UNIT 1 THE INTERNET

Structure **Page No.**

1.0 INTRODUCTION

The Internet is worldwide computer network that interconnects, million of computing devices throughout the world. Most of these devices are PC's, and servers that store and transmit information such as web pages and e-mail messages. Internet is revolutionizing and enhancing the way we as humans communicate, both locally and around the globe. Everyone wants to be a part of it because the Internet literally puts a world of information and a potential worldwide audience at your fingertips.

The Internet evolved from the ARPANET (Advanced Research Projects Agency) to which other networks were added to form an inter network. The present Internet is a collection of several hundred thousand of networks rather than a single network. From there evolved a high-speed backbone of Internet access for sharing these of networks. The end of the decade saw the emergence of the World Wide Web, which heralded a platform-independent means of communication enhanced with a pleasant and relatively easy-to-use graphical interface.

World Wide Web is an example of an **information protocol/service** that can be used to send and receive information over the Internet. It supports:

- **Multimedia Information** (text, movies, pictures, sound, programs . . .).
- **HyperText Information** (information that contains links to other information resources).
- **Graphic User Interface** (so users can point and click to request information instead of typing in text commands).

The **World Wide Web** model follows **Cient/Server** software design. A service that uses client/server design requires two pieces of software to work: **Client Software**, which you use to request information, and **Server Software**, which is an **Information Provider.**

The server software for the World Wide Web is called an **HTTP server** (or informally a Web server). Examples are **Mac HTTP, CERN HTTP, and NCSA HTTP.** The client software for World Wide Web is called a Web browser. Examples are: **Netscape, and Internet Explorer.**

1.1 OBJECTIVES

After going through this unit students should be able to:

- Make classification of networks;
- understand two types of networking models;
- understand the concept of packet switching;
- understand how to access to the internet;
- list the services available on Internet; and
- understand how does the Internet works.

1.2 CLASSIFICATION OF NETWORKS

There are different approaches to the classification of compute Networks. One such classification is based on the distance approach. In this section we will discuss such networks.

The networks can be classified into LAN, MAN and WAN networks. Here, we describe them into brief to understand the difference between the types of network.

Local Area Network (LAN)

LAN is a privately - owned computer networks confined to small geographical area, such as an office or a factory widely used to connect office PCs to share information and resources. In a Local area network two or more computers are connected by same physical medium, such as a transmission cable. An important characteristic of Local Area networks is speed. i.e. they deliver the data very fast compared to other types of networks with typical data transmission speed are 10-100 Mbps.

A wide variety of LANs have been built and installed, but a few types have more recently become dominant. The most widely used LAN system is the Ethernet system. Intermediate nodes (i.e. repeaters, bridges and switches) allow LANs to be connected together to form larger LANs. A LAN may also be connected to another LAN or to WANs and MANs using a "router".

In summary, a LAN is a communications network, which is:

- local (i.e. one building or group of buildings)
- controlled by one administrative authority
- usually high speed and is always shared

LAN allows users to share resources on computers within an organization.

Metropolitan Area Network (MAN)

A MAN, basically a bigger versions of a LAN is designed to extend over an entire city. It may be single network such as a cable television network, or it may be a means of connecting a number of LANs into a large network so that resources may be

shared for example, a company can use a MAN to connect the LANs in all of its offices throughout a city.

A MAN typically covers an area of between 5 and 50 km diameter. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings

The MAN, its communications links and equipment are generally owned by either a consortium of users or by a single network provider who sells the service to the users. This level of service provided to each user must therefore be negotiated with the MAN operator, and some performance guarantees are normally specified.

A MAN often acts as a high-speed network to allow sharing of regional resources (similar to a large LAN). It is also frequently used to provide a shared connection to other networks using a link to a WAN.

Wide Area Network (WAN)

The term Wide Area Network (WAN) usually refers to a network, which covers a large geographical area, and use communications subnets (circuits) to connect the intermediate nodes. A major factor impacting WAN design and performance is a requirement that they lease communication subsets from telephone companies or other communications carriers. Transmission rates are typically 2 Mbps, 34 Mbps, 155 Mbps, 625 Mbps (or sometimes considerably more). The basic purpose of the subnet is to transmit message from one end to another end through intermediate nodes.

In most WAN a subnet consists of two types of elements: (i) Transmission lines (ii) Switching element.

Transmission lines also called channels move about from one machine to another machine. The basic purpose of the switching element is to select the outgoing path for forwarding the message.

Numerous WANs have been constructed, including public switched networks, large corporate networks, military networks, banking networks, stock brokerage networks, and airline reservation networks. A WAN is wholly owned and used by a single company is often referred to as an enterprises network.

1.3 NETWORKING MODELS

There are two types of networking models available: OSI reference Model and the TCP/IP Network Model for the design of computer network system. In this section we shall look at these models.

OSI (Open System Interconnection) Networking Model

An open system is a model that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to open communication between different devices without requiring changes to the logic of the underlying hardware and software.

The OSI model is not a protocol, it is a model for understanding and designing a network architecture that is inter- operable, flexible and robust.
The OSI model has a seven-layered architecture. These are:

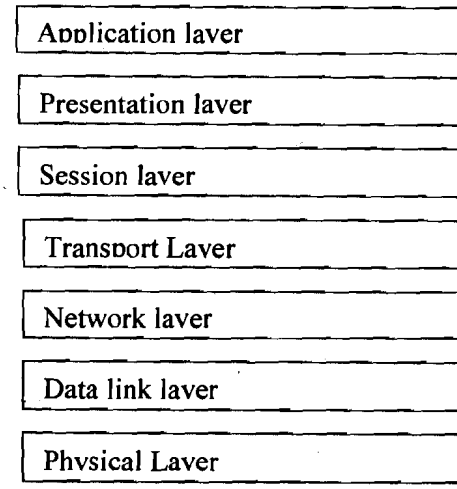

Figure 1: OSI Model

Physical layer: the physical layer is concerned with sending raw bits between the source and destination nodes over a physical medium. The source and destination nodes have to agree on a number of factors.

Signal encoding: how are the bits 0 and 1 to be represented?

Medium: what is the medium used and its properties?

Bit synchronization: is the transmission synchronous or asynchronous?

Transmission type: whether the transmission is serial or parallel?

Transmission mode: is the transmission simplex, half-duplex or full duplex?

Topology: what is the network topology i.e. star, mesh, ring or bus?

Data link layer: the data link layer is responsible for transmitting a group of bits between the adjacent nodes. The group of bits is known as frame. The network layer passes a data unit to the data link layer and data link layer adds the header information to this data unit. The data link layer performs the following functions:

- **Addressing:** Headers and trailers are added containing the physical addresses of the adjacent nodes and removed on a successful delivery.
- **Framing:** Grouping of/bits received from the network layer into manageable units called frame
- **Flow control:** to regulate the amount of data that can be sent to the receiver.
- **Media access control (MAC):** who decide who can send data, when and how much.
- **Synchronization:** this layer also contains bits to synchronize the timing to know the bit interval to recognize the bit correctly.
- **Error control:** it incorpoprates the CRC to ensure the correctness of the frame.
- **Node to node delivery:** it's also responsible for error-free delivery of the entire frame/packet to the next adjacent node.

Network layer: The network layer is responsible for routing a packet within the subnet that is, from source to destination nodes across multiple nodes in the same network or across multiple networks. This layer also ensures the successful delivery of a packet to the destination node. The network layer performs the following functions:

- Routing: To find the optimal route

- Congestion control: which is based on two approaches (i) Increase on the resources (ii) Decrease the word
- Accounting and billing

Transport layer: this layer is the first end-to-end layer. Header of the transport layer contains information that helps send the message to the corresponding layer at the destination node. The message is broken into packets and may travel through a number of intermediate nodes. This layer takes care of error control and flow control both at the source and destination for the entire message. The responsibilities of the transport layer are:

- Host-to-host message delivery
- Flow Control
- Segmentation and reassembly

Session layer: the main functions of this layer are to establish, maintain and synchronize the interaction between two communication hosts. It makes sure that once a session is established it must be closed gracefully. It also checks and establishes connections between the hosts of two different users. The session layer also decides whether both users can send as well as receive data at the same time or whether only one host can send and the other can receive. The responsibilities of session layer are:

- **Sessions and sub sessions:** this layer divides a session into sub session for avoiding retransmission of entire message by adding the checkpoint feature.
- **Synchronization:** this layer decides the order in which data needs to be passed to the transport layer.
- **Dialog control:** this layer also decides which user application sends data and at what point of time and whether the communication is simplex, half duplex or full duplex.
- **Session closure:** this layer ensures that the session between the hosts is closed gracefully.

Presentation layer: when two hosts are communicating with each other they might use different coding standards and character sets for representing data internally. This layer is responsible for taking care of such differences. This layer is responsible for:

- Data encryption and decryption for security
- Compression
- Translation

Application layer: it's the topmost layer in the OSI model, which enables the user to access the network. This layer provides user interface for network applications such as remote login, World Wide Web and FTP. The responsibilities of the application layer are:

- File access and transfer
- Mail services
- Remote login
- World Wide Web

TCP/IP Networking Model

TCP/IP is an acronym for Transmission Control Protocol / Internet Protocol. TCP/ IP is a collection of protocols, applications and services. TCP/IP protocol were developed prior to the OSI model therefore its layers do not match with the OSI model.

The TCP/IP protocol suit is made of the five layers: Physical, data link, network, transport & application. The first four layers provide physical standards network

interface, internetworking and transport mechanism whereas the last layer comprises of the functionalities of the three topmost layers in the OSI model.

1.4 WHAT IS A PACKET SWITCHING?

End systems are connected together by communication links. There are many types of communication links, which are made of different types of physical media, including fiber optics, twisted pair, coaxial cable and radio links. Different links can transmit data at different rates. The link transmission rate is often called the bandwith of the link, which is typically measured in bits/second. The highest the bandwith, the more is the capacity of the channel. End systems are not usually directly attached to each other via a single communication link. Instead, they are indirectly connected to each other through intermediate switching devices known as routers. A router takes a chunk of information arriving on one of its incoming communication links and forwards that chunk of information on one of its outgoing communication links. In the jargon of computer networking, the chunk of information is called a packet. The path that the packet takes from the sending end system, through a series of communication links and routers, to the receiving end system is known as a route or path through the network. Rather than providing a dedicated path between communicating end systems, the Internet uses a technique known as packet switching that allows multiple communicating end systems to share a path, or parts of a path, at the same time. Similar to a router, there is another special machine called gateways used in the network that allows different networks to talk to the Internet, which uses TCP/IP.

Packet switching is used to avoid long delays in transmitting data over the network. Packet switching is a technique, which limits the amount of data that a computer can transfer on each turn. Packet switching allows many communications to proceed simultaneously. Each packet contains a header that specifies the computer to which the packet should be delivered and the destination is specified using computer's address. Computers that share access to a network take turns in sending packets. On each turn, a given computer sends one packet. IP uses this packet switching concept to deliver messages on the Internet If the destination address does not exist on the local network, it is the responsibility of that network's router to route the message one step closer to its destination. This process continues until the destination machine claims the message packet.

1.5 ACCESSING THE INTERNET

Before we can use the Internet, we have to gain access to it. This access is achieved in one of several ways, which we will discuss in this section. Above all, the Internet is a collection of networks that are connected together through various protocols and hardware.

Dial-up Connection: one of the commonest ways of connection to Internet is through dial up connection using a modem and a telephone line. Using these you can connect to a host machine on the Internet. Once connected the telecommunications software allows you to communicate with the Internet host. When the software runs it uses the modem to place a telephone call to a modem that connects to a computer attached to the Internet.

The SLIP (Serial Line Internet Protocol) or PPP (Point to Point Protocol): two protocols; **serial line interface protocol (SLIP)** and the **point-to-point protocol (PPP),** 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 of the Internet's facilities.

Internet Service Providers

As mentioned earlier, nobody truly owns the Internet, but it is maintained by a group of volunteers interested in supporting this mode of information interchange. Central to this control is the Internet service provider (ISP) which 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 systems, 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 worldwide Internet content, these lower-tier ISPs are interconnected through national and international upper-tier ISPs, such as Sprint. 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 (see below), and conforms to certain naming and address conventions.

ISDN (Integrated Services Digital Network) Service

The whole idea of ISDN is to digitize the telephone network to permit the transmission of audio, video and text over existing telephone lines. The purpose of the ISDN is to provide fully integrated digital services to users.

The use of ISDN for accessing the Internet has breathed new life into the ISDN service. ISDN's slow acceptance was due mostly to a lack of a need for its capabilities. Being a digital interface, ISDN has provided a means for accessing web sites quickly and efficiently. In response to this new demand, telephone companies are rapidly adding ISDN services.

The ISDN standard defines three channels types, each with the different transmission rate: bearer channel (B), data channel (D) and hybrid channel (H) (see the following table)

Channel	Data Rate (Kbps)
B	64
D	16, 64
H	384, 1536, 1920

The B channel is defined at a rate of 64 Kbps. It is the basic user channel and can carry any type of digital information in full duplex mode as long as the required transmission does not exceed 64 kbps. A data channel can be either 16 or 64 kbps depending on the needs of the user used to carry control signals for B channels.

Of the two basic rate B channels, one is used to upload data to the Internet and one to download from the Internet. The D Channel assists in setting up connection and maintaining flow control. There are three ways ISDN can be used to interface to the Internet, by using a modem, adaptor, or bridge/router. ISDN modems and adaptors limit access to a single user. Both terminate the line into an ISDN service. The difference between them is that the ISDN modem takes the Internet traffic and pushes it through the computer serial port, while, the faster ISDN adaptor connects directly to the computer's buses.

ISDN bridge/routers allow for local network connections to be made through ISDN to the Internet. The ISDN termination is made into an Ethernet-type LAN so that multiple users can achieve access to the Net through a single access address. Transfer rates between user and the Internet are between 56 and 128 Kbps.

Direct ISP Service through Leased Line

The most costly method of accessing the Internet is to use leased lines that connect directly to the ISP. This will increase access rate to anywhere between 64 K and 1.5 Mbps, depending on the system in use. Equipment called data service units (DSU) and channel service units (CSU) are set up in pairs, one pair at the customer site and the 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 cables or unshielded twisted-pair (UTP) copper wire.

Cable Modem

One more way of accessing the Internet currently being developed is the use of cable modems. These require that you subscribe to a cable service and allow you two-way communication with the Internet at rates between 100K and 30 Mbps. The cable modem performs modulation and demodulation like any other modem, but it also has a tuner and filters to isolate the Internet signal from other cable signals. Part of the concern for use of the cable modem is to formulate LAN adapters to allow multiple users to access the Internet. A medium access control (MAC) standard for sending data over cable is being formulated by the IEEE 802.14 committee.

1.6 INTERNET PROTOCOLS

A communication protocol is an agreement that specifies a common language two computers use to exchange messages. For example, a protocol specifies the exact format and meaning of each message that a computer can send. It also specifies the conditions under which a computer should send a given message and how a computer should respond when a message arrives. Different types of protocols are used in Internet such as IP and TCP. A computer connected to the Internet needs both TCP and IP software. IP provides a way of transfering a packet from its source to destination and TCP handles the lost datagrams and delivery of datagrams. Together, they provide a reliable way to send data across the Internet. We discuss about these protocols in brief in the following section.

1.6.1 Internet Protocol (IP)

The Internet protocol specifies the rules that define the details of how computers communicate. It specifies exactly how a packet must be formed and how a router must forward each packet on toward its destination. Internet Protocol (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. When sending or receiving data, the message gets divided into little chunks called packet. Each of these packets contains both the senders Internet address and the receiver's address. The packet that follows the IP specification is 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 the 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 the datagram must be sent across another network, the router creates a new network packet, encloses the datagram inside the packet and sends the packet across another network toward 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 send each packet across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another

protocol, the Transmission Control Protocol to put them back in the 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 travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

1.6.2 Transmission Control Protocol (TCP)

TCP makes the Internet reliable. TCP solves many problems that can occur in a packet switching system. TCP provide the following facilities:

- TCP eliminates duplicate data.
- TCP ensures that the data is reassembled in exactly the order it was sent
- TCP resends data when a datagram is lost.
- TCP uses acknowledgements and timeouts to handle problem of loss.

The main features of TCP are:

Reliability: TCP ensures that any data sent by a sender arrives at the destination as it was sent. There cannot be any data loss or change in the order of the data. Reliability at the TCP has four important aspects:

- Error Control
- Loss control
- Sequence control
- Duplication control

Connection-oriented: TCP is connection-oriented. Connection-oriented means a connection is established between the source and destination machines before any data is sent i.e. a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. The connections provided by TCP are called Virtual Connections. It means that there is no physical direct connection between the computers.

TCP is used along with the Internet Protocol 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 Packet) that a message is divided into for efficient routing through the Internet. TCP provides for a reliable, connection-oriented data transmission channel between two programs. Reliable means that data sent is guaranteed to reach its destination in the order sent or an error will be returned to the sender.

For example, when an HTML file is sent to someone from a Web server, the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end (the client program in our computer), TCP reassembles the individual packets and waits until they have arrived to forward them as a single file.

TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

Check Your Progress 1

1. State whether True or False:

   a) Internet is a Global network and is managed by a profit-oriented organization.
   b) TCP does not control duplication of packets.
   c) For logging in to Internet you must have an account on its host machine.
   d) A router is used at the network layer.
   e) Internet provides only one-way communication.

2. What are the different layers in the TCP/IP networking Model?
3. Describe the facilities provided by the TCP?

1.7 INTERNET ADDRESS

Addresses are essential for virtually everything we do on the Internet. The IP in TCP/IP is a mechanism for providing addresses for computers on the Internet. Internet addresses have two forms:

- Person understandable which is expressed as words
- Machine understandable which is expressed as numbers

The following can be a typical person understandable address on Internet:

VVS @ ignou.ac.in

VVS is an username which in general is the name of the Internet account. This name is same as the one, which you may use when logging into the computer on which you have your Internet account. Logging in is the process of gaining access to your account on a computer, which is shared by several users. Your Internet account is created on it.

@ Connect "who" with where:

.ignou is a subdomain (could be several in each could be separated by (dot). Last one is referred to a domain).

.edu is a domain top or what part in – It refers to "where" part which is a country code.

1.7.1 Structure of Internet Servers Address

The structure of an Internet server's address keyed into a client's software is as follows:

http://www.microsoft.com

Where:

http is the communication protocol to be used
www is the notation for World Wide Web
.Microsoft is the registered domain Name associated with the IP address of an Internet Server.
.com the server provides commercial services to clients who connect to it.

To help to speed up access, its IP address can be directly represented in form of numbers. 127.57.13.1 instead of the domain name, m*icrosoft.com.* In this case no name resolution needs to take place.

An Internet address is a unique 32-bit number that is typically expressed as four 8-bit octets, with each octet separated by a period. Each of the octets can take on any number from 0 through 255.

Hosts, Domains and Subdomains

Hosts are in general, individual machines at a particular location. Resources of a host machine is normally shared and can be utilized by any user on Internet. Hosts and local networks are grouped together into domains, which then are grouped together into one more larger domains. For an analogy a host computer is considered as an apartment building in a housing complex and your account is just an apartment in it.

Domain may be an apartment complex, a town or even a country. Sub-domains may correspond to organizations such as IGNOU. India comes under a large domain. "IN". Computers termed as name servers contain database of Internets host addresses. They translate word addresses or persons understandable into numeric equivalents. Let us see another example of Internet address:

http://www.ignou.ac.in

What does it all mean? Actually to the ISP server, very little. The server wants to see something quite different. It wants to see a 32-bit number as an Internet address. Something like this equivalent decimal grouping:

198.168.45.249

The Internet addresses, known as universal resources locators (URL), are translated from one form to the other using an address resolution protocol. The first address is in the form we are most used to and that user use to access an Internet site. In this example, the address is for a website, identified by the hypertext transfer protocol (http), which controls access to web pages. Following http is a delimiter sequence, ://, and identification for the world wide web (www).

The domain name, ignou.ac follows www and identifies the general site for the web.(dot) edu is one example of a domain top, which is a broad classification of web users. Other common domain tops are:

.com for commerce and businesses
.gov for government agencies
.mil for military sites
.org for all kinds of organizations.

Lastly, in this example is a country code, again preceded by a dot. Here we are using in for the India, which is the default country.

Addresses may be followed by subdomains separated by dots or slashes (/) as needed. These addresses are translated into a 32-bit (4 decimal numeric groups) address shown as for http:// www.ignou.ac.in we will further discuss this topic in the next section.

1.7.2 Address Space

Internet addresses are divided into five different types of classes. The classes were designated A through E. class A address space allows a small number of networks but a large number of machines, while class C allows for a large number of networks but a relatively small number of machines per network. The following figure lists five address classes used in classical network addresses.

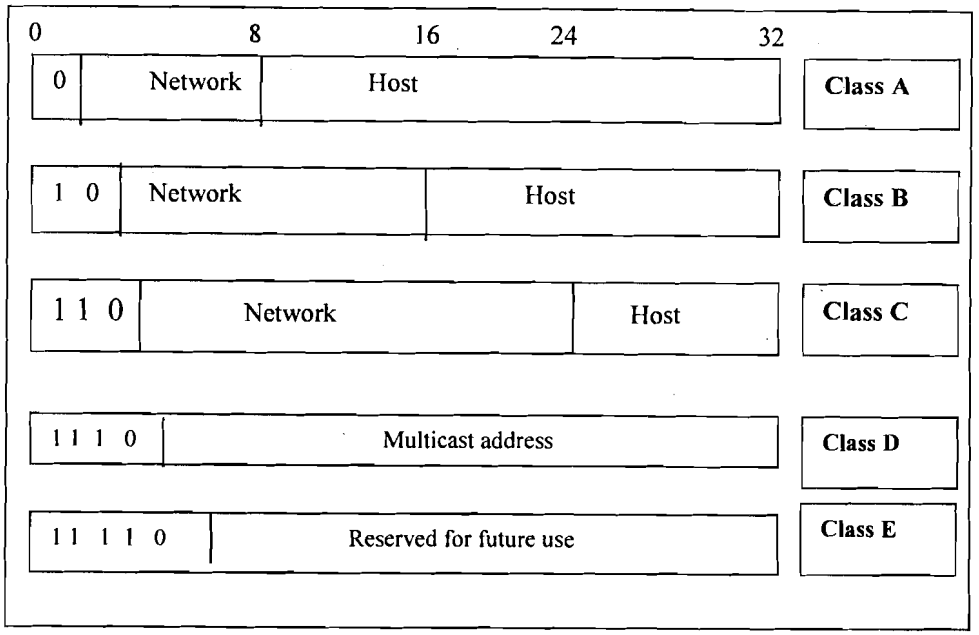

Figure 2: The IP Address Structure

Regardless of the class of address space assigned, organizations assigned a particular class of address will not utilize the entire address space provided. This is especially in the case of class A and Class B address allocation schemes.

Ports

A port is an additional 16-bit number that uniquely identifies the particular service on any given machine on the Internet. Port numbers are 16 bit wide, therefore each computer on the Internet has a maximum number of 2^{16} or 65,536 ports. The particular application is identified by its unique port number in the same way that a specific television station has a unique channel number.

Port numbers are divided into three ranges:

- Well-known ports are those from 0 through 1,023.
- Registered ports are those from 1,024 through 49,151.
- Dynamic and private ports are those from 49,152 through 65,535.

Well-known ports, those ranging from 0 through 1,023 are where most common services on the Internet are residing. These ports are controlled and assigned by the Internet Assigned Number Authority (IANA) and on most systems can be used only by system (root) processes or by programs executed by privileged users.

1.8 HOW DOES THE INTERNET WORK?

As discussed in the previous section every computer connected to the Internet has a unique address. Let's say your IP address is 1.2.3.4 and you want to send a message to the computer with the IP address 5.6.7.8. The message you want to send is "Hello computer 5.6.7.8!" Let's say you've dialed into your ISP from home and the message must be transmitted over the phone line. Therefore the message must be translated from alphabetic text into electronic signals, transmitted over the Internet, and then translated back into alphabetic text. How is this accomplished? Through the use of a **protocol stack**. Every computer needs one to communicate on the Internet and it is usually built into the computer's operating system (i.e. Windows, Unix, etc.). The protocol stack used on the Internet is refered to as the TCP/IP protocol stack, which was discussed in section 1.3.

If we were to follow the path that the message "Hello computer 5.6.7.8!" took from our computer to the computer with IP address 5.6.7.8, it would happen something like this:

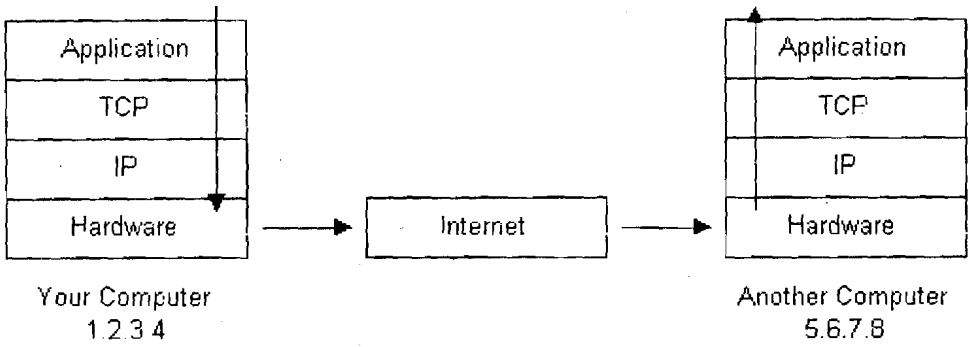

Figure 3: Environment of the Packet Flow

1. The message would start at the top of the protocol stack on your computer and work it's way downward.
2. If the message to be sent is long, each stack layer that the message passes through may break the message up into smaller chunks of data. This is because data sent over the Internet (and most computer networks) are sent in manageable chunks. On the Internet, these chunks of data are known as **packets**.
3. The packets would go through the Application Layer and continue to the TCP layer. Each packet is assigned a **port number**, which is used by program on the destination computer to receive the message because it will be listening on a specific port.
4. After going through the TCP layer, the packets proceed to the IP layer. This is where each packet receives it's destination address, 5.6.7.8.
5. Now that our message packets have a port number and an IP address, they are ready to be sent over the Internet. The hardware layer takes care of turning our packets containing the alphabetic text of our message into electronic signals and transmitting them over the phone line.
6. On the other end of the phone line your ISP has a direct connection to the Internet. The ISPs **router** examines the destination address in each packet and determines where to send it. Often, the packet's next stop is another router. More on routers and Internet infrastructure later.
7. Eventually, the packets reach computer 5.6.7.8. Here, the packets start at the bottom of the destination computer's TCP/IP stack and work upwards.
8. As the packets go upwards through the stack, all routing data that the sending computer's stack added (such as IP address and port number) is stripped from the packets.
9. When the data reaches the top of the stack, the packets have been re-assembled into their original form, "Hello computer 5.6.7.8!"

1.9 INTRANET AND EXTRANET

Intranets are basically "small" Internets. They use the same network facilities that the Internet does, but access is restricted to a limited sphere. For instance, a company can set up an intranet within the confines of the company itself. Access can be tightly controlled and limited to authorized employees and staff. There is no connection to the Internet or any other outside network. Functions like web sites, file uploads and downloads, and e-mail is available on intranets within the confines of the network. Since frivolous sites are no longer available, there is no employee time lost due to accessing them. There is, of course, the limitation of the networking area. The very benefit of restricting access to all of the facilities available on the Internet also restricts communication to other desirable locations. This is where the extranet steps in.

An extranet is network that connects a number of intranets into a truly mini-Internet Access is extended to all the intranets connected through the extranet, but, again, not to the Internet. Extranets requires a constant Internet connection and a hypertext transfer protocol (http) server.

Extranets can also be used to connect an intranet to the Internet so that remote offsite access can be made into a company's intranet by an authorized individual. This can facilitate through an extranet.

Basically, it uses passwords and smart cards to log in to a gateway server that checks the requester's security credentials. If the user checks out, he or she is allowed access into the company's intranet structure.

A number of URL address are set aside for intranet and extranet use. Essentially because intranets are self-contained networks, the same set of addresses can be used by all intranets without conflict. Extranet addresses are designed to recognize the intranets they connect and correctly preface each intranet address with an identifier. This allows two interconnected intranets to retain the same set of address values and keep them from being mistaken. One class A address, ranging from 10.0.0.0 to 10.255.255.255 is reserved for intranet usage. Again, since an intranet is a self-contained system, it only needs one class A network to designate the main network. Subnetworks use reserved class B and class C addresses. There are 16 class B addresses, from 172.16.0.0 ti 172.31.255.255 and 256 class C addresses, which range from 192.168.0.0 to 192.168.255.255.

1.10 INTERNET INFRASTRUCTURE

So now you know how packets travel from one computer to another over the Internet. But what's in-between? What actually makes up the Internet infrastructure or backbone?

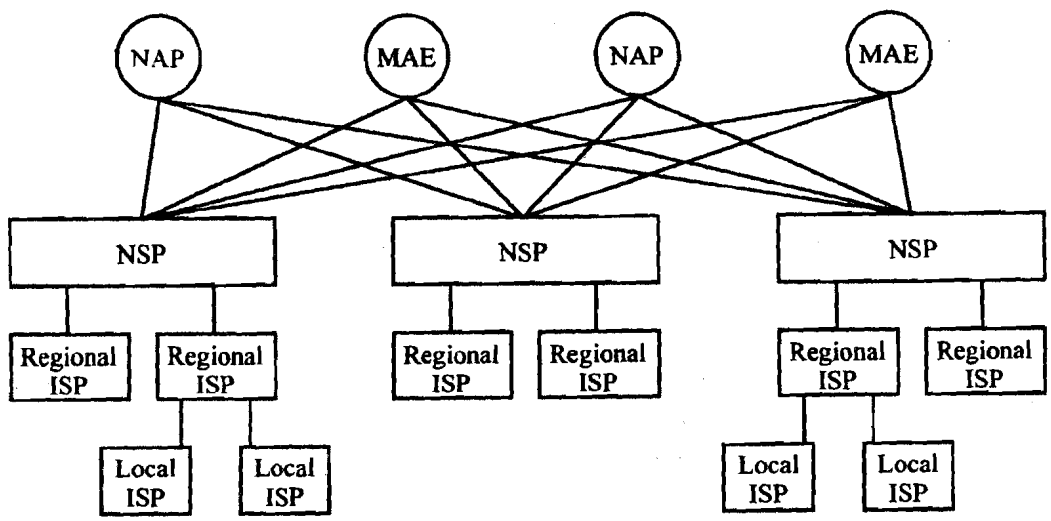

Figure 4: Internet Backbone

The Internet backbone is made up of many large networks, which interconnect with each other. These large networks are known as **Network Service Providers** or **NSPs**. These networks **peer** with each other to exchange packet traffic. Each NSP is required to connect to **Network Access Points** or **NAPs**. At the NAPs, packet traffic may jump from one NSP's backbone to another NSP's backbone. NSPs also interconnect at **Metropolitan Area Exchanges** or **MAEs**. MAEs serve the same purpose as the

NAPs but are privately owned. NAPs were the original Internet interconnects points. Both NAPs and MAEs are referred to as Internet Exchange Points or **IX**s. NSPs also sell bandwidth to smaller networks, such as ISPs and smaller bandwidth providers. Below is a picture showing this hierarchical infrastructure.

This is not a true representation of an actual piece of the Internet. The above figure is only meant to demonstrate how the NSPs could interconnect with each other and smaller ISPs. None of the physical network components are shown in this figure. This is because a single NSP's backbone infrastructure is a complex drawing by itself. Most NSPs publish maps of their network infrastructure on their web sites and can be found easily. To draw an actual map of the Internet would be nearly impossible due to it's size, complexity, and ever changing structure.

The Internet Routing Hierarchy

So how do packets find their way across the Internet? Does every computer connected to the Internet know where the other computers are? Do packets simply get 'broadcast' to every computer on the Internet? The answer to both the preceeding questions is 'no'. No computer knows where any of the other computers are, and packets do not get sent to every computer. The information used to get packets to their destinations is contained in routing tables kept by each router connected to the Internet.

Routers are packet switches. A router is usually connected between networks to route packets between them. Each router knows about it's sub-networks and which IP addresses they use. The router usually doesn't know what IP addresses are 'above' it. Examine the figure below. The black boxes connecting the backbones are routers. The larger NSP backbones at the top are connected at a NAP. Under them are several sub-networks, and under them, more sub-networks. At the bottom are two local area networks with computers attached.

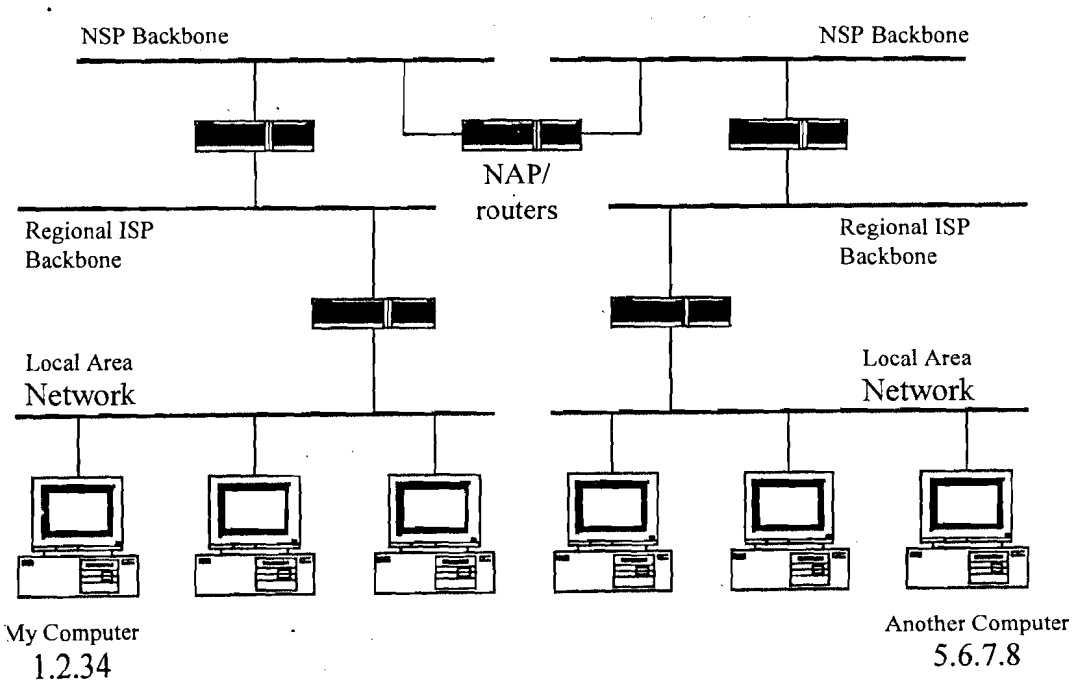

Figure 5: Routes Connecting in Network

When a packet arrives at a router, the router examines the IP address put there by the IP protocol layer on the originating computer. The router checks it's routing table. If the network containing the IP address is found, the packet is sent to that network. If the network containing the IP address is not found, then the router sends the packet on a default route, usually up the backbone hierarchy to the next router. Hopefully the

next router will know where to send the packet. If it does not, again the packet is routed upwards until it reaches a NSP backbone. The routers connected to the NSP backbones hold the largest routing tables and here the packet will be routed to the correct backbone, where it will begin its journey 'downward' through smaller and smaller networks until it finds it's destination.

Domain Names and Address Resolution

But what if you don't know the IP address of the computer you want to connect to? What if you need to access a web server referred to as *www.anothercomputer.com*? How does your web browser know where on the Internet this computer lives? The answer to all these questions is the **Domain Name Service** or **DNS**. The DNS is a distributed database, which keeps track of computer's names and their corresponding IP addresses on the Internet.

Many computers connected to the Internet host part of the DNS database and the software that allows others to access it. These computers are known as DNS servers. No DNS server contains the entire database; they only contain a subset of it. If a DNS server does not contain the domain name requested by another computer, the DNS server re-directs the requesting computer to another DNS server.

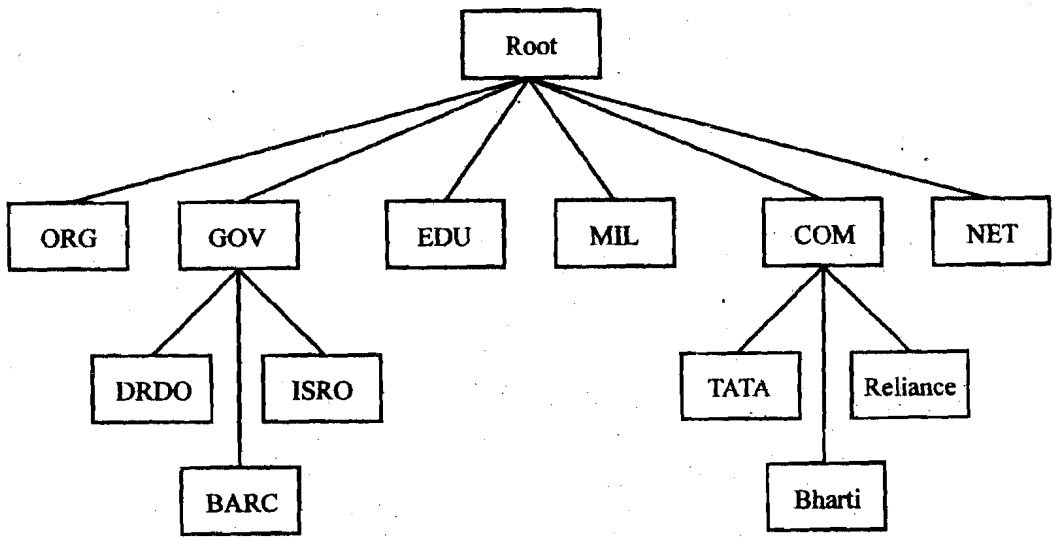

Figure 6: DNS Hierarchy

The Domain Name Service is structured as a hierarchy similar to the IP routing hierarchy. The computer requesting a name resolution will be re-directed 'up' the hierarchy until a DNS server is found that can resolve the domain name in the request. Figure 6 illustrates a portion of the hierarchy. At the top of the tree are the domain roots. Some of the older, more common domains are seen near the top. What is not shown are the multitude of DNS servers around the world which form the rest of the hierarchy.

When an Internet connection is setup (e.g. for a LAN or Dial-Up Networking in Windows), one primary and one or more secondary DNS servers are usually specified as part of the installation. This way, any Internet applications that need domain name resolution will be able to function correctly. For example, when you enter a web address into your web browser, the browser first connects to your primary DNS server. After obtaining the IP address for the domain name you entered, the browser then connects to the target computer and requests the web page you wanted.

1.11 PROTOCOLS AND SERVICES ON INTERNET

To work with Internet and to utilize its facilities we use certain tools. For example, Telnet is a tool, which is utilized for logging on remote computers on the Internet. Let us briefly discuss about some of the important tools and services.

1.11.1 Domain Name System

Domain name is a name given to a network for ease of reference. Domain refers to a group of computers that are known by a single common name. Somebody has to transfer these domain names into IP addresses. It is decided on the physical location of the web server as well as where the domain name is registered. Some generic domain names are:

Domain name	Description
Com	Commercial organization
Edu	Educational organization
Gov	Government organization
Mil	Military group
Org	Non-profit organization

Thus, humans use domain names when referring to computers on the Internet, whereas computers work only with IP addresses, which are numeric. DNS was developed as a distributed database. The database contains the mappings between the domain names and IP addresses scattered across different computers. This DNS was consulted whenever any message is to be sent to any computer on the Internet. DNS is based on the creation of the hierarchical domain based naming architecture, which is implemented as a distributed database. It is used for mapping host names and email addresses to IP addresses. Each organization operates a domain name server that contains the list of all computers in that organization along with their IP addresses. When an application program needs to translate a computer's name into the computer's IP address, the application becomes a client of the DNS. It contacts a domain name server and sends the server an alphabetic computer name then the server returns the correct IP address. The domain name system works like a directory. A given server does not store the names and addresses of all possible computers in the Internet. Each server stores the name of the computers at only one company or enterprise.

1.11.2 SMTP and Electronic Mail

One of the very useful things about Internet is that it allows you almost instantly exchange of electronic message (e-mail) across the worlds. E-mail is a popular way of communication on the electronic frontier. You can E-mail to your friend or a researcher or anybody for getting a copy of a selected paper. Electronic mail system provides services that allowed complex communication and interaction. E-mail provide the following facilities:

- Composing and sending/receiving a message.
- Storing/forwarding/deleting/replying to a message.
- Sending a single message to more than one person.
- Sending text, voice, graphics and video.
- Sending a message that interacts with other computer programs.

Another commonly used Internet service is electronic mail. E-mail uses an application level protocol called **Simple Mail Transfer Protocol** or **SMTP**. SMTP is also a text-based protocol, but unlike HTTP, SMTP is connection oriented. SMTP is also more complicated than HTTP.

When you open your mail client to read your e-mail, this is what typically happens:

1. The mail client (Netscape Mail, Lotus Notes, Microsoft Outlook, etc.) opens a connection to it's default mail server. The mail server's IP address or domain name is typically setup when the mail client is installed.
2. The mail server will always transmit the first message to identify itself.
3. The client will send an SMTP HELO command to which the server will respond with a 250 OK message.
4. Depending on whether the client is checking mail, sending mail, etc. the appropriate SMTP commands will be sent to the server, which will respond accordingly.
5. This request/response transaction will continue until the client sends an SMTP QUIT command. The server will then say goodbye and the connection will be closed.

Similarly, when you send an e-mail message your computer sends it to an SMTP server. The server forwards it to the recipients mail server depending on the email address. The received message is stored at the destination mail server until the addressee retrieves it. To receive E-mail a user Internet account includes an electronic mailbox. A message sent for you is received at your Internet host computer, where it is stored in your electronic mailbox. As soon as you login into your Internet account, one of the first things you should do is to check your mailbox.

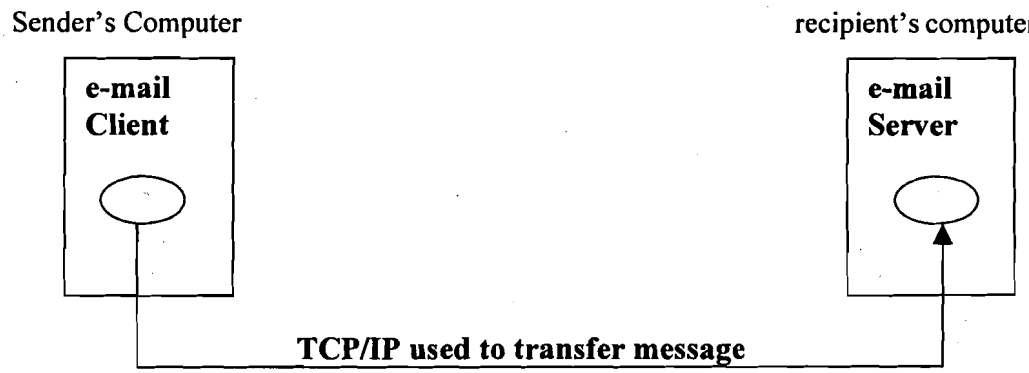

Figure 7: An e-mail transfer across the Internet uses two programs: client and server

E-mail system follows the client-server approach to transfer messages across the Internet. When a user sends an E-mail message a program on the sender's computer becomes a client. It contacts an e-mail server program on the recipient's computer and transfers a copy of the message. Some of the mail programs those exist on Internet are UCB mail, Elm, Pine etc. However, one thing, which you must emphasize while selecting a mail program, is the user friendliness of that program. Through E-mail on Internet you can be in direct touch of your friend and colleagues.

Mailing lists on Internet

Another exciting aspect about the E-mail is that you can find groups of people who share your interests-whether you are inclined toward research, games or astronomy. E-mail provides a mechanism for groups of people who have shared interests to establish and maintain contact. Such interest groups are referred to as *mailing lists* (lists for short). After all they are mailing lists of the members e-mail addresses. You can subscribe to any of such lists. You will receive copies of all the mail sent to the list. You can also send mail to al subscribers of the list.

1.11.3 Http and World Wide Web

One of the most commonly used services on the Internet is the World Wide Web (WWW). The application protocol that makes the web work is **Hypertext Transfer**

Protocol or **HTTP**. Do not confuse this with the Hypertext Markup Language (HTML). HTML is the language used to write web pages. HTTP is the protocol that web browsers and web servers use to communicate with each other over the Internet. It is an application level protocol because it sits on top of the TCP layer in the protocol stack and is used by specific applications to talk to one another. In this case the applications are web browsers and web servers.

HTTP is a connectionless text based protocol. Clients (web browsers) send requests to web servers for web elements such as web pages and images. After the request is serviced by a server, the connection between client and server across the Internet is disconnected. A new connection must be made for each request. Most protocols are connection oriented. This means that the two computers communicating with each other keep the connection open over the Internet. HTTP does not however. Before an HTTP request can be made by a client, a new connection must be made to the server.

When you type a URL into a web browser, this is what happens:

1. If the URL contains a domain name, the browser first connects to a domain name server and retrieves the corresponding IP address for the web server.
2. The web browser connects to the web server and sends an HTTP request (via the protocol stack) for the desired web page.
3. The web server receives the request and checks for the desired page. If the page exists, the web server sends it. If the server cannot find the requested page, it will send an HTTP 404 error message. (404 means 'Page Not Found' as anyone who has surfed the web probably knows.)
4. The web browser receives the page back and the connection is closed.
5. The browser then parses through the page and looks for other page elements it needs to complete the web page. These usually include images, applets, etc.
6. For each element needed, the browser makes additional connections and HTTP requests to the server for each element.
7. When the browser has finished loading all images, applets, etc. the page will be completely loaded in the browser window.

Most Internet protocols are specified by Internet documents known as a **Request For Comments** or **RFCs**. RFCs may be found at several locations on the Internet.

WWW is an Internet navigation tool that helps you to find and retrieve information links to other WWW pages. The WWW is a distributed hypermedia environment consisting of documents from around the world. The documents are linked using a system known as hypertext, where elements of one document may be linked to specific elements of another document. The documents may be located on any computer connected to the Internet. The word "document" is not limited to text but may include video, graphics, databases and a host of other tools.

The World Wide Web is described as a "wide area hypermedia information initiative among to give universal access to large universe of documents". World Wide Web provides users on computer networks with a consistent means to access a variety of media in a simplified fashion. A popular software program to search the Web is called **Mosaic,** the Web project has modified the way people view and create information. It has created the first global hypermedia network.

Once again the WWW provides an integrated view of the Internet using clients and servers. As discussed earlier, clients are programs that help you seek out information while servers are the programs that find information to the clients. WWW servers are placed all around the Internet.

The operations of the Web mainly rely on **hypertext** as its means of interacting with users. But what is hypertext? Hypertext as such is the same as regular text that is it

can be written, read, searched or edited; however, hypertext contains connections within the text to other documents. The hypertext links are called **hyperlinks.** These hyperlinks can create a complex virtual web of connections.

Hypermedia is an advanced version of hypertext documents as it contains links not only to other pieces of text but also to other forms of media such as sounds, images and movies. Hypermedia combines hypertext and multimedia.

1.11.4 Usenet and Newsgroups

In Internet there exists another way to meet people and share information. One such way is through Usenet *newsgroups*. These are special groups set up by people who want to share common interests ranging from current topics to cultural heritages. These are currently thousands of Usenet newsgroups.

The Usenet can be considered as another global network of computers and people, which is interwined with the Internet. However, Usenet does not operate interactively like the Internet, instead Usenet machines store the messages sent by users. Unlike mail from mailing lists, the news articles do not automatically fill your electronic mailbox. For accessing the information on newsnet, one needs a special type of program called a newsreader. This program help in retrieving only the news you want from Usenet storage site and display it on your terminal. Usenet is like living thing, New newsgroups gets added, the groups which have too much traffic get broken up into smaller specialized groups, the groups even can dissolve themselves. However, all of this occurs based on some commonly accepted rules and by voting. For Usenet, there is no enforcement body; it entirely depends on the cooperation of its computers owners and users.

The newsgroups are really meant fro interaction of people who share your interests. You can post your own questions as well as your answers to the questions of others, on the Usenet. One thing, which is worth mentioning here, is that when one is interacting wit people on Internet certain mannerism should be adopted. These rules are sometimes called "netiquette". In a face-to-face conversation you can always see a person's facial gestures and hand movements and can ascertain whether he is teasing or is being sarcastic or sometimes even lying. However, in on-line interaction one cannot see the person one is interacting with. The rules of netiquette may help to compensate some of these limitations of this on-line environment.

1.11.5 FTP

FTP (File Transfer Protocol), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (Hypertext Transfer Protocol), which transfers displayable Web pages and related files, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to downloading programs and other files to the computer from other servers. However, for such transfer you need an account name on a host and the password. The FTP program will make connection with the remote host, which will help you to browse its directories and mark files for transfer. However, you cannot look at the contents of a file while you are connected via FTP. You have to transfer the copy and then look at it once it is on your own account.

FTP includes many commands but only few are used to retrieve a file. A user needs to understand the three basic commands to connect to remote computer, retrieve a copy of file and exit the FTP program. The commands with their meanings are:

Command	Purpose
Open	connect to a remote computer
get	retrieve a file from the computer
bye	terminate the connection and leave the FTP program

Transferring a file via FTP requires two participants: an FTP client program and FTP server program. The FTP client is the program that we run on our computers. The FTP server is the program that runs on the huge mainframe somewhere and stores tens thousands of files. It is similar to an online library of files. The FTP client can download (receive) or upload (send) files to the FTP server. Using Web browser you can download the files but you can not upload the files. FTP applications will help you to upload the files to the web sites, which you are maintaining.

FTP only understands two basic file formats. It classifies each file either as a text file or a binary file. A text file contains a sequence of characters collected into lines. Although computers used ASCII encoding for text files, FTP includes commands to translate between ASCII and other character encoding. FTP uses the classification binary file for all nontext files. The user must specify binary for any file that contains:

- A computer program
- Audio data
- A graphic or video image
- A spreadsheet
- A document from a word processor
- A compressed file

FTP service compress files to reduce the total amount of disk space the files require. Before transferring a file user must tell FTP that the file contains ASCII text or nontext file. FTP assumes to perform ASCII transfers unless the user enters the binary command.

There are many FTP programs that you can download from the Internet. Windows has its own command line based FTP program. To execute it, select Run from Windows taskbar and type FTP and press enter. By typing open command you can.connect to any ftp server. To connect to FTP server you must have a login name and the password. Most of the FTP servers allow anonymous connections. In this case username is anonymous and password is your e-mail address.

Another important FTP program, which is available as a shareware, is WSFTP. Using this window based program it is easier to maintain your web site.

1.11.6 Telnet

TELNET stands for TErminal NETwork. Telnet is both a TCP/IP application and a protocol for connecting a local computer to a remote computer. Telnet is a program that allows an Internet host computer to become a terminal of another host on the Internet. Telnet is the Internet remote login service. Telnet protocol specifies exactly how a remote login interacts. The standard specifies how to client contacts the server and how the server encodes output for transmission to the client. To use the Telnet service, one must invoke the local application program and specify a remote machine. The local program becomes a client, which forms a connection to a server on the remote computer. The client passes keystrokes and mouse movements to the remote machine and displays output from the remote machine on the user's display screen. Telnet provides direct access to various services on Internet. Some of these services are available on your host, but Telnet is especially useful when these services are not available on your host. For example, if you want to use graphical interfaces designed by other users then Telnet, allows you to access their hosts and use their new interfaces. Similarly, whenever someone creates a useful service on his host, Telnet

allows you to access this valuable information resource. This tools Is especially useful for accessing public services such as library card catalogues, the kind of databases available on the machine etc. You can also log into any catalogue service of a library and use it.

The working of TELNET

1. The commands and characters are sent to the operating system on the common server computer.
2. 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 an agreed format known as Network Virtual Terminal (NVT) characters and sends them to the TCP/IP protocol stack of the server computer. NVT is the common device between the client and server.
4. The commands and text are first broken into TCP and 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 software collects all the IP packets, verifies their correctness and reconstructs the original command and handover the commands or text to that computer operating system.
6. The operating system of the server computer hands over these commands or text to the TELNET server program, which is executing on that remote computer.
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. The TELNET cannot directly handover the commands or text to the operating system so TELNET hands over the commands/text to the Psuedo-terminal driver.
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 application program on the remote server.

The working of the TELNET is extremely simple. Suppose you are working as a faculty member of Indira Gandhi National Open University. You have a typical account FACULTY-1 on the IGNOU computer, which is one of the hosts of the Internet. You are selected for academic exchange scholarship to USA. You will get a user account in U.S.A. However, all your colleagues know only your IGNOU account. Thus, using Telnet you can always log on to your account in India for mail your papers for using programs etc.

There are many databases available on the Internet. You can explore these databases using Telnet. There are going to be many Internet services yet to be created. Every year and better means of accessing the treasures of the Internet is appearing in which Telnet is the key for accessing.

Check Your Progress 2

1. State whether True or False:

   a) E-mail can be used to send text, pictures and movies.
   b) Usenet facility is same as that of mailing list facility.
   c) Anonymous FTP allows viewing and retrieving a file from the archieve of a host without having an account on that machine.
   d) Telnet is used for remote login.
   e) An Internet address is a 16-bit number.
   f) Each computer on the Internet has a maximum number of 2^{16} or 65,536 ports.

2. What is an Internet address?
3. What is FTP?
4. What is Telnet?

1.12 INTERNET TOOLS

In this section we shall look at two software tools available on the Internet.

1.12.1 Search Engines

Search Engines are programs that search the web. Web is a big graph with the pages being the nodes and hyperlinks being the arcs. Search engines collect all the hyperlinks on each page they read, remove all the ones that have already been processed and save the rest. The Web is then searched breadth-first, i.e. each link on page is followed and all the hyperlinks on all the pages pointed to are collected but they are not traced in the order obtained. Automated search is the service that is provided by Search engines. An automated search service allows an individual to find information that resides on remote computers. Automated search systems use computer programs to find web pages that contain information related to a given topic. It allows to locate:

- Web pages associated with a particular company or individual
- Web pages that contain information about a particular product.
- Web pages that contain information about a particular topic.

The results of an automated search can be used immediately or stored in a file on disk to use it later. The results of a search are returned in the form of a web page that has a link to each of the items that was found. Automated search is helpful when a user wants to explore a new topic. The automated search produces a list of candidate pages that may contain information. The user reviews each page in the list to see whether the contents are related to topic or not. If so, the user records the location or if not user moves on to the page in the list. Search mechanisms uses a similar method of search as in the telephone book i.e. before any user invoke the search mechanism a computer program contacts computers on the Internet, gathers a list of available information, sorts the list and then stores the result on a local disk on the computer that runs a search server. When a user invokes a search, the user client program that contacts the server. The client sends a request that contains the name the user entered. When the request arrives at the server, it consults the list of file names on its local disk and provides the result.

1.12.2 Web Browser

A Web browser is software program that allows you to easily display Web pages and navigate the Web. The first graphical browser, Mosaic, was developed in Illinois at the National Center for Supercomputing Applications (NCSA). Each browser displays Web-formatted documents a little differently. As with all commercial software, every program has its own special features.

The two basic categories of Web browser are:

- **Text-only browsers**: A text-only browser such as Lynx allows you to view Web pages without showing art or page structure. Essentially, you look at ASCII text on a screen. The advantage of a text-only browser is that it displays Web pages very fast. There's no waiting for multimedia downloads.

- **Graphical browsers**: To enjoy the multimedia aspect of the Web, you must use a graphical browser such as Netscape Navigator or NCSA Mosaic. Graphical browsers can show pictures, play sounds, and even run video clips. The drawback is that multimedia files, particularly graphics, often take a long time to download. Graphical browsers tend to be significantly slower than their text-only counterparts. And this waiting time can be stretched even further with slow connections or heavy online traffic.

Many different browsers are available for exploring the Internet. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text.

Check Your Progress 3

1. State whether True or False

   a) Surfing means that you are sending for specific information on Internet.
   b) HTML is used for creating home page for World Wide Web.
   c) Hypermedia is same as Hypertext.
   d) Netscape these days is one of the widely used browser.
   e) Windows 95 provides software for browsing Internet.
   f) Hypertext documents contain links to other documents.

1.13 SUMMARY

This unit describes the basic concepts about an Internet. Internet is a network of networks where lot 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. The unit describes the various tools available on the Internet and the various services provided by the Internet to users. In this unit we have talked about the Electronic mail Usenet and newsgroups, FTP, Telnet and search engines. We also describe the use of frequently asked questions. The unit also describes the importance of Internet addresses. Addresses are essential for virtually everything we do on the Internet. There are many services available on the Internet for document retrieval. For browsing the Internet there are many browsers available such as Gopher and World Wide Web. Both of these browsers are easy to use and most popular browsing mechanisms on the Internet.

1.14 SOLUTIONS/ ANSWERS

Check Your Progress 1

1. True or false

   a) False
   b) False
   c) True
   d) True
   e) False

2. The TCP/IP networking model has five layers, which are:

   - The Physical Layer
   - The Data link Layer
   - The Network Layer
   - The Transport Layer
   - The Application layer

3. Transmission Control protocol provide various facilities which include:

   - TCP eliminates duplicate data.

- TCP ensures that the data is reassembled in exactly the order it was sent
- TCP resends data when a datagram is lost.
- TCP uses acknowledgements and timeouts to handle problem of loss.

Check Your Progress 2

1. True or false

   a) True
   b) True
   c) True
   d) True
   e) False
   f) True

2. Addresses are essential for virtually everything we do on the Internet. The IP in TCP/IP is a mechanism for providing addresses for computers on the Internet. Internet addresses have two forms:

   - Person understandable which expressed as words
   - Machine understandable which reexpressed as numbers

   Internet addresses are divided into five different types of classes. The classes were designated A through E. class A address space allows a small number of networks but a large number of machines, while class C allows for a large number of networks but a relatively small number of machines per network.

3. FTP (File Transfer Protocol), a standard Internet protocol. It is the simplest way to exchange files between computers on the Internet. FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files. Transferring a file via FTP requires two participants: an FTP client program and FTP server program. The FTP client is the program that we run on our computers. The FTP server is the program that runs on the huge mainframe somewhere and stores tens thousands of files.

4. Telnet is both a TCP/IP application and a protocol for connecting a local computer to a remote computer. Telnet is the Internet remote login service. Telnet protocol specifies exactly how a remote login interacts. The standard specifies how to client contacts the server and how the server encodes output for transmission to the client. To use the Telnet service, one must invoke the local application program and specify a remote machine.

Check Your Progress 3

1. True or false

   a) False
   b) True
   c) False
   d) False
   e) True
   f) True