between the parenthisis.

13.8 CREATING YOUR OWN OBJECTS

There are different ways to create a new object:

1. Create a direct instance of an object

The following code creates an instance of an object and adds four properties to it:

```
personObj=new Object()
personObj.firstname="John"
personObj.age=50
personObj.eyecolor="blue"
```

2. Create a template of an object

The template defines the structure of an object:

```
function person(firstname,lastname,age,eyecolor) {
this.firstname=firstname
this.lastname=lastname
this.age=age
this.eyecolor=eyecolor
}
```

Notice that the template is just a function. Inside the function you need to assign things to this.propertyName. The reason for all the "this" stuff in is that you're going to have more than one person at a time (which person you're dealing with must be clear). That's what "this" is: the instance of the object at hand. Once you have the template, you can create new instances of the object, like this:

```
myFather=new person("John","Doe",50,"blue")
myMother=new person("Sally","Rally",48,"green")
```

JavaScript String Object: The String object is used to manipulate a stored piece of text.

JavaScript Date Object: The JavaScript Date object is used to work with dates and times.

JavaScript Array Object: The JavaScript Array object is used to store a set of values in a single variable name.

JavaScript Boolean Object: The JavaScript Boolean object is an object wrapper for a Boolean value.

JavaScript Math Object: The JavaScript Math object allows you to perform common mathematical tasks. It includes several mathematical constants and functions.

JavaScript Top-level Properties and Functions: The top-level properties and functions that can be used on all of the built-in JavaScript objects.

13.9 HTML DOM OBJECTS

In addition to the built-in JavaScript objects, we can also access and manipulate all of the HTML DOM objects with JavaScript. The HTML DOM defines a standard set of objects for HTML, and a standard way to access and manipulate HTML documents.

JavaScript Objects

Follow the links to learn more about the objects and their collections, properties, methods and events. **Contain lots of examples!**

Object	Description
Window	The top level object in the JavaScript hierarchy. The Window object represents a browser window. A Window object is created automatically with every instance of a <body> or <frameset> tag
Navigator	Contains information about the client's browser Screen
Screen	Contains information about the client's display screen
Histroy	Contains the visited URLs in the browser window
Location	Contains information about the current URL

HTML DOM Objects

Follow the links to learn more about the objects and their collections, properties, methods and events. **Contain lots of examples!**

Object	Description
Documents	Represents the entire HTML document and can be used to access all elements in a page
Anchor	Represents an <a> element
Area	Represents an <area> element inside an image-map
Base	Represents a <base> element
Body	Represents the <body> element
Button	Represents a <button> element
Event	Represents the state of an event
Form	Represents a <form> element
Frame	Represents a <frame> element
Frameset	Represents a <frameset> element
Iframe	Represents an <iframe> element
Image	Represents an <img> element
Input button	Represents a button in an HTML form
Input checkbox	Represents a checkbox in an HTML form
Input file	Represents a fileupload in an HTML form
Input hidden	Represents a hidden field in an HTML form
Input password	Represents a password field in an HTML form
Input radio	Represents a radio button in an HTML form

Input reset	Represents a reset button in an HTML form
Input submit	Represents a submit button in an HTML form
Input text	Represents a text-input field in an HTML form
Link	Represents a <link> element
Meta	Represents a <meta> element
Option	Represents an <option> element
Select	Represents a selection list in an HTML form
Style	Represents an individual style statement
Table	Represents a <table> element
TableDAta	Represents a <td> element
Table row	Represents a <tr> element
TextArea	Represents a <text area> element

13.10 SUMMARY

JavaScript is a scripting language. A script is sequence of code doing some specific job. It is always included in <script></script> tag. Javscript makes a Web page Interactive. The document. write is the standard command to display the output to the web page. All the programming statements if-else, while etc can be included in the JavaScript. JavaScript also have some events like onBlur, onLoad, onChange etc which are put on different components and called the function when event is fired. JavaScript also uses the concepts of object oriented programming.object.propname is used for accessing the property of an object and object. Method () is used to call the method or function. In the end JavaScript uses HTML DOM objects like Anchor, Image, InputButton etc to make the web page dynamic and interactive.

13.11 UNIT END QUESTIONS

Write a java script for the following questions:

1. Write text with JavaScript
2. Format text with HTML tags
3. JavaScript in the head section
4. JavaScript in the body section
5. Declare a variable, assign a value to it, and display it
6. If statement, If...else statement, Random link, Switch statement.
7. Alert box, Alert box with line breaks
8. Call a function, Function with an argument, Function that returns a value, Function with arguments, that returns a value
9. For loop, Looping through HTML headers, While loop, Do While loop, Break a loop, Break and continue a loop, Use a for...in statement to loop through the elements of an array.
10. The try...catch statement, The try...catch statement with a confirm box, The onerror event
11. Timing event in an infinite loop
12. Timing event in an infinite loop - with a Stop button
13. A clock created with a timing event

14. Create a direct instance of an object
15. Create a template for an object

Reference Books:

1. Harley Hahn:The internet,Tata McGraw Hill.
2. Introduction to java and Web Technology:G.S Baluja,Dhanpat rai & sons.
3. Web Technology:c.Xavier,BPB Publication
4. Javascript for the World wide web:Tm Negrino,Pearson Education

UNIT - XIV

ACTIVE SERVER PAGES (ASP)

STRUCTURE OF THE UNIT

14.0 Objectives
14.1 Introduction
14.2 My First ASP Page
14.3 Server Side Scripting
14.4 Output, Variables and Forms
14.5 Operators in ASP
14.6 Control Structures
14.7 Subroutines
14.8 Session, Application and Cookies
14.9 The Dictionary Object
14.10 Global.asa
14.11 Summary
14.12 Unit end questions

14.0 OBJECTIVE

After completing this unit, you will be able to:

- display date, time, and other information in different ways.
- make a survey form and ask people who visit your site to fill it out.

14.1 INTRODUCTION

Active Server Pages or ASP, as it is more commonly known, is a technology that enables you to make dynamic and interactive web pages. ASP uses server-side scripting to dynamically produce web pages that are not affected by the type of browser the web site visitor is using. The default scripting language used for writing ASP is VBScript, although you can use other scripting languages like JavaScript.

ASP pages have the extension ".asp" instead of ".htm", when a page with the extension .asp is requested by a browser the web server knows to interpret any ASP contained within the web page before sending the HTML produced to the browser. This way all the ASP is run on the web server and no ASP will ever be passed to the web browser.

Any web pages containing ASP cannot be run, by just simply opening the page in a web browser. The page must be requested through a web server that supports ASP, this is why ASP stands for Active Server Pages, no server, no active pages.

14.2 MY FIRST ASP PAGE

As ASP is going to be displayed as part of a web page we first need to create an HTML web page, open up your favorite text editor and type the following:

<html>

<head>

```
<title>My First ASP Page</title>
</head>
<body bgcolor="white" text="black">
<%
DIM strMessage
strMessage = "Hello World"
Response.Write (strMessage)
Response.Write ("<br>")
Response.Write ("The time on the server is: " & Time())
%>
</body>
</html>
```

Server-side scripts look a lot like HTML tags. However, instead of starting and ending with less-than (<) and greater-than (>) brackets, they typically start with <% and end with %>. The <% is called an *opening tag*, and the %> is called a *closing tag*. In between these tags are the server-side scripts. You can insert server-side scripts anywhere in your Web page, even inside HTML tags.

Next, call the file, *'my_first_asp_page.asp'* (don't forget the *'.asp'* extension) and save the file to a directory accessible through your web server (this will usually be, *'c:\inetpub\wwwroot'*, on IIS or PWS with a default install). To display the page open your web browser and type *'http://my_computer/my_first_asp_page.asp'*, where *'my_computer'* is replace this with the name of your computer. And that's about it, you have now created your first dynamic ASP web page!

14.3 SERVER-SIDE SCRIPTING

Functions and Procedures

abs (*n*: number)	Function. Returns the absolute value of *n*.
chr (*asciicharcode*: number)	Function. Returns a string containing the ASCII character specified by *asciicharcode*.
date	Function. Returns the current system date as a string.
day (*thedate*: string)	Function. Extracts the day of the month from *thedate* and returns it as a number.
hour (*thetime*: string)	Function. Extracts the hour value from *thetime* and returns it as a number.
left (*thestring*: string, *n*: number)	Function. Returns a string containing the first *n* characters of *thestring*.
len (*thestring*: string)	Function. Returns the number of characters in *thestring*.
minute (*thetime*: string)	Function. Extracts the minutes value from *thetime* and returns it as a number.
month (*thedate*: string)	Function. Extracts the month value from *thedate* and returns it as a number.

monthname (*themonth*: number)	Function. Returns a string containing the name of the month whose number is specified by *themonth*. nowFunction. Returns the current system date and time.
Request.Form (*fieldname*: string)	Function. Returns the contents of the field whose name is *fieldname*.

ServerVariables

All available server variables may be obtained with the script below. Just save the script to your server and it will show you the values for each of the ServerVariables (use an url like http://www.yoursite.com/yourdir/servervariables.asp?a=hello&b=end)

```
<html>
<head>
<TITLE>Server Variables</TITLE>
</head>
<body bgcolor=FFFFFF>
<%
For Each Key in Request.ServerVariables
response.write Key & ": " &
                    request.servervariables(Key) & " <br><br>"
Next
%>
</body>
</html>
```

Request.ServerVariables ("HTTP_User-Agent")	Function. Returns the client browser type as a string.
Request.ServerVariables ("REMOTE_HOST")	Function. Returns the client's domain name as a string.
Request.ServerVariables ("SERVER_NAME")	Function. Returns the domain name of the server as a string. If the server has no domain name, returns the server's IP address as a string.

List of server variables

ALL_HTTP	ALL_RAW	APPL_MD_PATH
APPL_PHYSICAL_PATH	AUTH_PASSWORD	AUTH_TYPE
AUTH_USER	CERT_COOKIE	CERT_FLAGS
CERT_ISSUER	CERT_KEYSIZE	CERT_SECRETKEYSIZE
CERT_SERIALNUMBER	CERT_SERVER_ISSUER	CERT_SERVER_SUBJECT
CERT_SUBJECT	CONTENT_LENGTH	CONTENT_TYPE
GATEWAY_INTERFACE	HTTPS	HTTPS_KEYSIZE
HTTPS_SECRET_KEYSIZE	HTTPS_SERVER_ISSUER	HTTPS_SERVER_SUBJECT
INSTANCE_ID	INSTANCE_META_PATH	LOCAL_ADDR

LOGON_USER	PATH_INFO	PATH_TRANSLATED
QUERY_STRING	REMOTE_ADDR	REMOTE_HOST
REMOTE_USER	REQUEST_METHOD	SCRIPT_NAME
SERVER_NAME	SERVER_PORT	SERVER_PORT_SECURE
SERVER_PROTOCOL	SERVER_SOFTWARE	URL
HTTP_PRAGMA	HTTP_HOST	HTTP_COOKIE
HTTP_ACCEPT_ ENCODING	HTTP_VIA	HTTP_ACCEPT
HTTP_ACCEPT_ LANGUAGE	HTTP_ACCEPT_CHARSET	HTTP_REFERER
HTTP_X_FORWARDED_ FOR	HTTP_CACHE_CONTROL	HTTP_USER_AGENT
ASP_VERSION	ASP_VERSION_MAJOR	ASP_VERSION_MINOR
		ASP_OS

14.4 OUTPUT, VARIABLES and FORMS

Displaying Date and Time in ASP

In ASP there are many functions for displaying date, time and text and format them as you want this to appear in web page.

Date function is use to displaying current date in a web page at the position you want it to appear is, syntax of date function is:

<% =date %>

The output of this page could be viewed through a web browser as

[FRI, Jan 26, 2007]

The above syntax made up of two different parts:

(i) The "date" part would get the current date from your server.

(ii) The " = " sign command the server to display date in the web pages.

Time function is use to displaying current time in a web page at the position you want it to appear is, syntax of time function is:

<% =time %>

The output of this page could be viewed through a web browser as

[3:20:35 PM]

Now (Date and Time) function is use to displaying current date and time in a web page at the position you want it to appear is, syntax of now function is:

<% =now %>

The output of this page could be viewed through a web browser as

[1/26/2004 3:20:35 PM]

Formatting the Date and Time

Active Server Pages has functions to format the current date and time displayed on a web page. We use now function together with the following formatting functions:

<% =month(now) %>	To display the number of the current month
<% =monthname(month(now)) %>	To display the name of the current month
<% =day(now) %>	To display the day of the current month
<% =year(now) %>	To display the current year
<% =weekday(now) %>	To display the day of the week as a number from 1 to 7
<% =weekdayname(weekday (now)) %>	To display the day of the week by name
<% =hour(now) %>	To display just the hour part of the current time
<% =minute(now) %>	To display just the minutes part of the current time
<% =second(now) %>	To display just the seconds part of the current time

To display today's date as *day/month/year*

<% =day(now) %>/<% =month(now) %>/<% =year(now) %>

The output of the above function will be 26/1/2007

Use the following command in your web page

The time is <% =time %>. That means it's <% =minute(now) %> minutes past <% =hour(now) %> o'clock.

The Output of the above command will look like this:

The time is 3:20:35 PM. That means it's 20 minutes past 15 o'clock.

Timevalue function can be used to convert the time in ***"HH:MM:SS PM"*** format for the inputs taken in many different ways a person can write the time. This can be useful if you're using a function that needs to be given the time in that exact format. The syntax for the timevalue is:

<% =timevalue("Input Time") %>

When it's 20 minutes and 35 seconds past 3 o'clock in the afternoon. The timevalue function can be written as:

<% =timevalue("15:20:35") %>

or <% =timevalue("3:20:35PM") %>

or <% =timevalue("15:20:35PM") %>

Make sure you type "15:20:35PM" and not "15:20:35 PM." The "35" and the "PM." should be run together, not separated by a space. When you view the page in Internet Explorer, you should see:

3:20:35 PM

Displaying Text in ASP

The **len** function tells you how many characters are in a word or sequence of words. All characters are counted, including the space character. The syntax of len function is:

<% =len("The Black fox running over the wall") %>

The output will look like:

There are 35 characters in "The Black fox running over the wall"

The **left** function can be used to look at the first few characters of a word or sequence of words. The syntax of left function is:

<% =left("Reinforcement", 2) %>

The output will look like:

"Reinforcement" begins with the letters Re.

The **right** function used to look at the last few characters of a word or sequence of words, <% =right("Reinforcement, 4) %>.

The output will look like:

The last four characters of the word "Reinforcement" is "ment".

Creating a Variable

You'll probably want to do more with your forms than display their contents in a Web page. For example, based on the contents of the form, you may want to create a variable and insert that variable in different places of your response page. You may need to create a variable. To do that, just make up a name and set it equal to the contents of the field.

For example, if you have a field called "Name" in your form, you can save it into a variable called "TheName" by typing:

<% TheName = Request.Form("Name") %>

If you want to display "VisitorName" several times within a text you only need to include the variable in the text. For example:

My name is <% =TheName %>.

Do you want to see <% =TheName %>?.

Using Forms in Active Server Pages

Forms are a convenient way to communicate with visitors to your Web site. Using forms, you can create a survey form and ask visitors to fill it out. When they fill out the form, you can process the results automatically. With forms, there are two steps: first you create the form, and then you process it. To create a form for an Active Server Page, just create a standard HTML form. To try out this example, create an HTML file ("form_response.html") and cut-and-paste the following text into it.

<html>

<head><title>Asking for information</title></head>

<body>

<form method="post" action="form_response.asp">

Your name: <input type="text" name="name" size="20">

Your email: <input type="password" name="email" size="15">

<input type="Submit" value="Submit">

</form>

</body>

</html>

Active Server Pages provide a mechanism for processing forms that, unlike CGI scripting, doesn't involve serious programming: the Request.Form Considering the form above, we may create the file below and get a response.

```
<html>
<head><title>Responding to a form</title></head>
<body>
Your name is <% =Request.Form("name") %> <BR>
Your email is <% =Request.Form("email") %>
</body> </html>
```

To display the contents of each field in the form, type:

<% =Request.Form(*fieldname*) %>

where *fieldname* is the name of the field.

14.5 OPERATORS

The following operators are supported in ASP server-side scripts:

- *Addition (+)*
- *Assignment (=)*
- *Division (/)*
- *Is*
- *Greater Than (>)*
- *Less Than (<)*
- *Mod*
- *Negation (-)*
- *Not Equal To (<>)*
- *Subtraction (-)*
- *And*
- *Concatenation (&)*
- *Exponentiation (^)*
- *Equals (=)*
- *Greater Than or Equal to (>=)*
- *Less Than or Equal to (<=)*
- *Multiplication (*)*
- *Not*
- *Or*
- *Xor*

Arithmetical Operators: ^, *, /, \, +, -, parenthesis

Operators	ASP Command	Result
Exponentiation	<% Myresult = 2^2 response.write (Myresult) %>	4
Multiplication	<% Myresult = 2*2 response.write (Myresult) %>	4
Division	<% Myresult = 2.5/2 response.write (Myresult) %>	1.25
Integer Division	<% Myresult = 2.5\2 response.write (Myresult) %>	1
Addition	<% Myresult = 2+2 response.write (Myresult) %>	4
Subtraction	<% Myresult = 2-2 response.write (Myresult) %>	0
Parenthesis (to establish order of preference for operators)*		
<% Myresult = 5+3/2^4/2*5 response.write (Myresult) %>		5.46875 80
<% Myresult = (((5+3)/2)^(4/2))*5 response.write (Myresult) %>		80

* Without parenthesis the order or preference for operations is the order in the table:
  first: exponentiation
  second: multiplication and division
  third: addition and substraction

Logical operators: And, Or, Xor, Eqv, Imp, Not

val1 And val2	True if both are true
val1 Or val2	True if one or both are true
val1 Xor val2	True if only one is true
val1 Eqv val2	True if both are true or both are false
val1 Imp val2	True if val2 is true or both are false
Not val	True if val is false

There are two examples showing theuse of logical operators in ASP

Example

```
<%
V1=10
V2=20
V3=30
if NOT V1>V2 AND V2<V3 then
response.write ("Correct order")
else
response.write ("Incorrect order")
end if
%>
```

O/p is Correct Order

Example

```
<%
V1=10
V2=20
V3=30
if V1<V2 AND V2<V3 then
response.write ("Correct order")
else
response.write ("Incorrect order")
end if
%>
```

O/p is Correct Order

Comparison operators: =, <>, >, >=, <, <=

In order to perform comparisons, lets define some variables:

```
<%
V1=10
V2=10
V3=20
%>
```

The variables may be string in order to perform the Comparisons below.

= (equal)

```
<%
if V1=V2 then
response.write ("Response1")
else
response.write ("Response2")
end if  %>
```

O/p is Response 1

<> (different)

```
<%
if V1<>V2 then
response.write ("Response1")
else
response.write ("Response2")
end if  %>
```

O/p is Response 2

> (greater than)

```
<%
if V1>V3 then
response.write ("Response1")
else
response.write ("Response2")
end if  %>
```

O/p is Response 2

>= (greater or equal)

```
<%   if V1>=V3 then
response.write ("Response1")
else
response.write ("Response2")
end if  %>
```

O/p is Response 2

< (less than)

```
<%   if V1<V3 then
response.write ("Response1")
else
response.write ("Response2")
end if
%>
```

O/p is Response 1

<= (less or equal)

```
<%
if V1<=V2 then
response.write ("Response1")
else                                          O/p is Response 1
response.write ("Response2")
end if  %>
```

14.6 CONTROL STRUCTURES

If....Then...Else

The If....Then...Else instructions sequence is very similar to the one we may find in different kind of scripting languages. Let's check an example.

```
<%   AA="water"
     If AA="water" Then
      response.write ("I want to drink water")
     Else
      response.write ("I want to drink milk")
     End If  %>
```

We may use it this way:

```
<%   AA="water"
     If AA="water" Then %>
     I want to drink water
     <% Else %> I want to drink milk
     <% End If %>
```

In both cases we have checked a condition (AA="water"), and we have get a positive instruction (to write the sentence "I want to drink water"). We are allowed to execute any kind of instructions (including If....then....Else) and as many instructions as we want .

For....Next

This instruction is also similar with different programming languages. Let's see a typical example.

I want to say "Hello" 10 times

```
     <BR>
     <% For mynumber = 1 to 10 %>
     <% =mynumber %> Hello<BR>
     <% Next %>
     END
```

In this case we have defined a variable ("mynumber") and using the For...Next instruction we have repeated 10 times line 4. Similarly to If....Then....Else instruction, we are allowed to execute any kind of instructions and as many of them as we want .

The For...Next instruction allows us to define the value of the increment.

```
<% For mynumber = 1 to 20 STEP 2
response.write("Hello<BR>")
Next %>
<% For mynumber = 20 to 1 STEP -2
response.write("Hello<BR>")
Next %>
```

In both cases we will get the same response ("Hello" 10 times). The increment may be positive or negative as shown in the example.

Do While...Loop

Again, we will define a condition and one or more instructions:

```
<% mynumber=0
Do While mynumber<10
        response.write("Hello<HR>")
        mynumber=mynumber+1
Loop  %>
```

In this example the condition is "mynumber<10" and the instructions defines a response text and an increment of the variable "mynumber". In the example, mynumber will be increased until it gets a value of 10. Then the loop will be abandon. Several instruction may be used within the loop.

Do Until....Loop

Quite similar to the previous one, it also includes a condition and one or more instructions:

```
<%
mynumber=0
Do Until mynumber=10
        response.write("Hello<HR>")
        mynumber=mynumber+1
Loop  %>
```

In this example, the condition is "mynumber=10", so mynumber will increase until it is equal to 10, and then the loop will abandon.

Select Case....End Select

This is a very useful instruction in case we want to check different values for variable. Lets check an example:

```
<%
mynumber=3
Select Case mynumber
Case 1
   Response.write ("Number 1")
```

```
Case 2
    Response.write ("Number 2")
Case 3
    Response.write ("Number 3")
Case 4
    Response.write ("Number 4")
Case 5
    Response.write ("Number 5")
Case Else
    Response write ("Mynumber is higher than 5")
End Select  %>
```

In this example, we have defined mynumber as 3, so when they are executed the instructions satisfying the condition (in this case only one instruction is executed, but there may be several instructions). Case Else is optional and executed when no case matches.

14.7 SUBROUTINES

Subroutines have the same utility in ASP as it has in other languages. The use of subroutines may be very useful when there are a lot of instructions to be performed within a subroutine. This way it will allow us to simplify the structure of our script.

```
<%
    TheName=request.form("name)
    if TheName="John" then
    ResponseToJohn()
    else
    ResponseToUnknown()
    end if
    Sub ResponseToJohn()
    response.write ("Hi, John. How are you?")
    response.write ("<br>Did you know I got married last month?")
    End Sub
    Sub ResponseToUnknown()
    response.write ("Hi. How are you?")
    End Sub
%>
```

In order to call a subroutine, we will use this kind of code:

Whatever()

Where, "Whatever" is the name of the subroutine (it is recommended to use a very descriptive name of the task we want to perform within the subroutine to make it easier to understand the script). We may also provide information to the subroutine in order to perform the specified task.

The data will be provided this way:

Whatever (data1, data2 ... dataN)

subroutines are very useful to avoid repeating a specific number of tasks several times within the script, so that the script looks more organized and it is smaller.

14.8 SESSION, APPLICATION AND COOKIES

The Session method

The first time a user accesses to our pages some connections and disconnections took place. During this process the server and the client will interchange information to identify each other. Due to this exchange of information our server will be able to identify a specific user and this information may be use to assign specific information to each specific client. This relationship between computers is call a session. During the time a session is active, it is possible to assign information to a specific client by using Session method.

The Application method

With Session method we have defined a value for Session("whatever")="Joe", but this information can not be share between visitors (Session("whatever") has a unique value for each visitor). To allow sharing information Application method is used. Session and Application method has been used to create a simple chat script (copy and paste the code to your site and it will work immediately.

The Cookies method

This method is very similar to Session method: the basic difference is that with Cookies method the information is save in the clients computer and not in the server, so it is more suitable for sites with a lot of visitors. This method implies sending information to the client and requesting it whenever the information is needed. Additionally, we will learn how to delete the information save in the client's computer when it is not necessary anymore. When the visitor gets to our asp file we may save information related with him in his computer. The order will be like this one:

```
<% response.Cookies ("whatever")="information" %>
```

When this line is executed, the visitor will have the information in his computer, and whenever we need that information, we may request it using this code:

```
<% =request.Cookies ("whatever") %>
```

or

```
<% variable1=request.Cookies ("whatever") %>
```

14.9 THE DICTIONARY OBJECT

In order to learn how Dictionary object works we will create a small script which will translate number 1 to 10 from English to Spanish.

```
<%
SET MyDictionary=CreateObject("Scripting.Dictionary")
MyDictionary.Add "one","uno"
MyDictionary.Add "two","dos"
MyDictionary.Add "three","tres"
MyDictionary.Add "four","cuatro"
MyDictionary.Add "five","cinco"
MyDictionary.Add "six","seis"
```

```
MyDictionary.Add "seven","siete"
MyDictionary.Add "eight","ocho"
MyDictionary.Add "nine","nueve"
MyDictionary.Add "ten","diez"
EnglishNumber="four"
SpanishNumber=MyDictionary.Item (EnglishNumber)
Response.Write(SpanishNumber)
%>
```

How the script works

- First we have define a Dictionary named "Mydictionary".
- We have add to the dictionary the data corresponding to the different number in English and Spanish. When adding pairs of English and Spanish numbers to the Dictionary object, the number writen in English is a Key, and the number writen in Spanish a Item.
- Then, we have defined a variable named EnglishNumber and we have provided a value for this variable.
- Further, we have defined a new variable (SpanishNumber) and we get its value from the dictionary by indicating what we want to get the Item corresponding to a specific Key (EnglishNumber).
- Finally, the translated number is send to our visitor. The response will be "cuatro".

We may change the values in our dictionary by using the codes:

- MyDictionary.Key ("one")="1" In the original script the key "one" will be substitute by a new key value ("1"). The item "uno" will not be changed.
- MyDictionary.Item ("two")="2" In the original script the item corresponding to key "two" will be substitute by a new item value ("2"). The key "two" will not be changed.

We may display the number of element pairs in the dictionary by using the code "MyDictionary.Count".

14.10 GLOBAL.ASA

Global.asa is a text file locate in your main directory (/global.asa). Below is the basic structure of a global.asa file.

```
<SCRIPT LANGUAGE="VBScript" RUNAT="Server">
Sub Application_OnStart
.....
End Sub
Sub Application_OnEnd
.....
End Sub
Sub Session_OnStart
.....
End Sub
Sub Session_OnEnd
.....
End Sub
</SCRIPT>
```

This file will be activated in these cases:

- When the first visitor accesses our pages
- When a new session starts.

In both cases, we may determine a series of events to be executed in the file above.

1.	Application_OnStart	It is execute before the first session is started.
2.	Application_OnEnd	It is execute when the application is finished.
3.	Session_OnStart	It is execute when the server creates a new session (when a new client accesses our server).
4.	Session_OnEnd	It execute when a session is abandon or after certain period of time without contact between the client and the server (normally after 20 minutes or so from the last request from a specific client, the server will consider that user were come back, so it will delete all the information related to that session).

14.11 SUMMARY

Active Server Pages or ASP, as it is more commonly known, is a technology that enables you to make dynamic and interactive web pages. ASP uses server side scripting to dynamically produce web pages that are not affected by the type of browser. The default scripting language used for writing ASP is VBScript, although you can use other scripting languages like JavaScript.

14.12 UNIT END QUESTIONS

1. What do you mean by ASP? What are the advantages of using ASP?
2. What is the order of execution for an ASP application?
3. What are the various commands for formatting Date and Time?
4. What is the significance of Timevalue function?
5. How can you create variable in ASP?
6. What is the order of precedence for Logical Operators?
7. Discuss the various control structures used in ASP?
8. How does server identify and execute the server side scripts with in HTML code?
9. What is Global.asa file?
10. What is a session?
11. When is the Session_OnStart event fired?

REFERENCE BOOKS

1. Active Server Pages Programming : A concise course by A.Dedeke
2. Designing Active Server Pages : Scott Mitchell's Guide to write reusable code by Scott Mitchell
3. Active Server Pages 3.0 by example by Jeff Spotts
4. ASP Programming for the absolute beginner : The fun way to learn programming by John Gosney
5. ASP in a Nutshell : A desktop quick reference by A.Keyton Weissinger

UNIT - XV

ACTIVE SERVER PAGES (ASP) CONTD.

STRUCTURE OF THE UNIT

15.0 Objective
15.1 Arrays
15.2 Creating a table from data in a string
15.3 Sorting
15.4 Math Functions
15.5 Open, Read and Create Files
15.6 File System Objects
15.7 Create and Delete Folders
15.8 Get List of Files
15.9 Get List of Folders
15.10 Working with Databases
15.11 Summary
15.12 Unit end Questions

15.0 OBJECTIVE

After completing this unit, you will be able to:

- Working with arrays in ASP
- Open, Read and Create Files and File System Objects
- Open Datable

15.1 ARRAYS

Instead of having our information (variables or numbers) in variables like Mydata1, Mydata2, Mydata3 etc, by using arrays our information will be in an unique variable. Let´s check an example:

```
<html>
<title>My Array</title>
<body>
<%
DIM MyData(2,2)
MyData (0,0) = "1"
MyData (0,1) = "2"
MyData (0,2) = "3"
MyData (1,0) = "4"
MyData (1,1) = "5"
MyData (1,2) = "6"
MyData (2,0) = "7"
```

MyData	0	1	2
0	1	2	3
1	4	5	6
2	7	8	9

UNIT - XV

ACTIVE SERVER PAGES (ASP) CONTD.

STRUCTURE

15.0 Objective
15.1 Arrays
15.2 Creating a table from data in a string
15.3 Sorting
15.4 Math Functions
15.5 Open, Read and Create Files
15.6 File System Objects
15.7 Create and Delete Folders
15.8 Get List of Files
15.9 Get List of Folders
15.10 Working with Databases
15.11 Summary
15.12 Unit end Questions

15.0 OBJECTIVE

After completing this unit, you will be able to:

- Working with arrays in ASP
- Open, Read and Create Files and File System Objects
- Open Datable

15.1 ARRAYS

Instead of having our information (variables or numbers) in variables like Mydata1, Mydata2, Mydata3 etc, by using arrays our information will be in an unique variable. Let´s check an example:

```
<html>
<title>My Array</title>
<body>
<%
DIM MyData(2,2)
MyData (0,0) = "1"
MyData (0,1) = "2"
MyData (0,2) = "3"
MyData (1,0) = "4"
MyData (1,1) = "5"
MyData (1,2) = "6"
MyData (2,0) = "7"
```

MyData	0	1	2
0	1	2	3
1	4	5	6
2	7	8	9

```
MyData (2,1) = "8"
MyData (2,2) = "9"
Response.write (MyData (1,2))        %>
</body> </html>
```

In this example we have defined array named **Mydata** by using "**DIM**" and we have defined the size of the array. We may consider the table above as the source of information for our array. After defining the array we have assigned values to the array elements. In the response page, we will send the value assigned to MyData(1,2) in the array. The first number will be the row and the second the column, so that in our case the response page will show the value "6".

Very often, we will define an array from data obtained from a table with only one column. Let's check an example:

```
<html>
<title>My Array</title>
<body>
<%
DIM MyData(9)
MyData (0) = "0"
MyData (1) = "1"
MyData (2) = "2"
MyData (3) = "3"
MyData (4) = "4"
MyData (5) = "5"
MyData (6) = "6"
MyData (7) = "7"
MyData (8) = "8"
MyData (9) = "9"
Response.write (MyData (5))   %>
</body> </html>
```

MyData	
0	1
1	4
2	7
3	3
4	4
5	5
6	6
7	7
8	8
9	9

The table given above is the original table for the array in the script. In the response page we will send the value assigned to MyData(5) in the array. The response page will return 5. It is also possible to define an array with more dimensions as for example MyData(5,5,5,5).

Working with Arrays

In the examples above we have defined all the values within the script one by one, but this assignment may be done in a different ways, as it is described in the example bellow:-

```
<pre>
<%
MyArray=Array(Zero,one,two,three,four,five,six,seven,eight,nine)
%>
```

```
Thearray(0): <% =Thearray(0) %>
Thearray(1): <% =Thearray(1) %>
Thearray(2): <% =Thearray(2) %>
Thearray(3): <% =Thearray(3) %>
Thearray(4): <% =Thearray(4) %>
Thearray(5): <% =Thearray(5) %>
Thearray(6): <% =Thearray(6) %>
Thearray(7): <% =Thearray(7) %>
Thearray(8): <% =Thearray(8) %>
Thearray(9): <% =Thearray(9) %>
</pre>
```

In the above example the array has been create from a string, and each component of the array has been separated by a comma. The Array method will do it for us easily.

We may also want to use a different string with a different delimiter to define the components in our array:

```
<pre>
<%
TheText="Zero=one=two=three=four=five=six=seven=eight=nine"
Thearray=split (TheText,"=")    %>
Thearray(0): <% =Thearray(0) %>
Thearray(1): <% =Thearray(1) %>
Thearray(2): <% =Thearray(2) %>
Thearray(3): <% =Thearray(3) %>
Thearray(4): <% =Thearray(4) %>
Thearray(5): <% =Thearray(5) %>
Thearray(6): <% =Thearray(6) %>
Thearray(7): <% =Thearray(7) %>
Thearray(8): <% =Thearray(8) %>
Thearray(9): <% =Thearray(9) %>
</pre>
```

In this example we have defined the variable **TheText**, and whithin this variable, we have include a the strings separated by "=". In the next line, we have split the variable **TheText** into an array of strings (Thearray). **Split** command have been used to break **TheText** and "=" has been used as a delimiter to separate the substrings. In the response page we have indicated the individual values of **Thearray** one by one. It may happen to have a variable we want to split, but we do not know how many substrings we may get. In that case we may use **ubound** command to discover how many elements are in our array, and then we may use that value to write them by using a For-next loop (see example below).

```
<pre>
```

```
<%
TheText="a,f,w,d,u,t,e,u,f,v,o"
Thearray=split (TheText,"=")      %>
How many String do I have in TheArray?
<% =ubound(Thearray)+1 %>
<%
For n=0 to ubound(Thearray)
 Response.write (Thearray(n) & "<BR>")
next
%>
</pre>
```

Filtering values from a array

In the next example we will filter the information in our array, and we will display only part of it.

```
<pre>
<%
dim MyArray(9)
MyArray (0) = "Zero"
MyArray (1) = "One"
MyArray (2) = "Two"
MyArray (3) = "Three"
MyArray (4) = "Four"
MyArray (5) = "Five"
MyArray (6) = "Six"
MyArray (7) = "Seven"
MyArray (8) = "Eight"
MyArray (9) = "Nine" %>
Find strings containing "t" (case sensitive)
<% =join(filter(MyArray,"t",True,0),",") %>
Find strings containing "t"
<% =join(filter(MyArray,"t",True,1),",") %>
Find strings which do not contain "t" (case sensitive)
<% =join(filter(MyArray,"t",False,0),",")  %>
Find strings which do not contain "t"
        <% =join(filter(MyArray,"t",False,1),",") %>
</pre>
```

Output of the above example is:

Find strings containing "t" (case sensitive)	Eight
Find strings containing "t"	Two,Three,Eight
Find strings which do not contain "t" (case sensitive)	Zero, One, Two, Three, Four, Five, Six, Seven, Nine
Find strings which do not contain "t"	Zero, One, Four, Five, Six, Seven, Nine

The array and the assigment of values has been done as usual, and in the second part of the script we have used some lines similar to this one:

<% =join(filter(MyArray,"t",True,0),",") %>

In this lines we have filter the values at MyArray and we have join them.

filter (MyArray,"t",True,0)

This part of the line have search for "t" in MyArray. True means we have selected the strings containing the search string (in this case."t"). False will indicate that we are selecting the strings which do not contain the search string. 0 means our search is case sensitive (a binary comparison). 1 will mean it is not a case sensitive search (a textual comparison)

join(filter(MyArray,"t",True,0),",") The complete line will join the filtered strings with the delimiter indicated (in this case ",")

15.2 CREATING A TABLE FROM DATA IN A STRING

In order to understand this script we will consider we have a table like the one bellow, and that this table was the original source of information we used to create our table:

Peter	Student	Chicago	123
John	Teacher	London	234
Sue	Manager	Sidney	789

From the table we got these three lines by separating the values by commas:

Peter,	student,	Chicago,	123
John,	teacher,	London,	234
Sue,	Manager,	Sidney,	789

And finally we connected the three lines by separating the values with "/":

Peter, student, Chicago, 123 /John, teacher, London, 234 / Sue, Manager, Sidney, 789

The string obtained was saved to a variable named Mydata in the script bellow. The resulting page will show a table like the original. This script is not limited by number of rows or columns (the maximum amount of them is calculate each time we run the script).

<% Mydata="Peter, student, Chicago, 123 / John, teacher, London, 234/Sue, Manager, Sidney, 789"

Createtable()

%>

<%

Sub **CreateTable()**

MyRows=split (Mydata,"/")

```
RowsNumber=ubound(MyRows)
Response.write ("<table border=1>")
For i=0 to RowsNumber
DatainRow=split (MyRows(i),",")
NumberofDatainRow=ubound(DatainRow)
Response.write ("<tr>")
For n=0 to NumberofDatainRow
Response.write("<td>" & DatainRow(n) & "</td>")
Next
Response.write ("</tr>")
Next
Response.write ("</table>")
End Sub
%>
```

This script may be used for several purposes: we may generate Mydata by filtering values from an array as shown below:

```
<%
Dim Myclients(3)
Myclients(0)="Peter Smith,Chicago,Manager,123"
Myclients(1)="John Smith,New York,Accountant,124"
Myclients(2)="George Smith,Chicago,Administration,245"
Myclients(3)="Sam Smith,Dallas,Consultant,567"
SearchFor="Chicago" For Sorting in Ascending Order the script will be:
Mydata=join(filter(Myclients,SearchFor,True,1),"/")
Createtable()
%>
```

This code in combination with Createtable() Subroutine in the previous example will display only the clients from Chicago. The SearchFor variable may be obtained from a form.

15.3 SORTING: ASCENDING OR DESCENDING ORDER

In the following examples we will show how to order values in a array. The only difference between arrays below is indicated in bold:

to get ascending values,	if *MyArray(i)>MyArray(j)*, values will be replace by each other.
to get descending values,	if *MyArray(i)<MyArray(j)*, values will be replace by each other.

When comparing values, i will be always greater or equal to j. Scripts will work both for numbers

or string.

For Sorting in Ascending Order the script will be:

```
<%
        MyArray=Array(25,14,20,45,25,4,1,31,22,7)
        max=ubound(MyArray)
        For i=0 to max
          For j=i+1 to max
        if MyArray(i)>MyArray(j) then
        TemporalVariable=MyArray(i)
        MyArray(i)=MyArray(j)
        MyArray(j)=TemporalVariable
           end if
         next
        next
        Response.write ("The sorted values are those ones: <BR>")
        For i=0 to max
        Response.write (MyArray(i) & "<BR>")
        next
%>
```

For Sorting in descending Order the script will be:

```
<%
        MyArray=Array("John","Peter","Anna","Alberto","George",
        "Unai")
        max=ubound(MyArray)
        For i=0 to max
        For j=i+1 to max
        if MyArray(i)<MyArray(j) then
        TemporalVariable=MyArray(i)
        MyArray(i)=MyArray(j)
        MyArray(j)=TemporalVariable
        end if
        next
        next
        Response.write ("The sorted values are these ones: <BR>")
        For i=0 to max
        Response.write (MyArray(i) & "<BR>")
        next
%>
```

15.4 MATH FUNCTIONS

Function	Desription	Syntax
Abs(*number*)	Absolute value of a number	Abs(n)= <% =Abs(n) %>
Sin(*number*)	Sine of number (number must be in radians)	Sin(n)= <% =Sin(n) %>
Cos(*number*)	Cosine of number (number must be in radians)	Cos(n)= <% =Cos(n) %>
Tan(*number*)	Tangent of number (number must be in radians)	Tan(n)= <% =Tan(n) %>
Atn(*number*)	Arctangent of number (number must be in radians)	Atn(n)= <% =Atn(n) %>
Sqr(*number*)	Square of number (number must be positive)	Sqr(n)= <% =Sqr(n) %>
Fix(*number*) and Int(*number*)	Integer portion of number. Fix() and Int() will return different numbers for negative values.	Fix(n)= <% =Fix(n) %>
Log(*number*)	Natural logarithm of number	Log(n)= <% =Log(n) %>
Round(*number*)	Number rounded to an integer	Round(n)= <% =Round(n) %>
Round(*number, decimals*)	Number rounded to indicated decimal places	Round(n, m)= <% =Round(n,m)%>
Hex(*number*)	Conversion of number form base 10 to hexadecimal	Hex(n)= <% =Hex(n) %>
Oct(*number*)	Conversion of number form base 10 to octal	Oct(n)= <% =Oct(n) %>
Exp(*number*)	e raised to the power number	Exp(n)= <% =Exp(n) %>
Sgn(*number*)	Is the number positive or negative? • If positive value will be 1 • If negative value will be –1 • If number is 0, value will be 0	Sgn(n)= <% =Sgn(n) %>

15.5 OPEN, READ AND CREATE FILES

Open a text file

This one will be the basic code we need to open a text file:

```
<%
Set fs = CreateObject("Scripting.FileSystemObject")
Set wfile = fs.OpenTextFile("c:\Mydir\myfile.txt")
filecontent = wfile.ReadAll
wfile.close
Set wfile=nothing
Set fs=nothing
response.write(filecontent)      %>
```

The above script allows to perform the operation to open a text files in the server. We have defined a variable named "fs" to do it (we may change the name of this variable), then we have create a new variable named "wfile" and apply the method OpenTextFile to variable "fs". We

have also define which is the exact location of the file we want to open in this line (the complete path is necessary). We have read all the content of the file to a variable named "filecontent" using the instruction "ReadAll". Further wfile.close used to let the server know we have finished all operations involving files. Finally, response to the client with the content in the variable "filecontent" using "response.write".

Reading the Content of a Text File

We will consider a file with the following content:

learn.txt

1234567890

abcdefghij

ABCDEFGHIJ

We will read this file in different ways in order to use various commands available with filesystemobject.

Read (*number*) Will read number of characters specified (after reading position in the file will change)

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a=fso.OpenTextFile(Server.MapPath("\")&"/learn.txt")
mystring=a.Read(4)
Response.Write (mystring)
Response.Write ("<hr>")
mystring=a.Read(4)
Response.Write (mystring)
Set a = Nothing
Set fso = Nothing
%>
```

Output

1234

5678

ReadLine will read content in one line of the text file

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a=fso.OpenTextFile(Server.MapPath("\")&"/learn.txt")
mystring=a.readLine
Response.Write (mystring & "<BR>")
mystring=a.readLine
Response.Write (mystring & "<BR>")
mystring=a.readLine
```

```
Response.Write (mystring & "<BR>")
Set a = Nothing
Set fso = Nothing        %>
```

Output

1234567890
abcdefghij
ABCDEFGHIJ

ReadAll will read all the content in the text file

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a=fso.OpenTextFile(Server.MapPath("\")&"/learn.txt")
mystring=a.readAll
Response.Write (mystring & "<hr>")
Response.Write ("<pre>" & mystring & "</pre>")
Set a = Nothing
Set fso = Nothing        %>
```

Output

1234567890abcdefghijABCDEFGHIJ
1234567890
abcdefghij
ABCDEFGHIJ

Skip (number) Skip number of characters specified (after reading position in the file will change)

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a=fso.OpenTextFile(Server.MapPath("\")&"/learn.txt")
a.Skip(5)
mystring=a.read(8)
Response.Write mystring
Response.Write "<BR>"
a.Skip(1)
mystring=a.read(8)
Response.Write mystring
Set a = Nothing
Set fso = Nothing        %>
<HR>Line break is two characters
```

Output

67890 a

cdefghij

Line break is two characters

SkipLine Skips line in the text file (after reading position in the file will change)

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a=fso.OpenTextFile(Server.MapPath("\")&"/learn.txt")
a.SkipLine
mystring=a.readLine
Response.Write mystring
Set a = Nothing
Set fso = Nothing        %>
```

Output

abcdefghij

Column / Line will return position in the text file

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a=fso.OpenTextFile(Server.MapPath("\")&"/learn.txt")
a.Skip(15)
ColumnNumber=a.Column
Response.Write ("ColumnNumber: " & ColumnNumber & "<BR>")
LineNumber=a.Line
Response.Write ("LineNumber: " & LineNumber & "<BR>")
Set a = Nothing
Set fso = Nothing
%>
```

Output

ColumnNumber: 4

LineNumber: 2

AtEnd Of Line Will let us know when the line ends

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a=fso.OpenTextFile(Server.MapPath("\")&"/learn.txt")
While not a.AtEndOfLine
Response.write(a.Read(1) & "<BR>")
Wend
Set a = Nothing
Set fso = Nothing
%>
```

Output

1
2
3
4
5
6
7
8
9
0

AtEndOfStream Will let us know when the file ends

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a=fso.OpenTextFile(Server.MapPath("\")&"/learn.txt")
While not a.AtEndOfStream
Response.write(a.readline & "<BR>")
Wend
Set a = Nothing
Set fso = Nothing        %>
```

Output

1234567890
abcdefghij
ABCDEFGHIJ

Create and Write a text file

The basic code we need to create a file is very similar to that one we have used to open a file:

```
<%
thetext="Write this text in the file"
Set fs = CreateObject("Scripting.FileSystemObject")
Set wfile= fs.CreateTextFile("c:\Mydir\myfile.txt", True)
wfile.Write (thetext)
wfile.close
Set wfile=nothing
Set fs=nothing
response.write("Text created")          %>
```

The method used is "CreateTextFile"; it is necessary to indicate the complete path to the file we want to create and we may use the instruction True (to allow over-writing an existing file) or

False (if the file exists, it is not over-written). The script "wfile.Write" will write in the file the string variable "thetext".

We may also use this instruction to add content to the file

```
wfile.WriteLine (thetext1)
wfile.WriteLine (thetext2)
...
```

In this case we will write the content in variable "thetext1" in line 1, content in "thetext2" in line 2 etc.

15.6 FILE SYSTEM OBJECT

Get file related data: The following scripts is used to access the file related data

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a = fso.GetFile(Server.MapPath("\") & "\index.asp")
Response.Write("DateLastModified:" & a.DateLastModified & "<BR>")
Response.Write("DateLastAccessed:" & a.DateLastAccessed & "<BR>")
Response.Write("DateCreated: " & a.DateCreated & "<BR>")
Response.Write("Drive: " & a.Drive & "<BR>")
Response.Write("Name: " & a.Name & "<BR>")
Response.Write("ParentFolder:" & a.ParentFolder & "<BR>")
Response.Write ("Path: " & a.Path & "<BR>")
Response.Write ("ShortName: " & a.ShortName & "<BR>")
Response.Write ("ShortPath: " & a.ShortPath & "<BR>")
Response.Write ("Size: " & a.Size & "<BR>")
Response.Write ("Type: " & a.Type & "<BR>")
Response.Write ("Attributes: " & a.Attributes & "<BR>")
Set fileObject = Nothing
Set fso = Nothing        %>
```

Output

```
DateLastModified: 3/15/2002 3:03:32 AM
DateLastAccessed: 4/15/2002 7:45:01 AM
DateCreated: 4/1/2002 1:55:11 PM
Drive: e:
Name: index.asp
ParentFolder: E:\clientsites\codedcode.com
Path: E:\clientsites\codedcode.com\index.asp
ShortName: index.asp
ShortPath: E:\clientsites\ASPTUT~1.INF\index.asp
```

Size: 359

Type: ASP auto file

Attributes: 32

Get folder related data: The following scripts is used to access the folder related data

```
<%
Set fso = CreateObject("Scripting.FileSystemObject")
Set a = fso.GetFolder(Server.MapPath("\tryit\"))
Response.Write("DateLastModified:" & a.DateLastModified & "<BR>")
Response.Write("DateLastAccessed:" & a.DateLastAccessed & "<BR>")
Response.Write("DateCreated: " & a.DateCreated & "<BR>")
Response.Write("Drive: " & a.Drive & "<BR>")
Response.Write("Name: " & a.Name & "<BR>")
Response.Write("ParentFolder:" & a.ParentFolder & "<BR>")
Response.Write("Path: " & a.Path & "<BR>")
Response.Write("ShortName: " & a.ShortName & "<BR>")
Response.Write("ShortPath: " & a.ShortPath & "<BR>")
Response.Write("Size: " & a.Size & "<BR>")
Response.Write("Type: " & a.Type & "<BR>")
Response.Write("Attributes: " & a.Attributes & "<BR>")
Response.Write("IsRootFolder:" & a.IsRootFolder & "<BR>")
' to get list of files here
' to get list of folders here
Set a = Nothing
Set fso = Nothing        %>
```

Output

DateLastModified: 4/15/2002 7:23:17 AM

DateLastAccessed: 4/15/2002 7:23:20 AM

DateCreated: 2/4/2002 3:39:18 AM

Drive: e:

Name: prueba

ParentFolder: E:\clientsites\codedcode.com

Path: E:\clientsites\codedcode.com\tryit

ShortName: tryit

ShortPath: E:\clientsites\AspPk.INF\tryit

Size: 43940

Type: File Folder

Attributes: 48

IsRootFolder: False

15.7 CREATE AND DELETE FOLDERS

In those examples we will create and delete a subdirectory within cgi-bin directory in our site. Many often we will have permission to perform this operations only in this directory.

Create subdirectory "myfiles"

```
<%
Foldertocreate=server.mappath("\") &"/cgi-bin/myfiles"
Set fs = CreateObject("Scripting.FileSystemObject")
Set a = fs.CreateFolder(Foldertocreate)
Set fs=nothing
%>
Done
```

Delete subdirectory "myfiles"

```
<%
Foldertodelete=server.mappath("\") &"/cgi-bin/myfiles"
Set fs = CreateObject("Scripting.FileSystemObject")
fs.DeleteFolder(Foldertodelete)
Set fs=nothing
%>
Done
```

Delete a folder only in case it exists (to avoid errors)

```
<%
Foldertodelete=server.mappath("\") &"/cgi-bin/myfiles"
Set fs = CreateObject("Scripting.FileSystemObject")
if fs.FolderExists("c:\temp") then
fs.DeleteFolder "c:\temp"
end if
Set fs=nothing          %>
Done
```

15.8 GET LIST OF FILES

List of Files within main folder

```
<%
Whichfolder=server.mappath("\") &"/"
Dim fs, f, f1, fc
Set fs = CreateObject("Scripting.FileSystemObject")
Set f = fs.GetFolder(Whichfolder)
Set fc = f.files
For Each f1 in fc
```

```
Response.write (f1.name & "<BR>")
Next
%>
```

List of files within "cgi-bin" folder

```
<%
Whichfolder=server.mappath("\") &"/cgi-bin/"
Dim fs, f, f1, fc
Set fs = CreateObject("Scripting.FileSystemObject")
Set f = fs.GetFolder(Whichfolder)
Set fc = f.files
For Each f1 in fc
Response.write (f1.name & "<BR>")
Next
%>
```

15.9 GET LIST OF FOLDERS

List of Subfolders within main folder

```
<%
Whichfolder=server.mappath("\") &"/"
Dim fs, f, f1, fc
Set fs = CreateObject("Scripting.FileSystemObject")
Set f = fs.GetFolder(Whichfolder)
Set fc = f.subfolders
For Each f1 in fc
Response.write (f1.name & "<BR>")
Next
%>
```

List of subfolders within "cgi-bin" folder

```
<%
Whichfolder=server.mappath("\") &"/cgi-bin/"
Set fs = CreateObject("Scripting.FileSystemObject")
Set f = fs.GetFolder(Whichfolder)
Set fc = f.subfolders
For Each f1 in fc
Response.write (f1.name & "<BR>")
Next
%>
```

15.10 WORKING WITH DATABASES

Before we get into opening databases, I would like to take a moment to discuss the basic structure of the ASP model. Using VBScript, we have access to all the standard VB script objects, any ActiveX DLL's we make in VB5 - and the standard ASP objects. The two most important standard ASP objects are the Request and Response objects.

- The Request objects allows you to interrogate the URL command line, request.querystring("key"). To request information from a form, request.form("inputname"). Also to retrieve cookies (data stored on the clients machine), request.cookies("key")("data").
- The Response object allows you to write to the HTML file. A shorthand version of Response.write "string" is to just simply use an =, as the for next example above does. Also you can write a cookie, response.cookies("adv")("data")="string".

Opening a Database

First you need to create a database in Microsoft Access, or another database that provides an ODBC driver. Then you should go into the ODBC32 icon in your control panel, and add another system file. The name you give your database is used to find it when you open an ODBC source as below.

```
Set Conn = Server.CreateObject("ADODB.Connection")
Conn.Open "your database name"
```

Now you have established a connection to the database we can start to use SQL to retrieve the data.

The next statement builds a quick read only recordset for you to navigate;

```
set RS  = Conn.Execute("SELECT * FROM [table]
          WHERE [field]=1")
```

You can then step through the record in the recordset, say writing them to your web page like this;

```
If not RS.eof then
RS.movefirst
Do
    Response.write "Here is some Data" & RS("Field")
    Rs.movenext
Loop until RS.eof
End if
```

When you have to add or edit records, you have to create an explicit object from the ADO object like so;

```
Const adLockOptimistic = 3
Const adOpenKeyset = 1
Set RS = server.createobject("ADODB.Recordset")
set RS.ActiveConnection = Conn
RS.Open "SELECT * FROM [table]" , , adOpenKeyset, adLockOptimistic
```

```
RS.addnew
RS("field")="NewStuff"
RS.update
RS.close
set RS = nothing
```

15.11 SUMMARY

In this unit you are able to understand the basic functions of arrays like creating a table from data, filtering values from an array, sorting arrays in ascending and descending order, math function. You can open, read and create text files on server. You are also aware with FileSystemObject object and working with files and folders.

15.12 UNIT END QUESTIONS

1. What are Arrays? What is the maximum size of an array?
2. How can you resize an array?
3. How can you filter values from an array?
4. Discuss method for table creation from the data in a string.
5. Write down the ASP code to sort data of an array in ascending and descending order.
6. What are math function? List some of them.
7. What is a FileSystemObject object?
8. Write codes to perform the following:-
   (i) Open a text file
   (ii) Read a text file
   (iii) Write a text file
9. How can you create and delete a subdirectory within cgi-bin directory?
10. Write down the ASP code for opening a database.

REFERENCE BOOKS

1. Active Server Pages Programming : A concise course by A.Dedeke
2. Designing Active Server Pages : Scott Mitchell's Guide to write reusable code by Scott Mitchell
3. Active Server Pages 3.0 by example by Jeff Spotts
4. ASP Programming for the absolute beginner : The fun way to learn programming by John Gosney
5. ASP in a Nutshell : A desktop quick reference by A.Keyton Weissinger