UNIT 5 INTERNET BASICS

Structure

5.0 LEARNING OUTCOMES

In Unit 5 of this Block, an attempt has been made to explain to you the basics of Internet.

After reading this Unit, you will be able to:

- discuss that what is a computer network and why to network computers;
- differentiate between networks like LAN and WAN;
- identify the functionalities of clients and servers;
- know a brief history of the international initiative called Internet though it originated from various small and varied technology solutions;
- describe the working of Internet;
- discuss how to set up an Internet connection;
- identify the virtues of Post Office Protocol and VoIP;
- highlight the various options for keeping Internet more secure; and
- learn how to better search Internet/web resources.

5.1 INTRODUCTION

This unit introduces you to computer networking, the origins of the Internet, common concepts, terms and technologies of the Internet, basic tools of the Internet such as Email, World Wide Web, web browser and search engines. In addition, it explains what is Internet, how Internet works as a global network and how to set up Internet connection. This Unit also explains the Internet protocols - Post Office Protocol (POP), Voice over Internet Protocol (VoIP) – and their role in exchanging messages on email or making calls directly from a computer linked to broadband Internet connection. The Unit also provides guidelines for effective web searching.

5.2 COMPUTER NETWORK

A **network** is a group of two or more computers linked together for sharing of computing and data resources. The computer that you have in your home, office or in a cyber café, if not connected to any network, is an idle piece of machine; such a machine has limited functionality. It can only be used to run software applications or access data/ resources that reside or created inside the computer. When you connect your computer to a network, it becomes a network part. A networked computer can perform much more functions than what a computer can do as a standalone unit. You can download software, share data and communicate with computers linked to the network. However, when you connect your computer to a global network like the Internet, you can hope to do still more, like accessing and sharing data/ resources globally, not locally.

5.2.1 LAN and WAN

Computer networks such as LAN (Local Area Network) and WAN (Wide Area Network) vary in the geographical area they cover to connect computers. A LAN is a small computer network localised to a single or a group of neighbouring buildings. In most cases, ownership of the LAN is local, owned by the same organisation which houses the network. LAN can be used to share files, resources and if desired, an Internet connection also. In a LAN, there is a main computer called *server* and remote computers called *clients*. A typical LAN uses ATM (asynchronous transfer mode) networking and fibre cables for high speed connectivity and high data carrying capacity. Unlike a LAN, a WAN covers a larger geographic area. Most WANs are made up from several interconnected LANs.

LAN network can also be used to share a single Internet connection with all computers connected to local network. To connect LAN to Internet, LAN computers must communicate on TCP/IP protocol.

5.2.2 INTERNET

Internet is a global network of several interconnected TCP/IP networks. It is the largest computer network in the world connecting millions of computers. It is publically accessible to all. Every networked computer is a part of it (Internet). It is like a road in front of your house leading to the nearest town, then to the national highway and through highways to several other places and cities in the country. Like the highways, electrical lines, water supply lines or railway network, Internet connects countries and regions of the earth to one another through networked computers and communication lines.

5.3 CLIENTS AND SERVERS

Computers on the Internet are interconnected through client/server computing

technology. A client is a software programme in a computer (Desktop PC) that sends requests to a remote server (host computer that offers resources) on a network. The server computer in response sends information back to the client computer. On the Internet, web browsers are clients that connect to remote web servers; web browsers retrieve web pages from web servers for display. The same client/server model is also at work in the case of other Internet tools like e-mail, FTP and chat.

5.4 HISTORY OF INTERNET

The term "Internet" was first used in the Requests for Comments (RFC) document published on the TCP protocol (RFC 675: Internet Transmission Control Program, December 1974) as an abbreviation of the term Internetworking. It is used to denote a global network using TCP/IP. Internet is an outcome of consistent research in the field of computer and communication technology over the last five decades or more. The application of packet switching led to a protocol for internetworking. By using packet switching protocol multiple networks could be linked together for sharing computing data and resources. Being active in cutting edge military research, the United States Department of Defense's Advanced Research Projects Agency (DARPA) felt the need of networking institutions under the Agency with all other educational institutions where research work was underway for specific goals. To achieve this goal, the Agency (DARPA) established ARPANET in 1969. Similarly in the UK, the SERCnet (which later became JANET) was set up in 1974 providing network connectivity between British academic and research sites using packet switching technology. In between various technologies that were under-development had helped in enabling several other networks to exchange messages and share resources. With so many different network methods at hand, something was needed to unify networks by obliterating the differences between network protocols. Eventually, TCP/IP became a common inter-network protocol and was widely adopted in 1983. As a result, instead of individual networks becoming responsible for reliability, the hosts were made responsible for reliable network communication. The efforts of National Science Foundation (NSF) led to the creation of NSFNet backbone. Established in 1986, NSFNet was used exclusively to connect and provide access to a number of supercomputing centres established by the NSF. Internet in its initial periods was planned to cater to the needs of academic and research community and of the government institutions only. Though commercial use of Internet was forbidden, slowly and steadily commercial institutions became part of the network. They gradually started taking advantage of the Internet, even though it was still not clear during those initial periods of Internet as to what constituted commercial use of Internet and which one was a commercial institution. No doubt that the commercial interests in the Internet had made it what it is today. We still continue to see rapid strides in the commercial uses of the Internet such as in teleshopping, e-booking of railway and airline tickets.

A perfect story of Internet is difficult to write because it is the fruit of collective wisdom and collaborative efforts of so many persons from so many different countries and regions of the globe. Compared to developing countries, developed countries took better leverage of Internet technologies. It is quite common to see such countries in the limelight whenever we write Internet history. Largely a US effort in which many other countries also played important role in creating what eventually became the Internet. It is perhaps one of those international programmes which achieved complete success without any diplomacy; rather it became a reality mainly through the fruits of technology, collaboration and commerce.

5.5 HOW DOES INTERNET WORK?

The *Internet* lets you transfer information around the world in seconds. To understand how *all that data reaches* its destination, we need to know first about basics of Internet infrastructure, tools, protocols and technologies that interconnect various Internet devices.

Internet – Internet means a network of several interconnected networks. There is no single thing called The Internet. The Internet provides several different basic tools for data sharing. These are: Email, Chat, Instant Messaging (IM), File Transfer Protocol (FTP), Voice over Internet Protocol (VoIP), World Wide Web, Blog, Social Media and Telnet (remote login).

Internet Infrastructure – The Internet has an infrastructure at the backend though not visible to naked eyes. It is made up of many different elements such as hubs NAPs (Network Access Points), backbones and thousands of ISPs (Internet Service Providers. These networks connect together in many different ways. The backbones, known as the high level networks, connect together through network access points (NAPs). Several corporate entities who own the backbones have agreed to intercommunicate with each other at the NAPs.

Internet Topology - The topology of the Internet is loosely hierarchical. From bottom-to-top the hierarchy consists of end systems (PCs, workstations, etc.) connected to local Point of Presence (PoP) of the Internet Service Providers (ISPs). The local ISPs are in turn connected to regional ISPs, which in turn to the backbone through NAPs. The backbones at national and international level are interconnected together at NAPs.

At present several non-profit bodies oversee the technical pieces of the Internet infrastructure, Internet's technical specifications, regulate different aspects of it, or that seek to improve its stability and functionality, but no single agency or network has control over the Internet.

What is Internet Backbone? Backbones are fibre optic trunk lines with multiple fibre optic cables combined together to increase the capacity. Fibre optic cables are designated as OC for optical carrier, such as OC-3, OC-12 or OC-48. An OC-3 line is capable of transmitting 155 Mbps while an OC-48 can transmit 2,488 Mbps (2.488 Gbps).

Internet uses client/server model for running its basic tools such as Telnet, FTP, Gopher, E-mail and World Wide Web and others. In the client/server model, all computers on the Internet are either clients or servers. The computers that provide services to so many clients are *servers*; for example, Web servers, e-mail servers, FTP servers and so on. The computers that seek services from servers are *clients*. One server generally supports numerous clients; and multiple servers networked together in a pool handle the increased processing load as clients grow in number.

ISP (Internet service provider) is an organisation that provides connectivity/access to the Internet. Just as local customers pay to ISPs for Internet access, few ISPs themselves pay tier 1 ISPs for Internet access. Tier 1 ISP usually has a larger network than the contracting ISP. Contracting ISPs lease Internet connections from tier 1 or tier 2 ISPs. The role of an ISP is to take a local customer from the Point of Presence of the ISP to a network access point (NAP), which is a kind of "ramp" onto the backbone. **Point of presence** (PoP) is the proximity of physical location of the ISP to the backbone of the Internet.

What is TCP/IP? - Communication between computers and networks on the Internet

takes place in TCP/IP protocol, a set of technical standards that govern the transmission of data over the network. IP means Internet Address. Because Internet is a network of global computers, every computer must have an address called IP address. TCP means Transmission Control Protocol. It ensure that packets reach the pre-defined destination point and in correct order.

What is IP address? The IP number is called an "address" because it serves the same purpose as a home address; it is used to identify each device on the Internet and its location to help direct Internet traffic. IP address is a unique number given to identify a host computer on the Internet. It is a number string used for identification of computer on the network. A typical IP address looks like 144.16.192.17 (the same address in binary form in which the computers communicate looks like 10010000.00010000.11000000.00010001). The four numbers in an IP address are called octets, because they each have eight positions when viewed in binary form. There are 32 positions in all and hence IP addresses are considered 32-bit numbers. Since each of the eight positions can have two different states (1 or zero), the total number of possible combinations per octet is 2 to the power 8 or 256 with each octet containing any value between zero and 255. For example, IP address of IGNOU host is 14.139.40.44; it is this number that is used on the Internet to search IGNOU host.

Routers are network devices that determine the path to send information from one computer to another or from one network to another network. They are nothing but specialised computers that send messages/information/data packets along thousands of pathways. A router ensures that information reaches its intended destination and nowhere else. The primary function of a router is to connect networks together and keep broadcast traffic under control, allowing information to pass from one network to the other and preventing traffic on one network from spilling over to the other.

What is DNS? When the number of Internet sites were few, it was not so difficult to remember IP addresses to connect to any host or seek its service. But the number of IP addresses has become large and unwieldy now mainly due to explosive growth of networked computers on the Internet. To tackle the problem, a simple text file was maintained by the Network Information Centre that mapped names to IP addresses. Soon this text file also became so large and cumbersome to manage. As a solution, the University of Wisconsin created the Domain Name System (DNS) in 1983, which maps text names to IP addresses of Web servers hosting those sites automatically. It is only due to DNS that we need only to remember www.ignou.ac.in to access IGNOU site on the web and not its corresponding IP address.

DNS is an acronym for *Domain Name System*. It is an Internet service that automatically converts the domain name/hostname to the IP address of the Web server which hosts the site. It is therefore possible to address a Web site on TCP/IP networks by name and not by IP address. The importance of DNS lies in the fact that it is easier to remember the name of a site than its IP address described in numerals. DNS is a distributed, hierarchical database of name and IP address data that is widely used on the Internet.

URL (Uniform resource locator) indicates the unique address of a file that can be plain Web pages, other text documents, graphics, or programs on the World Wide Web. This is used by Web browsers, e-mail clients and other software to identify a *network resource* on the Internet. URL has a specific format: protocol://*hostname/location of the resource*. For example, URL for the B.Lib.Sc. Programme, Faculty of Library and Information Science that appears on the IGNOU is reproduced as follows: http://www.ignou.ac.in/ignou/aboutignou/school/soss/programmes/detail/148/2. When this URL is broken into its three constituent parts each appears as follows: (i) protocol

(http://), (ii) host name (www.ignou.ac.in) and (iii)location (/ignou/aboutignou/school/soss/programmes/detail/148/2).

A Digital Object Identifier (DOI) is a permanent identifier given to a Web file or other Internet resource. It helps a user to find a lost Internet resource when its URL changes. Using DOI, the user is automatically redirected to its new URL. URL/IP address of a digital object may change with time, but not its DOI name. The use of DOI names as identifiers makes managing of intellectual property in a networked environment much easier and more convenient and allows the construction of automated services and transactions. Over 45 million DOI names have been assigned by DOI System registration agencies in the US, Australasia and Europe. The DOI system is managed by the International DOI Foundation, an open membership consortium including both commercial and non-commercial partners and has recently been accepted for standardisation within ISO.

Internet tools : To use Internet you need basic tools such as e-mail, telnet, FTP, World Wide Web; all of these tools comply with suite of TCP/IP protocols. All these tools are now available on the web platform. You will learn more about these tools in the next Unit.

How does information travel on the Internet? - The Internet runs on TCP/IP (Transmission Control Protocol/Internet Protocol) suite of protocols. When a user sends any file from one point to another on the Internet, TCP protocols divided the file into parts (packets). Each of these packets is separately numbered and includes the Internet address of the destination point. The different packets for a given file may travel on different routes through the Internet. When they arrive at their destination, they are reassembled into the original file. It all sounds very complex and time consuming, but TCP manages this process of dividing the file into packets and reassembling them into the original file occurs very, very quickly. Internet Protocol, handles the address part of each packet so that it gets to the right destination. Without such a common set of protocols, communication between Internet devices (clients and servers) cannot happen.

- Data is divided up into *packets*
- Data routes across the Internet can be *switched* to avoid congestion
- Entire mechanism is handled by the TCP/IP protocols

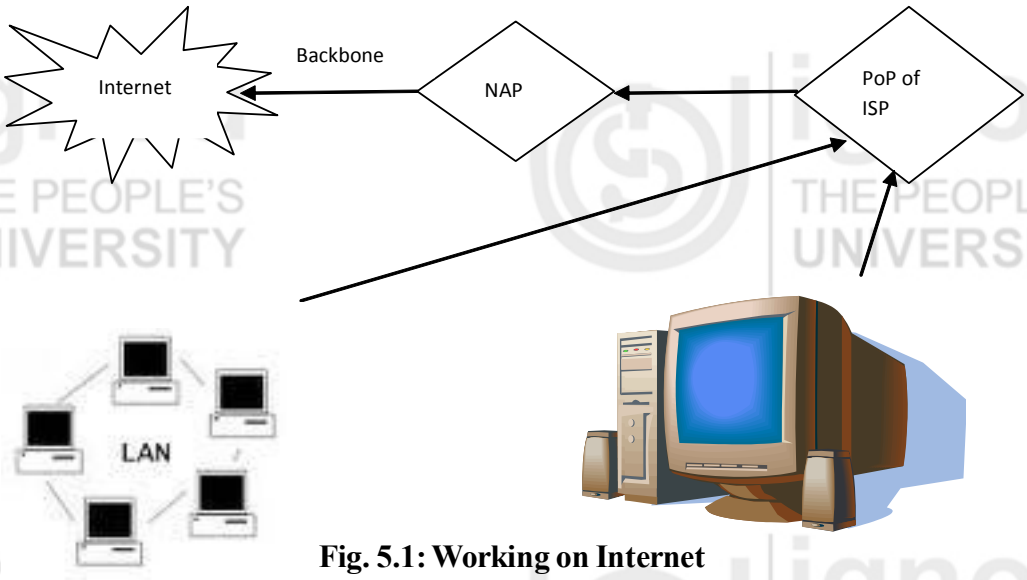

Fig. 5.1: Working on Internet

Source: http://wally.cs.iupui.edu/n241_06/files/web/index.htm

Self Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

1) Describe briefly how DNS makes it easy for us to access Internet.

.....

.....

.....

.....

2) What are protocols?

.....

.....

.....

.....

3) What is Internet and explain how is Internet different from LAN and WAN?

.....

.....

.....

.....

4) What is IP address, hostname, domain hierarchy?

.....

.....

.....

.....

5.6 SETTING UP INTERNET CONNECTION

How to connect a computer to Internet? To connect a local computer to Internet you need to buy/rent a connection from an Internet Service Provider (ISP). Currently, ISPs offer three options for Internet connections: Wi-Fi, broadband and dial-up Internet connections. Setting up the Internet connection with each of these options varies. In general, hardware resources that you need to setup an internet connection are: computer (desktop or laptop), Internet modem (broadband, or dial-up), computer manual and a telephone. You don't need telephone connection if you are using Wi-Fi. You connect to the Internet via wireless network access point.

Broadband Internet is a 'high access speed' service. The dial-up connection is a non-broadband internet service, cheaper but slower in access speeds. Most Internet users are moving towards the faster broadband Internet connection. Different speeds of Internet connections permit different quantum of download. Presently, a connection having download speeds of 256 kbps or more is classified as broadband.

You need to approach Internet service provider (ISP) to get Internet connection and for installation of setup. You can also do setup installation yourself with the help of the manual/brochure provided by the ISP. MTNL/BSNL offers 2 Mbps minimum download speed for its broadband connections in the country currently. Apart from MTNL/BSNL there are private ISPs such as mobile telephone providers like Airtel and Reliance.

Activity I: Identify how the Internet connection is setup in our home or office and prepare a manual of the same.

5.7 POST OFFICE PROTOCOL BASICS

How E-mail programme gets you email messages? POP (Post Office Protocol) is a protocol that is used to retrieve e-mail from a mail server, which is housed on the service provider's computer. Most e-mail applications, for example e-mail client, use POP protocol, although some can use the newer IMAP (Internet Message Access Protocol)

E-mail system delivers electronic mail messages to one or more recipients on the Internet. In TCP/IP protocols, communication is online, *i.e.* both the sender and the receiver must be on the network at the same time for exchanging communication. For electronic mail, this model of communication does not work. E-mail must use a "send and forget" model, just like the postal mail. This sort of decoupling of the sender and receiver is critical to the design of the e-mail system. Also critical to the entire e-mail system is the requirement that communication is accomplished between specific users, not between particular machines. This makes e-mail system inherently different from many other types of communication on TCP/IP networks. The most popular access method today is the simple offline access model, where a client device accesses a server, retrieves e-mail and deletes it from the server. The Post Office Protocol (POP) was designed for quick, simple and efficient mail access.

5.8 VOICE OVER INTERNET PROTOCOL (VOIP)

Voice over Internet Protocol (VoIP) as the name suggests converts your voice signals into digital signals so that converted voice signals could travel over the Internet. If you are calling from a regular phone number, the signal is reconverted to a regular telephone signal before it reaches the destination. VoIP allows you to make a call directly from a computer using broadband Internet connection, a special VoIP phone, or a traditional phone connected to a special adapter.

5.9 SECURITY OPTIONS

With the Internet gaining prominence globally and given its increasingly high usage including in critical operations, there exists the need to enforce a strong security in computer systems to check and prevent data theft and fraud. The instances of stealing all your personal information on the Internet without your knowledge are growing. Think of the situation if the same information reaches into the hands of some dubious persons who may misuse it for financial or other personal gains. Phishing is the act of luring gullible e-mail users to reveal their personal information such as usernames, passwords and credit card details with the purpose of misusing such details for committing frauds.

There is no one single solution for enforcing computer security nor is there any foolproof solution. We can only attempt to make systems more secure by preventing or blocking computer access to all those who are not authorised to use the same. Some of the

solutions that we can apply to prevent and block unauthorised access are listed below:

1) **Secure access**: The 'access authorisation/authentication control system' is commonly used to restrict unauthorised access to a computer system. The checks suggested to control access are: user password, identification card, smart card or biometric solution. Of all these solutions, password is the most commonly used access control mechanism. To make it foolproof password must be strong enough to prevent anyone guessing it right. Secondly, it should be changed quite often. Make it a regular practice to block access to your desktop while you are away.

2) **Install virus scanner**: Anti-virus software helps to identify, thwart and eliminate computer viruses (programmes to cause damage to a computer or network operation) and other malicious software (malware, spyware). It keeps users informed about virus reports and sends virus alerts.

3) **Protect against malware**: Install a malware detection programme. Malware is malicious, hostile, intrusive software which attackers use to disrupt computer operation, gather sensitive information, or gain access to private computer systems. These malware start working automatically and corrupt your computer and network. Malware can monitor a computer keyboard, recording such information as passwords or credit card numbers and then relay such identity data to thieves. Malware includes various types of software such as adware, spyware, viruses, trojans and more. The best way to protect your computer against such malware and malicious attacks is to avoid accessing such sites.

4) **Maintain backups**: Maintain backup copies of important files periodically in different storage media and at different locations.

5) **Use encryption**: Encryption techniques help in keeping data legible but only to those who are entitled to view the same.

6) **Employ firewalls**: Firewalls installed on computer systems and networks restrict network traffic according to configuration defined by the system administrator.

7) **Avoid cookies**: Disable cookies while accessing doubtful, dubious sites on the Internet.

8) A cookie is a small piece of data sent from a website and stored in a user's web browser automatically while a user is browsing a website. It is also known as an HTTP cookie, web cookie, or browser cookie. When the user browses the same website again in the future, the data stored in the cookie can be retrieved by the website to notify the website of the user's previous activity. Although cookies cannot carry viruses and cannot install malware on the host computer, tracking cookies and especially third-party tracking cookies are commonly used as ways to compile long-term records of individuals' browsing histories.

9) **Prevent phishing**: Some e-mails coming from unknown companies, masquerading as trustworthy entities, are in fact phishing e-mails. They are deliberately sent to lure you to reveal your bank account number, credit card number and so on only to misuse your personal data later and cheat you. Phishing e-mails may contain links to websites that are infected with malware. Avoid responding to such phishing mails. The other modes of electronic communication such as instant messaging, social media sites also pose phishing threats.

10) **Configure proxy server**: A proxy server acts as a middleman for Internet connections. It makes most computer systems on the network more secure. Proxy

server offers added advantages such as content filtering and performance enhancements (as caching helps accessing the same site again and again by reducing network load and enabling faster access).

11) **Ignore spam mails**: Do not encourage spams by responding to such mails. The best way is to install a spam filter in the mail programme. If that fails, delete such mails without opening is another option. Do not open mail and attachments of unknown senders. Spam mails are known as unsolicited bulk mails, junk mails, or commercial mails.

12) **Keep a watch on downloads**: Internet is a reflection of the world we live in. It provides access to both good content and bad content in similar proportions. Keep a watch on free downloads of music, video and software programmes, etc. This is important since some of them have the potential to deliver hidden malware with the dubious intensions to either corrupt your system or steal your personal information for ulterior motives.

13) **Virus wall measures by computer staff/Internet service provider**: Some users are unaware of any virus infection making holes in their own PCs. But such viruses can be detected by the use of virus wall, antivirus server and regular monitoring of bandwidth usage at the gateway. The problematic client IP entries on such servers can be identified. IT staff can arrive at counter measures to keep ICT facilities free from any threats. Virus wall is a programme used to block the transmission of files infected by a virus.

14) Regularly (weekly) perform a Windows update and periodically scan your files.

Self Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

5) Discuss how to make Internet systems secure.

.....

.....

.....

.....

6) What is client/server technology and explain its importance on the Internet?

.....

.....

.....

.....

7) What is the difference between IP address and URL web address?

.....

.....

.....

.....

8) What is the difference between www and internet?

.....

.....

.....

.....

9) How does information travel on the Internet?

.....

.....

.....

.....

10) Explain difference between malware and spyware.

.....

.....

.....

.....

Activity II: Prepare a checklist of the various security options adopted on your computer.

5.10 WEB SEARCH

The World Wide Web (aka Web) is a vast pool of information resources, comprising millions of documents. Internet is the means to access this set of interlinked resources. Information on the Web is just a click away.

Google, Excite, Lycos, AltaVista, Infoseek and Yahoo are all search engines. These search engines can discover information on almost any topic in seconds. For starting a web search, type the URL of a Web search engine in the search bar on your Internet browser. The home page of the search engine will open up. It has a search box. For searching information on this search engine you have to enter your query words in the search box.

For example, to find documents containing an exact phrase, type the phrase with double quotes into the search window. For example, typing "library classification" will return documents that contain the phrase "library classification" but not Web pages that contain only 'library' or 'classification'.

Typing the phrase library classification without any double quotes will retrieve documents containing the terms 'library', 'classification' and 'library classification'.

Some tips for conducting a better search

- Search should be simple: just type whatever comes to mind in the search box. Most queries do not require advanced operators or complicated syntax. Simple is good. Most of the time, you will find exactly what you are looking for with just a basic query (the word or phrase you are searching for).
- Every search word matters. Generally, all the words we type in the query will be used by the search software.
- Search is always case insensitive. A search for 'ignou' is the same as a search for 'IGNOU'.
- Generally, punctuation and other special characters are ignored.
- Think how the page we are looking for will be written. Since a search engine is a program that matches the words we give to pages on the web, use the words that are most likely to appear on the page.
- Brevity is rewarding. Describe what we need as briefly as possible. The goal of each word in a query is to focus it further. Each additional word used in the query limits the results leading to loss of useful information. We can always refine the search by adding more terms (even from the results) if we did not get what we wanted.
- Avoid using common words and leave out ambiguous phrases. Choose descriptive words. The more the word chosen for search is unique, the more the chances to get relevant results.

Activity III: Conduct a search on local festivals on at least three search engines and make a list of the important ones and its coverage in the search engines.

5.11 SUMMARY

The Unit enabled you to understand the basics of Internet like what is a computer network, how a local area network differs from a wide area network and the functionalities of clients and servers. A short history of the technological revolution called Internet is also attempted. A brief explanation of the working of Internet has been given. How to set up an Internet connection is explored. Utility of protocols, POP and VoIP are touched. Being so distributed and varied with massive user base, security is crucial to Internet success and some options to keep systems more secure are highlighted. The Unit ends with how to conduct effective search on Internet.

5.12 ANSWERS TO SELF CHECK EXERCISES

1) DNS is an acronym for *Domain Name System*. It is an Internet service that automatically converts the domain name/hostname to the IP address of the Web server which hosts the site. It is therefore possible to address a Web site on TCP/IP networks by name and not by IP address. The importance of DNS lies in the fact that it is easier to remember the name of a site than its IP address described in numerals. DNS is a distributed, hierarchical database of name and IP address data that is widely used on the Internet.

2) Protocols are rules, standards, or an agreed-upon language that govern the communication (transmission of data packets) between different machines, computers, or nodes on a network. If two devices in a network need to communicate, they need to use a common protocol.

3) Internet is a globally interconnected network of TCP/IP networks of LANs and WANs. LAN is a private and localised network. Several interconnected LANs constitute WAN. The Internet, by contrast, is a global, public network (global WAN) that links millions of smaller networks with over a billion computers connected at any given time. Internet and LAN differ not only in terms of geographical coverage of the network, but in terms of network protocol also. LAN network works on Ethernet protocol or Token Ring or FDDI. Internet uses TCP/IP protocol. You have to use TCP/IP if you want a computer to work on the Internet. For this reason TCP/IP protocol is used on LAN to share a single Internet connection with all computers on LAN.

4) IP address is a unique number given to identify a host computer on the Internet. It is a number string used for identification of computer on the network. For example, IP address of IGNOU host is 14.139.40.44; it is this number that is used on the Internet to search IGNOU host. The IP number is called an "address" because it serves the same purpose as a home address; it is used to identify each device on the Internet and its location to help direct Internet traffic.

   A hostname is a unique name by which a computer is known on a network; it corresponds to an IP address. IP addresses are hard to remember, so we usually identify networked computers using hostnames (aka hosts). Hostnames are automatically translated into IP addresses by a special system called DNS (short for Domain Name System). For example, the hostname for IGNOU host is www.ignou.ac.in.

   A hostname is composed of two parts. The first part is the local name, which in the above example is 'www'. The second part 'ignou.ac.in' is the domain name. When you combine the two parts you have the hostname. A domain name may be a hostname if it has been assigned to an Internet host and associated with the host's IP address. The part 'www' in the hostname implies that the named networked computer serves web pages.

   Domain names are hierarchical. Domain name is composed of two or more parts (separated by dots). Each part in the domain name hierarchy corresponds to top-level domain, second-level domain or to sub-domain. For example, the domain name for IGNOU is ignou.ac.in. In this domain name, the top-level domain is '.in' (called as dot-in), followed by second-level domain such as '.ac' (called as dot-ac) and third-level domain is 'ignou'. The 'www' in the hostname of IGNOU (www.ignou.ac.in) is simply another level to the domain name (also known as a sub-domain).

5) Despite every precaution to protect the Internet system against viruses, it is impossible to stop viruses altogether. The steps to keep the system secure against viruses are: (i) maintain up to date antivirus definitions, (ii) perform regular scanning of e-mail servers and internet traffic to minimise the system exposure to viruses, (iii) password controlled access to the system, (iv) employ firewall to control network traffic, (v) maintain regular backups, (vi) avoid accessing dubious sites, (viii) avoid responding to such phishing mails, spam mails, and (ix) watch free downloads.

6) Computers on the Internet are interconnected through client/server computing technology. A client is a software programme in a computer (Desktop PC) that sends requests to a remote server (host computer that offers resources) on a network. The server computer in response sends information back to the client

computer. Consider a Web browser and a Web server. Web browsers are clients that connect to web servers, retrieve web pages on request from the server for display. Communication between web client and web server takes place on TCP/IP and HTTP protocols. The client/server model is also at work in the case of other Internet tools like e-mail, FTP, Telnet and chat.

7) An IP address specifies just the location of the host computer while a URL specifies location, protocol and specific resource. A URL (Uniform Resource Locator) indicates the unique address of a file that can be web pages, documents, graphics, or programms on the Web. This is used by Web browsers, e-mail clients and other software to identify a *network resource* on the Internet URL requires a DNS server to identify and locate the host computer, while an IP address doesn't. A DNS locates and translates Internet domain name or the alphanumeric text of the URLs into associated IP addresses. Without the DNS, the request would fail as the computer would not be able to find the host. IP address can be part of a URL, although it is more common to see a domain name instead of an IP address.

8) The World Wide Web (WWW) is one set of tools running on the Internet to support websites. The Internet itself is a global, interconnected network of computing devices for enabling a wide variety of interactions and communications between its devices. The Internet and the World Wide Web bear a whole-to-part relationship. The World Wide Web broadcasts HTML pages viewed by using free software called web browsers. Web runs on HTTP (Hypertext Transfer Protocol), the language which allows consequential access to web pages. HTTP is a set of rules that control how files and other information are transferred between computers.

9) The Internet runs on TCP/IP (Transmission Control Protocol/Internet Protocol) suite of protocols. When a user sends any file from one point to another on the Internet, TCP protocols divided the file into parts (packets). Each of these packets is separately numbered and includes the Internet address of the destination point. The different packets for a given file may travel on different routes through the Internet. When they arrive at their destination, they are reassembled into the original file. It all sounds very complex and time consuming, but TCP manages this process of dividing the file into packets and reassembling them into the original file occurs very, very quickly. Internet Protocol, handles the address part of each packet so that it gets to the right destination. Without such a common set of protocols, communication between Internet devices (clients and servers) cannot happen.

- Data is divided up into *packets*
- Data routes across the Internet can be *switched* to avoid congestion
- Entire mechanism is handled by the TCP/IP protocols.

10) Malware (short for "malicious software") is a general term used to refer to the entire class of malicious software; spyware is just one of them. Malware are meant to impair the function of a computer like cause errors, slow your computer down or spread viruses. Spyware often doesn't cause major damage like other malware. When your system is connected to the Internet, it extracts personal information like credit card number and can and can therefore cause much more long-term damage by giving other people access to your online accounts, bank information and more. Spyware is mostly propagated through web pages, file sharing programs and "free" utilities installed from the Internet.

5.13 KEYWORDS

Cookie : A cookie is a small piece of data purposely sent from a website visited and the data so sent is stored in a user's web browser while a user is browsing the website.

Malware : Malware is malicious, hostile, intrusive software which attackers use to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Phishing : Phishing is the act of luring gullible e-mail users to reveal their personal details such as usernames, passwords and credit card details with the purpose of misusing such details for committing frauds.

Spam : Spam mails are known as unsolicited bulk mails, junk mails, or commercial mails.

5.14 REFERENCES AND FURTHER READING

American University in Cairo. *Internet Introduction*. June 2002. Web. 2 April 2013. <http://unsweb.aucegypt.edu/UNSWEB2/NetIntro.htm#what_makes_the_internet_work>.

Ascension Parish Library. *Internet Basics* an *Introductory Workshop to the Internet and the World Wide Web. Report*. Web. 15 April 2013. <http://saisdadultandcommunitycomputerclasses.wikispaces.com/file/view/Internet+basics+Handout.pdf>.

College of Arts and Sciences. *Lab 1.2: Internet Basics*. Web. 11 April 2013. < http://www.cis.uab.edu/courses/cs101/lab/lab1-2.pdf>.

HTTP State Management Mechanism – Overview. *IETF*. April 2011. Web. 2 April 2013. <http://tools.ietf.org/html/rfc6265>.

Milwaukee Public Library Foundation. *Internet Basics Class Outline.* Spring 2008. Web. 14 April 2013. <http://www.mpl.org/file/curriculums/Internet%20Basics%20Curriculum%20Spring%2008.pdf>.

University of North Carolina at Chapel Hill Libraries. *Internet Basics.* Dec 2012. Web. 12 April 2013. <http://www.lib.unc.edu/cws/handouts/Internet_Basics.pdf>.