Indira Gandhi
National Open University
School of Social Sciences

BLI-224
ICT Fundamentals

Block

1

BASICS OF ICT

Programme Design Committee

Prof. Uma Kanjilal (Chairperson)
Faculty of LIS, SOSS, IGNOU

Prof. B.K.Sen, Retired Scientist, NISCAIR
New Delhi

Prof. K.S. Raghavan, DRTC
Indian Statistical Institute, Bangalore

Prof. Krishan Kumar, Retired Professor
Dept. of LIS, University of Delhi, Delhi

Prof. M.M. Kashyap, Retired Professor
Dept. of LIS, University of Delhi, Delhi

Prof. R.Satyanarayana
Retired Professor, Faculty of LIS, SOSS, IGNOU

Dr. R.Sevukan (Former Faculty Member)
Faculty of LIS, SOSS, IGNOU

Prof. S.B. Ghosh, Retired Professor
Faculty of LIS, SOSS, IGNOU

Prof. T. Viswanathan, Retired Director
NISCAIR, New Delhi

Dr. Zuchamo Yanthan
Faculty of LIS, SOSS, IGNOU

Conveners:

Dr. Jaideep Sharma
Faculty of LIS, SOSS, IGNOU

Prof. Neena Talwar Kanungo
Faculty of LIS, SOSS, IGNOU

Programme Coordinators

Prof. Jaideep Sharma and
Prof. Neena Talwar Kanungo

Course Coordinator

Prof. Uma Kanjilal

Programme Editor

Prof. Jaideep Sharma

Course Preparation Team

Unit No(s).	Contributor(s)
1-3	Dr. Naveen Kumar Singh
4	(Late) Prof. T. Viswanathan

Internal Faculty:
Prof. Uma Kanjilal
Prof. Neena Talwar Kanungo

Course Editor
Prof. Uma Kanjilal

Material Production

Mr. Manjit Singh
Section Officer (Pub.)
SOSS, IGNOU

Secretarial Assistance

Ms. Sunita Soni
SOSS
IGNOU

Cover Design

Ms. Ruchi Sethi
Web Designer
E Gyankosh
IGNOU

July, 2014

ISBN : 978-81-266-6771-0

Further information on Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110 068 or visit University's Website http://www.ignou.ac.in.

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi by Director, SOSS.

Lasertypesetted at Graphic Printers, 204, Pankaj Tower, Mayur Vihar, Phase-I, Delhi-110091.

Printed at :

BLOCK 1 BASICS OF ICT

Introduction

Information Communication Technology (ICT) is undoubtedly playing an important role in almost every aspect of our life. Development in computer technology both in terms of speed and storage capacity provides a tremendous support in terms of information management. Computers are now ubiquitous in almost all offices, and have become a part and parcel of almost all activities in libraries and information centres.

Last few decades have witnessed significant development in the field of telecommunications, computer networking and Internet. Computer technology combined with communication and network technology has great potential to support one and all even those residing in the remote corners of the world, in processing, storage and dissemination of information. The world is evolving towards a Networked Electronic Information Society (NEIS) with the convergence of technologies and has invaded almost all aspects of our life.

For the Library and Information professionals it is essential that they are adept with the emerging technologies so that they are in a convenient position to use ICT according to the various requirements of libraries and information centres.

This block has four Units. In **Unit 1** on **Basics of Computer Technology** you are introduced to the computer hardware and other I/O devices. It also discusses Ubuntu operating system. **Unit 2, Basics of Communication Technology** discusses data communication modes, communication hardware and protocols and standards. **Unit 3** introduces you to the **Basics of Network Technology**. It covers LAN, WAN and wireless technology. The last unit in this Block, **Unit 4** is on **Technology Convergence** covering its genesis and convergence from the point of view of technology, protocol, access, services and applications.

Blank Page

UNIT 1 BASICS OF COMPUTER TECHNOLOGY

Structure

1.0 OBJECTIVES

After completing this Unit, you will be able to:

- describe the basic architecture of the computer;
- discuss the use of various hardware and peripheral devices;
- explain the functions of major hardware components; and
- understand the basic working of Ubuntu Linux operating system.

1.1 INTRODUCTION

The utilisation of computer technology is well recognised, in almost all fields of governance, businesses, libraries, education, etc. Today, computer technology has infused every sphere of common man. From banking to shopping, railway reservation to medical prescription. In this unit, we will introduce you to the basic computer technology and how it works? Knowing internal and external components of a computer system is important for a beginner of computer technology. This unit will provide you the basic knowledge about the devices associated with computer system particularly in the context of library systems. In addition we will also try to discuss some of the basic functions of an operating system, which actually creates an interface between the computer hardware and you. Please note that this unit covers only the basics of computer technology. For further details you may refer to suggested further readings given at the end of the unit.

1.2 OVERVIEW OF COMPUTER SYSTEM

Before starting an introduction about computer, let us understand the need and reason why computers are so much important for us. Generally computers help us in performing tasks that are repetitive, involve calculation or manipulation of data and perform tasks that involve storage of large quantities of information.

Computer can be defined as "An electronic machine that is capable of interpreting and executing stored program (sequence of instructions), input data, perform operation on data (calculation and logical operations), and output the results". The data which normally we deal with consists of numeric and characters such as decimal digits 0 to 9, alphabets A to S, operators (e.g. +, -, >, =, etc.) and many other special characters or images (e.g.; @, {,],etc.). However, computers cannot understand such form of data and hence it has to be transformed into binary-form (also known as machine language) by using two symbols 0 and 1, which are called binary digits or bits. For Example: If we want a computer to do ADD (2, 3); computer needs to map this particular instruction into a binary form. Lets assume the mapping is "01= ADD, 2=10, 3=11", for a computer this instruction will be "01 10 11". One of the key aspects in program execution is the execution of an instruction. The key questions that can be asked in this respect are:

a) How are the instructions supplied to the computer?

b) How are they interpreted and executed?

Most of today's computers look like what is illustrated in Figure 1.1. The designs are based on concepts developed by John Von Neumann referred to as the Von Neumann architecture (shown in Figure 1.2).

Fig. 1.1: A Modern Computer

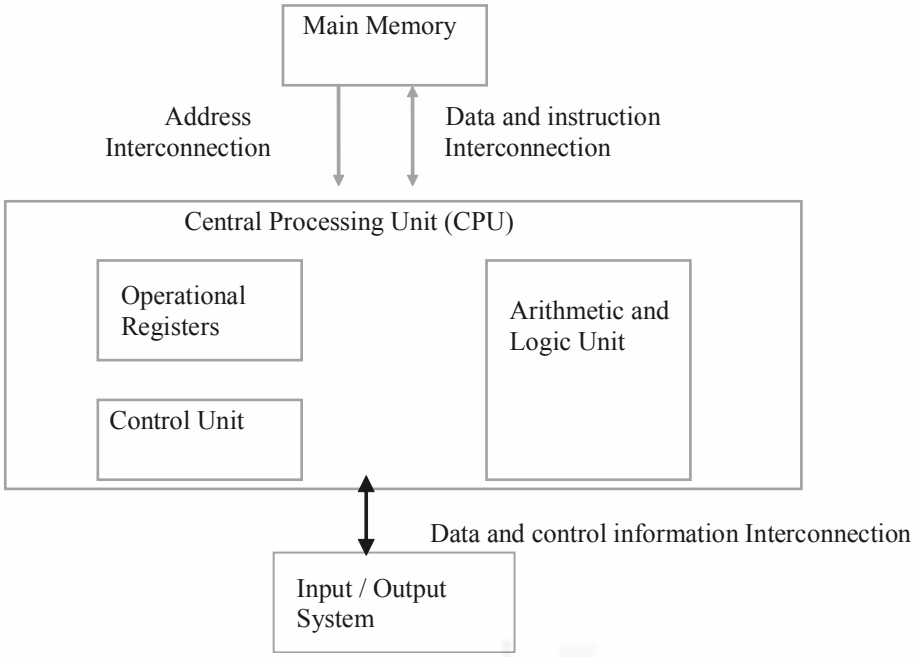

Fig. 1.2: Von Neumann Computer Architecture

Von-Neumann proposed that there should be a unit performing arithmetic and logical operation on the data. This unit is termed as Arithmetic Logic Unit (ALU). One of the ways to provide instruction to such computer will be by connecting various logic components in such a fashion, that they produce the desired output for a given set of inputs. The process of connecting various connections is termed as Hardwired. But this is a very inflexible process of programming. Let us have a general configuration for arithmetic and logical functions. In such a case there is a need of a control signal, which directs the ALU to perform a specific arithmetic or logic function on the data. Therefore, in such a system, by changing the control signal the desired function can be performed on data. Any operation, which needs to be performed on the data, can be obtained by providing a set of control signals. Thus, for a new operation one only needs to change the set of controls.

The Arithmetic Logic Unit (ALU) and the Control Unit (CU) together are termed as the Central Processing Unit (CPU). The CPU is the most important component of a computer's hardware. The ALU performs the arithmetic operations such as addition, subtraction, multiplication and division, and the logical operations such as:

- Is A = B? (where A and B are both numeric or alphanumeric data)
- Is a given character equal to M (for male) or F (for female)?

The control unit interprets instructions and produces the respective control signals. How can the instructions and data be put into the computers? The instruction and data needs to be supplied by external environment. For this an input module is needed. The main responsibility of input module is to put the data in the form of signals that can be recognised by the system. Similarly, we need another component, which will report the results in proper format and form. This component is called output module. These components are referred together as input/output (I/O) components.

The memory unit stores all the information in a group of memory cells, also called memory locations, as binary digits (bits). Each memory location has a unique address and can be addressed independently. The contents of the desired memory locations are

provided to the central processing unit by referring to the address of the memory location. The amount of information that can be held in the main memory is known as memory capacity. The capacity of the main memory is measured in Kilo Bytes (KB) or Mega Bytes (MB). One kilobyte stands for 2^{10} bytes which 1024 bytes (or approximately 1000 bytes). A mega byte stands for 2^{10} Kilobytes, which is approximately little over one million bytes.

Computers are therefore, made of four major components (parts):

1) **Input units:** Humans interface with the computer through devices like the mouse and keyboard.

2) **Central Processing Unit**: Referred as "Brain" of the computer that controls all computer operations, processes information and computes results. It is the logical component of a computer system that interprets and executes program instructions. This component comprises:

   - Control Unit- that interprets program instruction, directs the internal operation, and controls the flow of data in and out of primary memory.
   - Arithmetic and Logical Unit- that performs the arithmetic and logical operations.
   - Memory- also called primary memory holds the input/output data and program instructions. Memory is made of Integrated Circuits or Chips that are tiny silicon chips. In each chip thousands of electronic components are engraved.

3) **Secondary Storage** or Auxiliary Storage is a means for permanently storing data. Do not confuse it with the memory. Memory is a small size storage, which is used by CPU and operating system for its own use. Due to this reason it is sometimes not considered as major components of computer system, instead it is considered as an input/output Device.

4) **Output Units:** data is transferred from a computer to an output device like the printer and monitor where the results are displayed.

1.3 COMPUTER PERIPHERALS AND HARDWARE

There are two terms commonly used in computer world, computer hardware or simply hardware and peripherals. Let us discuss what we mean by these terms. As you know computer is an electronic device that has the ability to store, retrieve, and process data. The physical parts that make up a computer (the central processing unit, input, output, and memory) are called **hardware**. Any hardware device connected to a computer and any part of the computer outside the CPU and working memory is known as **Peripherals**. Some examples of peripherals are keyboards, mouse, monitors, printers, scanners, barcode reader, tape drives, microphones, speakers, joysticks, plotters, and cameras.

1.3.1 Computer Peripherals

When you look on a simple computer you can see Central Processing Unit (CPU) cabinet, Monitor, Keyboard and Mouse. Your computer and you interact through these peripherals. The keyboard and monitor are the minimum peripherals you should have with your computer. Your choice of peripherals depends on personal preference and the complexity of the interactions you intend to have with your computer.

Computer Monitors

The computer monitor is an output device that displays input on a screen and is very similar to a television monitor. When the computer wants to display something, it calculates how it needs to change the color and brightness of the different pixels, and changes the values in the video memory. The smaller the pixels, the clearer and sharper the picture appears on the monitor. Earlier CRT monitors were used as given below in the figure 1.3a. Nowadays the LCD monitors (as shown in figure 1.3b) are in common use these are thinner in size and uses lesser electricity.

Fig. 1.3a: CRT Monitors

Fig. 1.3b: LCD Monitors

Keyboard

The computer receives most of its input from the user via the keyboard that is very similar to the typewriter keyboard as shown in figure 1.4 given below. This input device is connected by a cable to the keyboard port on the back of the computer. There are extra keys on the computer's keyboard that are not found on a normal typewriter. The exact manner in which the keys function depends on the software program. We have different type of keyboards available nowadays which can support multimedia activities and Internet browsing.

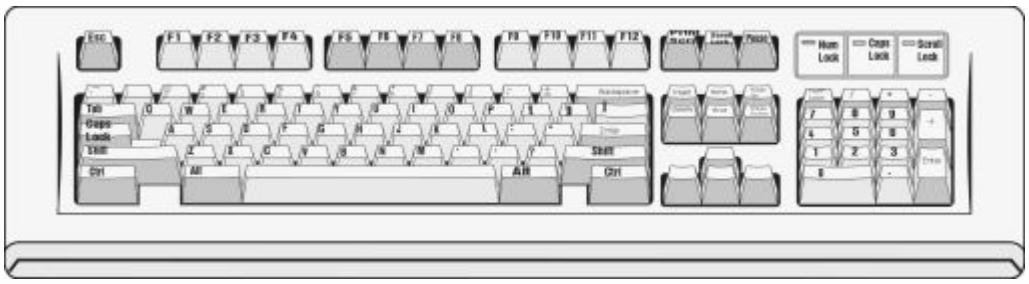

Fig. 1.4: A Computer Keyboard

As shown below in the figure 1.5, mouse is a pointing input device attached to the computer that controls the movement of the cursor on the screen. It allows the user to execute commands using point & click and click & drag techniques. As the user moves the mouse across the pad, the cursor moves across the screen. The mouse should always be used with a mouse pad to provide a smooth surface for mouse movement and to help keep the mouse from damage. If you "run out of room" on the pad, simply

pick up the mouse and move it to the opposite edge and continue movement. Generally, mouse has two buttons (left and right) and newer mice have a scroll wheel between the two. Mouse commands are executed by "clicking". The term "click" refers to the left mouse button.

Fig. 1.5: Mouse a Pointing Device Attached to the Computer

Printer

A printer is an output device to transfer images and text from a computer to a printed page as given below in figure 1.6. Printers take information from the CPU and transfer it to paper, provide a hard copy (permanent human-readable text and/or graphics) of documents stored in electronic form, usually on physical print media such as paper or transparencies. Many printers are primarily used as local peripherals, and are attached by a printer cable or, in most new printers, a USB cable to a computer, which serves as a document source. Some printers, commonly known as network printers, have built-in network interfaces (typically wireless or Ethernet), and can serve as a hardcopy device for any user on the network. Individual printers are often designed to support both local and network connected users at the same time.

There are a number of different printer technologies available: Dot Matrix, Ink Jet or Laser. Inkjet printers use small cartridges full of different colour inks. They squirt a tiny drop of ink onto the paper using a bubble or pressure to form a dot. All the dots are layered on top of each other to form the desired colour. Laser printers are more expensive to run but produce a crisper image.

Fig. 1.6: Laser Printer

Scanner

An input device that is becoming less used with the advent of digital cameras. A scanner (shown below in the figure 1.7) is an optional extra rather than a necessity peripheral device connected to the Personal Computer (PC) via the parallel port or USB port. It allows you to digitise a flat, paper image and transfer it to your computer where the image can be manipulated. For instance you may use it for digitizing old photographs that can be stored on the hard drive, repaired, enhanced and printed out on a printer.

Fig. 1.7: A Scanner

Barcode Readers

Barcode reader is an input device for reading printed barcodes. We can also say it's a special scanner for barcodes. You all must have seen barcodes, that are printed on most of the products we use in our daily life. It looks like thin and thick series of black lines as shown below in figure 1.8:

Fig. 1.8: Example of a Barcode

Barcode reader consists of a light source, a lens and a light sensor interpreting optical impulses into electrical signals. Furthermore, almost all barcode readers contain decoder circuitry analysing the barcode's image data provided by the sensor and sending the barcode's content to the scanner's output port.

The barcode reader types can be classified based on the scanning methods; some of these types are described below:

Pen Readers

It requires the operator to swipe the pen over the code. Pen type readers consist of a light source and a photodiode that are placed next to each other in the tip of a pen or wand. A pen reader is shown below in figure 1.9.

Fig. 1.9: Pen Type Barcode Readers

To read a barcode, the tip of the pen moves from corner to corner the bars in a stable shift. The photodiode measures the intensity of the light reflected back from the light source and produces a waveform that is used to measure the widths of the bars and white spaces in the bar code. Black bars in the bar code absorb light and white spaces reflect light so that the voltage waveform produced by the photo diode is a representation of the bar and space pattern in the bar code. Further, the scanner decodes this waveform.

Laser scanners

Laser scanners as shown below in figure 1.10, work similar like a pen readers except that they use a laser beam as the light source and normally utilise either a reciprocating mirror or a rotating prism to scan the laser beam back and forth across the barcode.

Fig. 1.10: Laser type Barcode Readers

CCD Readers

Charge Coupled Device readers also called as LED scanner, use an array of hundreds of tiny light sensors queued up in a row in the head of the reader, it is shown in figure 1.11. Every sensor measures the intensity of the light immediately in front of it.

Fig. 1.11: LED Barcode Readers

The important difference between a LED reader and a pen or laser scanner is that the LED reader is measuring emitted ambient light from the bar code whereas pen or laser scanners are measuring reflected light of a specific frequency originating from the scanner itself.

Camera-Based Readers

Two dimensional imaging scanners or camera based barcode readers are the newest types of barcode reader currently available. They use a small video camera to capture an image of a bar code as depicted in a figure 1.12. The reader then uses digital image processing techniques to decode the barcode.

Fig. 1.12: Camera based Barcode Readers

Speaker

Computer speakers shown in figure 1.13 or multimedia speakers, are external speakers, commonly equipped with a low-power internal amplifier.

Fig. 1.13: A Set of Computer Speaker

Modem

A modem enables a computer to transmit data over telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms. Modems come in two forms: Internal and External; Internal modems are PCI cards that you can connect as shown in the figure 1.14a. In figure 1.14b External modem is shown, that are kept outside of your computer, connected either by a USB or Serial Port.

Fig. 1.14a: Internal Modem

Fig. 1.14b: External Modem

Radio-Frequency Identification (RFID)

RFID architecture works like a small area (generally in few meters) client-server network based on radio frequencies for communication between client and server. It has two component RFID Client Tag and RFID server or antenna or receiver. RFID tag is applied or incorporated into an object or a product for the purpose of identification and tracking using radio waves. RFID tag is an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, and other specialised functions. The receiver or antenna is for receiving and transmitting the signal. There are generally three types of RFID tags as shown below in the table 1.1:

Table 1.1: Classification of RFID tags

ACTIVE RFID TAGS	Contain a battery and can transmit signals autonomously.
PASSIVE RFID TAGS	Have no battery and require an external source to provoke signal transmission.
BATTERY ASSISTED PASSIVE (BAP)	Require an external source to wake up but have significant higher forward link capability providing great read range.

Among the many uses of RFID equipments, one is its implementation in libraries. This technology has gradually begun to replace the conventional barcodes on library items. The RFID tag can contain many identifying information, such as a book's title, author's name, publication year, publisher name, book type, etc. This information is read by an RFID reader, which replaces the standard barcode reader. The RFID tag used on products or library materials typically measures 50 mm X 50 mm. It may replace or be added to the barcode to provide an innovative and easier way for other inventory management also. It can also act as a security device, taking the place of the more traditional electromagnetic security strip and not only the books, but also the membership cards could be fitted with an RFID tag.

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) What is a significance of ALU in CPU?

.....

.....

.....

.....

2) Calculate the number of bits in two-kilobytes.

.....

.....

.....

.....

3) How inkjet printers work?

.....

.....

.....

.....

4) Differentiate between LED and Pen type barcode readers.

.....

.....

.....

.....

5) How RFID technology can be useful for library management?

.....

.....

.....

.....

1.3.2 Computer Hardware

In general when we use the term hardware it refers to nuts and bolts available at the hardware shops. Similarly the nuts and bolts of a computer is called hardware, which is a physical, electrical, and mechanical parts of the computer. In the last decade or so, the hardware technologies have seen many changes and also have advanced remarkably. From few kilobytes of RAM (Random Access Memory), now the PCs have couple of Gigabytes of RAM, hard-disks have also improved from few Gigabytes to hundreds of Gigabytes memory space, and also other drives and monitor have also emerged with better performance and cost. In this section we will study about the different internal hardware components of a computer.

CPU (Central Processing Unit)

The CPU is the computer's control center, it appears as shown in figure 1.15. Think of it as the brain that does all the thinking (computation). It reads instructions from your software and tells your computer what to do. The actual CPU is about 1.5 inches square, yet it is the most critical part of the computer. The speed at which the CPU processes information internally is measured in Megahertz (MHz) and Gigahertz (GHz). 1 GHz is equal to 1,000 MHz. Generally; processors with higher MHz or GHz enhance your ability to run creative, entertainment, communication, and productivity applications.

Fig. 1.15: Central Processing Unit

Motherboard

Sometimes called the system board or main board, the motherboard is the main circuit board of a PC. The motherboard (shown in figure 1.16) is the central nervous system and circulatory system, plus much more, all rolled into one. The motherboard typically

contains the processor (or CPU), BIOS (basic input/output system), memory, mass storage interfaces, serial and parallel ports, expansion slots, and all the controllers required to communicate with standard peripheral devices, such as the display screen, mouse, keyboard and disk drive. Collectively, some of the chips, which reside on the motherboard are known as the motherboard's chipset.

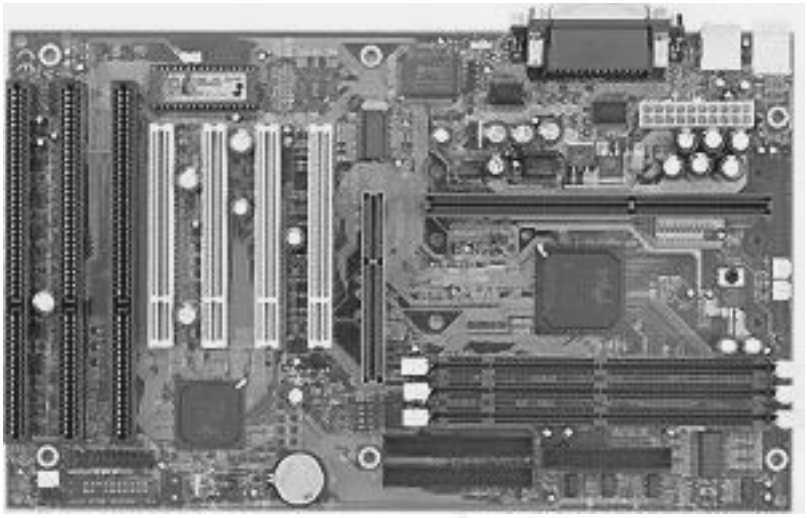

Fig. 1.16: The Motherboard

Power Supply Unit

The Power Supply Unit appears as shown in figure 1.17, is the most important component in a PC. This is the core of the system and is needed to supply power to the motherboard, which in turn, supplies power to all the other components inside and sometimes outside the computer case. Its fundamental function is to convert available power from the wall socket, to the type that a computer can use. It converts 230 volt current and splits it into useable +3.3v, +5v and +12v DC current.

Fig. 1.17: Power Supply Unit

ROM (Read Only Memory)

A type of memory chip which does not lose information even when the power is turned off. Once data is programmed into the ROM chip, its contents cannot be altered. For example, ROM BIOS chips are used to store information for starting up your computer.

RAM (Random Access Memory)

RAM as shown in figure 1.18 are chips that allow data to be written to, however unlike hard disks, the data is short term and is only used for the duration the PC is switched on. Data can be accessed very quickly using this method of temporary storage. Memory comes in many different types and sizes depending on the type of motherboard you have.

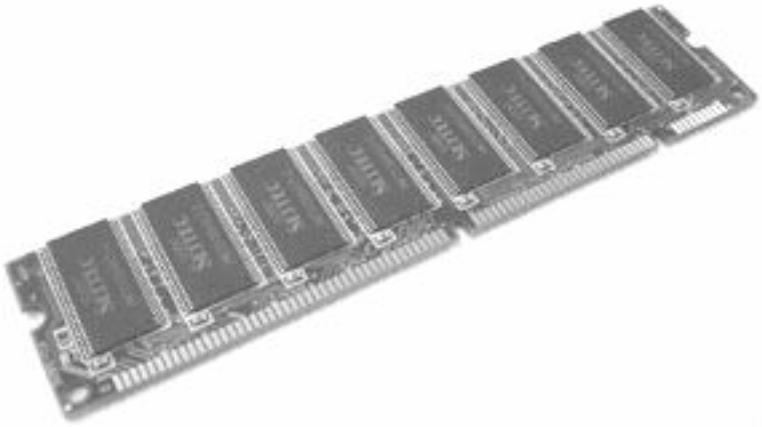

Fig. 1.18: Random Access Memory

Storage Devices

Computers are also known, as data processing machine, to store and process data computer must have memory. There are different kinds of memories like primary memory and secondary memory, primary memories like RAM (random access memory) and ROM (read only memory) is computer personal memory used to process its own data. However, the secondary memory is an off-line memory, which is used to store and carry the data like floppy disk, compact disk, hard disk etc.

Hard disk: It is normally large size memory that a computer uses to store information. Most computers come with one or two hard drives, situated inside the computer cabinet. The terms hard drive and hard disk are used interchangeably. Today's hard disks provide fast access and can hold several gigabytes of information as compared to megabytes on floppy disks. But hard disks are permanently fixed with screws in the computer cabinet; rarely we plug it out because detaching it frequently is not safe. Hence, to carry data we need some removable memory disk, further in this section we have listed some of these removable disks.

Floppy Disk: These are removable disk that stores information magnetically. You can use a floppy disk to read/write information between computers, or to make a backup of your files. Floppy disks are 3.5 inches in diameter and have a storage capacity of 1.44 MB. These are now obsolete.

Zip disks: This is also a removable disk, which can store 100 - 250 MB of data. A special 3.5" removable disk drive is needed to retrieve the information from the computer and write to the zip disk. An external zip drive can be moved from one computer to another.

Cartridge tapes: These are magnetic tapes similar to cassette tapes used for the purpose of storage and backup. Since the information is stored sequentially, in the cartridge tapes, backup and retrieval of stored information is slower. The advantage of tape is that they can be purchased with large storage capacities (1– 4 GB) allowing the entire contents of the hard drive to easily fit on one tape.

CD-ROMS: Compact disks can store approximately 650-800 MB of data or 74-80 minutes of music. These drives are read only and cannot be used for recording data.

Read/Write CD-ROMS: CD-ROM drives that write, rewrite and record data. Two types of CD-ROM disks are used: CD-Recordable (CD-R) and CD-Read/Write (CD-R/W). CD-R/W's can only be "read" by CD Read/Write drives, while CD-R disks can be read by most CD-ROM drives.

Digital Video Disc (DVD): A digital video disc (DVD) is a type of optical disc storage technology that looks like a CD-ROM disc, but can store greater amounts of data. DVDs are often used to store full-length movies and other multimedia content that requires large amounts of storage space. But to run the DVD we should have a DVD drive.

USB/Flash Drive: USB drives are very popular removable disks in current time. It is a plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. These drives can be used in place of a floppy disk, zip drive disk, or CD. When the user plugs the device into their USB port, the computer's operating system recognises the device as a removable drive. Unlike most removable drives, a USB drive does not require rebooting after it is attached, do not require batteries or an external power supply, and is platform independent. Several USB drive manufacturers offer additional features such as password protection, and downloadable drivers that allow the USB drive to be compatible with older systems that do not have USB ports. USB drives are available in capacities ranging from 1GB to 32 gigabytes GB.

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.

6) What is BIOS?

.....

.....

.....

.....

7) How DVDs are different from CDs?

.....

.....

.....

.....

1.4 OPERATING SYSTEM

In contrast to the hardware, software are the non-physical components of the computer system. A set of instructions is known as programs and a set of programs, which gives a finite output, is called software. Operating system is the first software that you work on the first time or whenever you start your computer. Computers need something to manage all the hardware components and give an interactive interface to control these hardware devices, which are taken care by the computer operating system. There are different operating systems available like Microsoft Windows based operating systems like Windows 7 or UNIX or Linux variants etc. In this unit we will discuss Linux based operating system Ubuntu. Linux is a freely available, open source, Unix-like operating system. Written originally for the PC by Linus Torvalds, with the help of many other developers across the Internet, Linux now runs on multiple hardware platforms. Because of its speed, stability, and low cost, Linux became the fastest growing operating system

for servers. Today, Linux is widely used for both basic home and office uses. It is the main operating system used for high performance business and in web servers. Linux has made a huge impact in this world. Now days there are many Linux based operating systems available. Some of its most popular flavours are Red Hat Linux, Fedora and Ubuntu. Most of the Linux based operating system has the following given features, however these may vary from version to version:

- **Low Cost/Free:** Linux and much of its software come with the GNU General Public License and hence it is free and open source.
- **Stability:** Linux has high stability compared with other operating systems. There is no need to reboot the Linux system to maintain performance levels.
- **Performance:** Linux provides high performance on various networks. It has the ability to handle large number of users simultaneously.
- **Networking:** Linux provides a strong support for network functionality; client and server systems can be easily set up on any computer running Linux. It can perform tasks like network backup faster than other operating systems.
- **Flexibility:** Linux is very flexible and can be used for high performance server applications, desktop applications, and embedded systems. You can install only the needed components for a particular use. You can also restrict the use of specific computers.
- **Compatibility:** It runs all common Unix software packages and can process all common file formats.
- **Fast and Easy Installation:** Linux distributions come with user-friendly installation.
- **Better use of Hard Disk:** Linux uses its resources well enough even when the hard disk is almost full.
- **Multitasking:** Linux is a multitasking operating system. It can handle many things at the same time.
- **Open Source:** Linux is an Open source operating systems. You can easily get the source code for Linux and edit it to develop your personal operating system.

1.4.1 Ubuntu Operating System

Ubuntu is an operating system based on Linux that is also developed by a worldwide community of programmers. Ubuntu is based on the concept of free or open-source software, meaning that you do not pay any licensing fees for Ubuntu, and you can download, use, and share the operating system free of charge. Being a Linux-based operating system, Ubuntu has a well-deserved reputation for stability and security. Ubuntu is generally acknowledged to be the most widely used version of Linux available.

Comparing Ubuntu with Windows

Before starting with Ubuntu, it is very important for us to understand the differences between Windows and Ubuntu. The most noticeable way is licensing and distribution terms can be used to differentiate between Ubuntu operating systems and Microsoft Windows. Ubuntu is open software and it's completely "free software" free means the freedom to run, use, modify, redistribute copies, and release your improvements to the public. In addition to this it includes many of the software's used for everyday computing at no cost, unlike Windows. Some of these are given below:

Office Suite: A full office suite with a word processor, spreadsheet, and presentation software that can read and write in .doc, .xls, and .ppt formats and can also output to PDF.

Desktop Email Client: Evolution, an email program with a similar interface to Microsoft Outlook.

Web Browser: Firefox, the increasingly popular Web browser.

Others Software: Ubuntu's online Applications Guide lists some Ubuntu-compatible applications that allow you to edit images, listen to and manage music, edit and watch videos, read PDFs.

Updates and bug fixes: Frequent security updates and bug fixes for applications and the operating system are managed by Ubuntu which makes its working robust and bug free.

Start Linux Ubuntu

The following are few important steps and procedures will be helpful to install Ubuntu operating system, however it is important for you to check the minimum hardware requirements for Ubuntu installation as it may varies from version to version. As shown below in the figure 19 this screen appears as first boot screen, as you can see it has many options with an advice that for desktop or laptop installation default installation is suitable, however it can show some more option on press of F1 key.

Fig. 1.19: Ubuntu the First Boot Screen

As we are doing this installation for a desktop, let's prefer default option and press enter. We advise you not to go for server install unless you completely know about it. After you Press Enter, you may find a cluster of internal installation line scroll on the screen as shown below in figure 1.20, but it is normal processing so ignore it.

Fig. 1.20: Ubuntu Internal Installation Process on the Screen

After this Ubuntu will ask few questions to complete your personalised setting for language, time zone, username and password. In addition to these questions there are a few other questions that may cause some confusion. During installation it shows the status of the process being completed as shown below in figure 1.21.

Fig. 1.21: Status of the Process

When it will ask for Partitioning choose the Erase Entire Hard Drive option, if you are not installing Ubuntu with any other operating system on your computer. The boot loader determines which operating system the computer boots to. Hence, It is recommend to install Grub a boot loader to the MBR (Master Boot Record). Now you need to reboot your computer to install the other packages, if you are asked to drive out the installer disk, you can take it out as for further this disk is no more needed. If boot loader Grub is not installed in MBR as advised earlier you have to use boot-floppy or some other boot loader to finish the installation process. Once that finishes, you should get to a login screen as shown below in figure 1.22. Now you need to enter your recently created username and password during the installation process.

Fig. 1.22: Ubuntu Login Screen

1.4.2 Ubuntu File System

Before working on the operating system it is always important to understand the file system i.e. how files and folders or directories are organised in Linux.

Boot Directory: It has the boot information, including the Grub configuration file.

etc Directory: This has a lot of settings for software repositories you use and what other partitions or drives you have "mounted".

Home Directory: This is the only directory you will have access to without using your password to gain temporary administrator privileges. All of your files reside here, along with your settings and preferences, inside a folder called /home/username unless are not installed in a particular folder. So if your username is naveen, your files and settings will be in the /home/naveen folder.

Media Directory: or /mnt are where your media (CDs, DVDs, USB drives, etc.) and mounted partitions would go.

Root Directory: is the /home folder for root and has its own settings.

Usr Directory: is where a lot of stuff is stored that users will be using.

1.4.3 Common Commands and Utilities

The following are some of the basic commands you should know for working on any linux based operating system:

startx — If you happen to end up at a command-prompt without any graphics, you can log in and try typing this command to get back to the graphical (or "x") system.

xkill — Kills a misbehaving application. Once this command is run, the mouse cursor will become a skull and crossbones. Any window you click on after that will close immediately.

alias — Alias is used to substitute a small or more familiar name in place of a long string. It is commonly used for a long strings that are frequently used.

awk — awk utility is powerful data manipulation/scripting programming language (In fact based on the C programming Language). Use awk to handle complex task such as calculation, database handling, report creation etc.

cd — The cd sets the working directory of a process.

chmod — Chmod is a utility that changes the permission of a file.

chown — Chown is a utility that is also used to change file ownership.

cp — The cp command is used to copy files.

date — An essential command to set the date and time. Also a useful way to output current information when working in a script file.

df — The df command reports filesystem disk space usage. With no arguments, 'df' reports the space used and available on all currently mounted filesystems (of all types). Otherwise, 'df' reports on the filesystem containing each argument file.

pwd — To know the current working directory

ln — The ln command makes new, alternate file names for a file by hard linking, letting multiple users share one file. The ln command creates pseudonyms for files which allows them to be accessed by different names. These pseudonyms are called links. There are two different forms of the command and two different kinds of links that can be created.

ls — The ls command shows information about files. It lists the contents of a directory in order to determine when the configurations files were last edited.

man — Short for "manual," man displays information about commands and a keyword search mechanism for needed commands.

passwd A quick and easy way to change passwords on a system.

Shutdown Shutdown is a command that turns off the computer and can be combined with variables such as -h for halt or -r for reboot.

top Top provides an ongoing look at processor activity in real time. It displays a listing of the most CPU-intensive tasks on the system, and can provide an interactive interface for manipulating processes.

vmstat The vmstat command is used to get a snapshot of everything in a system, helping admins determine whether the bottleneck is CPU, memory or I/O. Run this command to get virtual memory statistics. vmstat reports information about processes, memory, paging, block IO, traps, and cpu activity.

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.

8) What are various features of Linux based operating system? List them.

.....

.....

.....

.....

9) How Ubuntu is different from Windows operating system?

.....

.....

.....

.....

1.5 SUMMARY

ICT is changing all most all aspects of our daily life and lifestyle. If we just see lot of computation and communication is happening around us, either when we check the examinations result on mobile or when we withdraw money from the banks ATM. The influences of ICT revolution are also felt in our Library system. In this unit, we introduced you to the computer hardware technology, how it works and what it is. The peripherals devices like RFID and Barcode reader; those are particularly used in libraries are also discussed. In addition, the fundamentals of Ubuntu- Linux based operating systems have been covered. We have given few basic steps, which will be useful for a learner during the installation of Ubuntu operating system. Further this unit explained about the file system of Ubuntu and few commands and utilities, which will be useful for working on this operating system.

1.6 ANSWERS TO SELF CHECK EXERCISES

1) The Arithmetic Logic Unit (ALU) and the Control Unit (CU) together are termed as the Central Processing Unit (CPU). The CPU is the most important component

of a computer's hardware. The ALU performs the arithmetic operations such as addition, subtraction, multiplication and division, and the logical operations. The control unit interprets instructions and produces the respective control signals.

2) One kilobyte stands for 2^{10} bytes which 1024 bytes so 2 kilobytes will be 2048.

3) Inkjet printers use small cartridges full of different colour inks. They squirt a tiny drop of ink onto the paper using a bubble or pressure to form a dot. All the dots are layered on top of each other to form the desired colour.

4) The important difference between a LED reader and a pen or laser scanner is that the LED reader is measuring emitted ambient light from the bar code whereas pen or laser scanners are measuring reflected light of a specific frequency originating from the scanner itself.

5) RFID technology has gradually begun to replace the conventional barcodes on library items. The RFID tag can contain bibliographic data of a particular book, which replaces the standard barcode reader. It may be used to provide an innovative and easier way for inventory management as well. It can also act as a security device, taking the place of the more traditional electromagnetic security strip. Apart from the books, membership cards could be fitted with an RFID tag.

6) The Basic Input Output System (BIOS) is software stored on a small memory chip on the motherboard. BIOS instructs the computer on how to perform a number of basic functions such as booting and keyboard control. It is also used to identify and configure the hardware in a computer such as the hard drive, optical drive, CPU, memory, etc.

7) CDs and DVDs are optical discs that are used to store data. Both are similar in composition and usage, however DVDs offer more data storage capacity compared to CDs. CDs are commonly used for audio and program files, while DVDs are used for video and program files.

8) Most of the Linux based operating system has the following given features:

- **Low Cost/Free:** Linux and much of its software come with the GNU General Public License and hence it is free and open source.
- **Stability:** Linux has high stability compared with other operating systems. There is no need to reboot the Linux system to maintain performance levels.
- **Performance:** Linux provides high performance on various networks. It has the ability to handle large number of users simultaneously.
- **Networking:** Linux provides a strong support for network functionality; client and server systems can be easily set up on any computer running Linux. It can perform tasks like network backup faster than other operating systems.
- **Flexibility:** Linux is very flexible and can be used for high performance server applications, desktop applications, and embedded systems. You can install only the needed components for a particular use. You can also restrict the use of specific computers.
- **Compatibility:** It runs all common Unix software packages and can process all common file formats.

- **Fast and Easy Installation:** Linux distributions come with user-friendly installation.
- **Better use of Hard Disk:** Linux uses its resources well enough even when the hard disk is almost full.
- **Multitasking:** Linux is a multitasking operating system. It can handle many things at the same time.
- **Open Source:** Linux is an Open source operating systems. You can easily get the source code for Linux and edit it to develop your personal operating system.

9) The most noticeable difference is licensing and distribution terms of Ubuntu operating systems and Microsoft Windows. Ubuntu is open software and it's completely "free software" free means the freedom to run, use, modify, redistribute copies, and release your improvements to the public. In addition to this it includes many of the software's used for everyday computing at no cost, unlike Windows.

1.7 KEYWORDS

ALU : Abbreviation of **a**rithmetic **l**ogic **u**nit, is one component of the CPU (central processing unit) that performs all arithmetic computations, such as addition and multiplication, and all comparison operations.

Barcode : The machine-readable representation of the Universal Production Code (UPC). Bar codes are read by a scanner that passes over the code and registers the UPC. The width of each black line and the subsequent white space between each line coincides with the numbers of the UPC.

Bit : Short for **bi**nary digi**t**, the smallest unit of information on a machine. The term was first used in 1946 by John Tukey. A single bit can hold only one of two values: 0 or 1.

Byte : Abbreviation for binary term, a unit of storage capable of holding a single character. A byte is equal to 8 bits.

CPU : CPU is the abbreviation for **c**entral **p**rocessing **u**nit. Sometimes referred to as the central processor or simply processor, is the brains of the computer where most calculations take place. In terms of computing power, the CPU is the most important element of a computer system.

CU : Short for **c**ontrol **u**nit, it is a typical component of the CPU that implements the microprocessor instruction set. It extracts instructions from

memory and decodes and executes them, and sends the necessary signals to the ALU to perform the operation needed.

GRUB : Short for GNU GRand Unified Bootloader is a boot loader package from the GNU Project which provides a user the choice to boot one of multiple operating systems installed on a computer or select a specific kernel configuration available on a particular operating system's partitions.

RFID : Short for **r**adio **f**requency **id**entification, a technology similar in theory to bar code identification. An RFID system consists of an antenna and a transceiver, which read the radio frequency and transfer the information to a processing device, and a transponder, or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted. RFID systems can be used where a unique identification system is needed.

1.8 REFERENCES AND FURTHER READING

Basandra, Suresh K. *Computer Today*. New Delhi: Galgotia Publication, 2003. Print

Leon, Alexis and Leon, Mathews. *Fundamentals of Information Technology*. New Delhi: Leon TechWorld publication, 1999. Print

Long, Larry. *Computer Fundamental*. New Delhi: Wiley Dreamtech Publication, 2004. Print

Saxena, Sanjay. *MS-Office for Everyone*. New Delhi, Vikas Publication House, 2001. Print

Websites:

http://www.ubuntuforums.org/

http://www.ubuntulinux.org/

UNIT 2 BASICS OF COMMUNICATION TECHNOLOGY

Structure

2.0 OBJECTIVES

After going through this Unit, you will be able to:

- understand the concept of Data Transmission terminology;
- differentiate between Serial and Parallel communication;
- differentiate between Analog and Digital Data Transmission;
- know different types of transmission modes;
- compare the different Transmission Media and their characteristics;
- explain the characteristics and working of devices used for data communication; and
- understand communication protocols/standards and realise its importance.

2.1 INTRODUCTION

We all are familiar with the term "Communication", its meaning is contextual and can be interpreted by different words. In general sense we can say the process of sharing ideas, information, and messages with others at a particular time and place is communication. Communication is a vital part of personal life and is also important in business, education, and any other situation where people encounter each other. Communication between two people is an outgrowth of methods developed over

centuries of expression. Gestures, the development of language, and the necessity to engage in joint action all play a part. Communication, as we see it today, has evolved a long way. In this unit we will discuss the primitive modes of computer communication used for data transfer in networks and Internet. Also, this unit will cover the devices used for computer communication. All communication between devices requires that the devices agree on the format of the data. The set of rules defining a format is known as a protocol. In the end of this unit we have briefly given the details of communication protocols/standards used for data transfer between computers particularly for Internet.

2.2 ANALOG AND DIGITAL COMMUNICATION

Communication from a source to a destination, that is, from one computer to another or from one device to another, involves the transfer of information from the sender to the receiver. The transfer of data from one machine to another machine such that, the sender and the receiver both interpret the data correctly is known as Data Communication. Broadly the data communication can be divided into two types Analog and Digital. As you may know that signals carry the data for communication, hence this classification of Analog and Digital is based on the signals which are used for data transfer.

2.2.1 Analog Signal

We mostly use analog signals in our day-to-day life. Whatever we are talking meaning voice signals, Radio and TV broadcasting signals, Electricity signals, Sunlight or other lights signals, all are nothing but examples of Analog signal. We can say Analog signals are Nature-Signals.

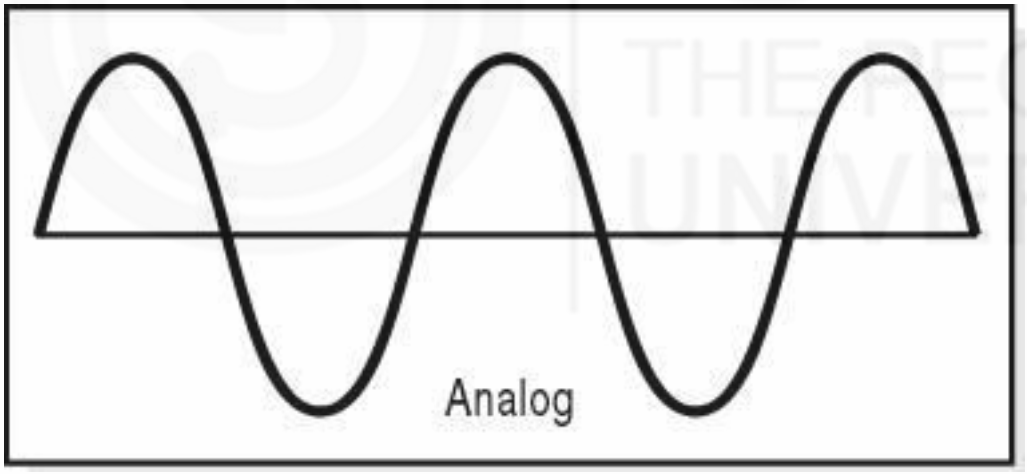

Fig. 2.1: Analog Signal

Technically, Analog signals vary constantly in one or more values; these changes in values can be used to represent data as depicted in the figure 2.1. An analog signal is continuous and can be represented by using sine waves. Human voice generates an analog (continuously varying) signal containing multiple frequencies that is transmitted as an analog signal over the medium.

It is important to note the limitations of analog signals. We know that signals are propagated with the energy and it get weaker with the distance therefore, in long distance communication like telephones, radio and TV communication we use a device named "Amplifiers". Amplifiers are used to overcome the attenuation that the signal suffers on its way. However, amplifiers amplify noise along with the original signal and hence, if the signal gets distorted, it cannot be reconstructed and it is a permanent loss. Due to this

reason, this type of transmission is not used where a high level of accuracy is needed. This is used in telephony where a slight distortion in human communication does not matter.

The ability to capture the slight nature of the real world is the single advantage of analog techniques. However, once captured, modern electronic equipment, no matter how advanced, cannot copy analog signals perfectly. By converting analog signals into digital, the original audio or video data can be preserved indefinitely within the specified error bounds and copied over and over without deterioration. Once continuously varying analog signals are measured and converted into digital form, they can be stored and transmitted without loss of integrity due to the accuracy of digital methods.

2.2.2 Digital Data Transmission

Digital data transmission describes any system based on discontinuous data or events. Computers are digital machines because at their most basic level they can distinguish between just two values, 0 and 1, or off and on, or high and low voltage as depicted in figure 2. There is no simple way to represent all the values in between, such as 0.25. All data that a computer processes must be encoded digitally, as a series of zeroes and ones.

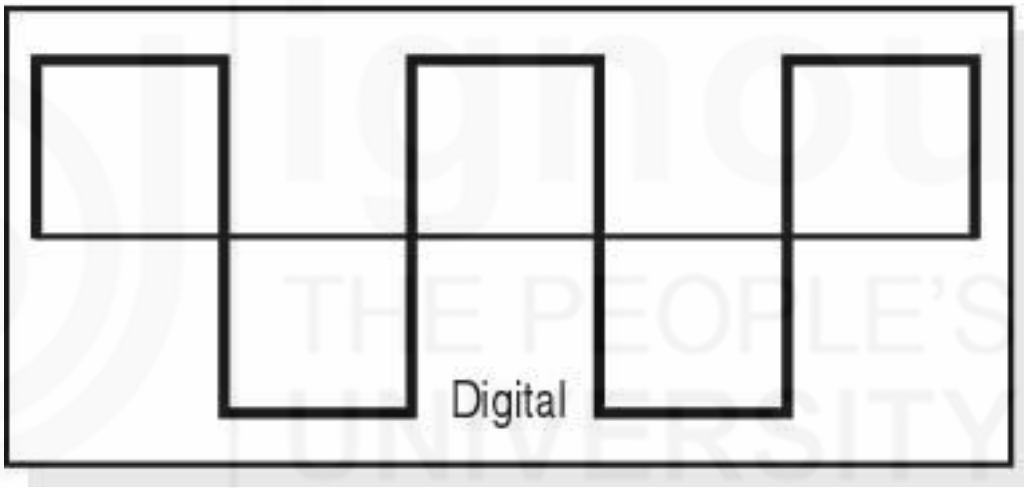

Fig. 2.2: Digital Signal

Information coming out of the computer is in the form of digital signals. The bandwidth of a digital signal is infinite as compared to any medium, which has a limited bandwidth. Therefore, as the signal is generated and enters the medium, at that point of entry, only limited frequencies are permissible on the medium and this depends upon the bandwidth. As the signal traverses over the medium it gets distorted and beyond a certain distance, the signal becomes unrecognizable from the original one. A hardware device called Repeater is used to regenerate the digital signal. The repeater measures the signal values at regular intervals to recognise the 0's and 1's in the signal and regenerates them. Hence, there is no loss of information. The number of repeaters to be used depends on the distance between the source and the destination. Any line with repeaters placed at appropriate distance is called a digital line.

When information, music, voice and video are turned into binary digital form, they can be electronically manipulated, preserved and regenerated perfectly at high speed. The millionth copy of a computer file is exactly the same as the original. This is, nevertheless, a major advantage of digital processing.

2.3 DATA COMMUNICATION MODES

Data can be transmitted from Source to Destination in a number of ways. The different modes of data transmission are outlined as follows:

- Asynchronous, Synchronous and Isochronous Communication.
- Simplex, Half Duplex and Full Duplex Communication.

2.3.1 Asynchronous, Synchronous and Isochronous Communication

When we communicate to each other, what is a basic fundamental principle? It is synchronisation of both persons, means when I am talking to you, you should listen to me and once I complete my words then you should deliver your speech otherwise we both will not be able to communicate. The same principle applies to computer or device communication and perhaps it is very important for computers are not intelligent enough to handle the cross talks. The three mechanisms used for synchronisation are Asynchronous, Synchronous and Isochronous Communication.

Asynchronous Communication

Asynchronous communication sends individual characters one at a time framed by a start bit and 1 or 2 stop bits. Each frame begins with a start bit that enables the receiving device to adjust to the timing of the transmitted signal. The message can begin at any time. Here, messages are kept as short as possible because, the sending and receiving devices should not draft out of synchronisation, when the message is being transferred. Asynchronous communication is most frequently used to transmit character data and is ideally suited for characters that are transmitted at irregular intervals, such as, when users are typing in character data from the keyboard.

Fig. 2.3: A Typical Frame Used to Transmit a Character

A typical frame used to transmit a character data has four components as shown in figure 2.3. Start bit is used to signals the starting a frame and enables the receiving device to synchronise itself with the message. Data Bits consists of 7 or 8 bits when character data is being transmitted. Parity Bit is an optionally used as a crude method for detecting transmission errors. Stop bit or bits signals the end of the data frame. You must be curious to know about Parity Bit. Error detection in asynchronous transmission makes use of the parity bit. Parity techniques can detect errors that affect only one bit and if two or more bits are affected by errors, the parity techniques may not be able to detect them. Asynchronous transmission is simple, inexpensive and is ideally suited for transmitting small frames at irregular intervals (e.g., typing from a keyboard). As each individual character is complete in itself, if a character is corrupted during transmission, its successor and predecessor will not be affected.

We would like to tell you that this type of transmission is not suitable for transferring large amounts of data or Audio and Video. Do you want to know, why? As we have discussed above that start, stop and parity bits need to be added to each character that is to be transmitted. This adds a high overhead to transmission and wastes the bandwidth; as a result, asynchronous transmission is undesirable for transmitting large amounts of data. Successful transmission inevitably depends on the recognition of the start bits.

These bits can be easily missed or occasionally spurious, as start bits can be generated by line interference, the transmission may be unsuccessful. Due to the effects of distortion the speed of asynchronous transmission is limited. If asynchronous transmission has these problems, then what are the alternatives do we have? Let us discuss this.

Synchronous Communication

An alternative way to transfer large data is, instead of sending single character or few bit we can send a group or block of data at once, and this methods is called synchronous communication.

Here, transmission begins at a predetermined regular time instant. A synchronous signal is used to tell the receiving station that a new frame is arriving and to synchronise the receiving station. In simple language you can say it is something like we inform to our friend that at particular time you will send some books, so be at home at that time to receive books. This information is nothing but a "synchronous signal". It is important to note that in computer communication Synchronous signals can be sent along with the message therefore, it generally utilises a bit pattern that cannot appear elsewhere in the messages, ensuring that they will always be distinct and easy for the receiver to recognise. As the transmitter and receiver remain in synchronisation for the duration of the transmission, frames can be of longer length.

As frames are longer the parity method of error detection is not suitable because, if multiple bits are affected, then, the parity technique will not report error accurately. Hence, the technique used with synchronous transmission is the Cyclic Redundancy Check (CRC). The transmitter uses an algorithm to calculate a CRC value that summarises the entire value of data bits. This CRC value is appended to the data frame. The receiver uses the same algorithm, recalculates the CRC and compares the CRC in the frame to the value that it has calculated. If these values match then, it is sure that the frame was transmitted without error.

An end bit pattern indicates the end of the frame. Like sync the bit pattern for end is such that, it will not appear elsewhere in the messages, ensuring that they will always be distinct and easy for the receiver to recognise at the end of the frame.

Synchronous transmission is more efficient because, only 4 additional bytes (for start and end frames) are required to transmit upto 64 k bits. Synchronous transmission is not really prone to distortion; as a result, it can be used at high speeds. However, even with these advantages synchronous transmission has some other limitations, first it is expensive as complex circuitry is required and it is difficult to implement. If an error occurs during transmission, rather than just a single character the whole block of data is lost. The sender cannot transmit characters simply, as they occur, but has to store them until it has built up a block. Thus, this is not suitable where characters are generated at irregular intervals.

Isochronous Communication

This is another alternative mechanism for data transmission, which combines the approaches of asynchronous and synchronous communications. As in the asynchronous method, each character has both the start and stop bits. The idle period (where no transmission takes place) between the two characters is not random but an exact multiple of one character time interval. If, the time to transmit a character (including its parity, start, stop bits) is **t**, the time interval between characters cannot be random as in the asynchronous method. It is also not 0 as in the synchronous method. It has to be t, 2t, 3t……nt , where n is any positive integer. Here, the signal is expected to be received

within certain delay bounds say Tmin to Tmax. Isochronous transmission guarantees transmission rates, and it is almost deterministic. It has low overheads and high speed. However, in isochronous transmission it is necessary to ensure that the clocking device is fault tolerant.

2.3.2 Simplex, Half Duplex and Full Duplex Communication

Based on "what point of time" sender or receiver can transfer the data, and what is a role of sender or receiver in the data communication; we have classified data transmission into three categories Simplex, Half Duplex and Full Duplex.

Simplex

This is one of the simplest techniques for data communication, in which we have one permanent sender and permanent receiver. In Simplex transmission, at any point of time one of the communicating devices can only send data, whereas the other can only receive it. Can you think about some example around?

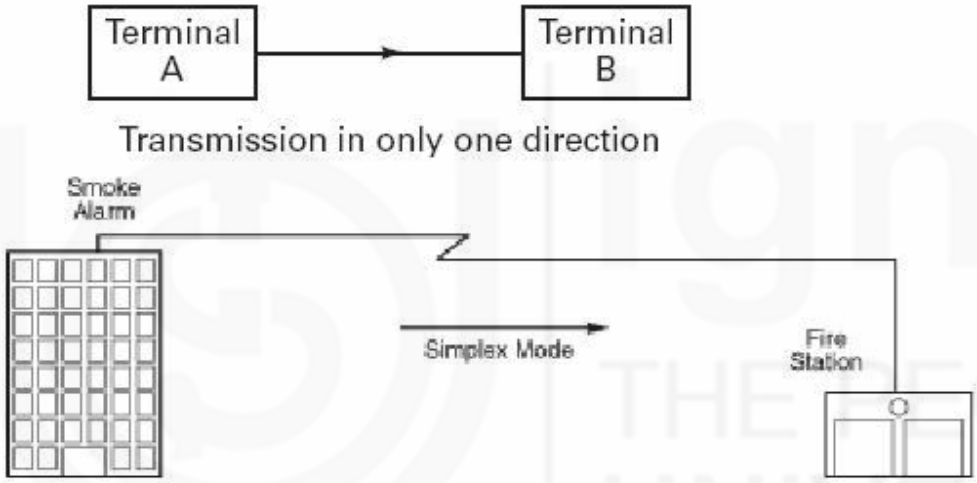

Fig. 2.4: Simplex Communication

It is like Sun, which permanently send light to us; it is also used in Broadcasting TV and Radio signals where, you can receive data from stations but can't transmit data back. These signals are unidirectional, where one party is the transmitter and the other is the receiver as shown in the Figure 2.4, where smoke alarm is shown which is connected with fire station, it is also an example of unidirectional communication. This type of channel design is easy and inexpensive to set up.

Half Duplex

As we know data communication is more about exchanging and sharing data, which may not be fulfilled by the simplex communication. Now, let's take an example where, communication is from both ways but at any point of time it is not simultaneous. This type of two-way communication where, only one party can transmit data at a time is called Half Duplex. Unlike, the Simplex mode here, both devices can transmit data though, not at the same time. Half duplex provides Simplex communication in both directions in a single channel as shown in figure 2.5, with an example of walky-talky communication.

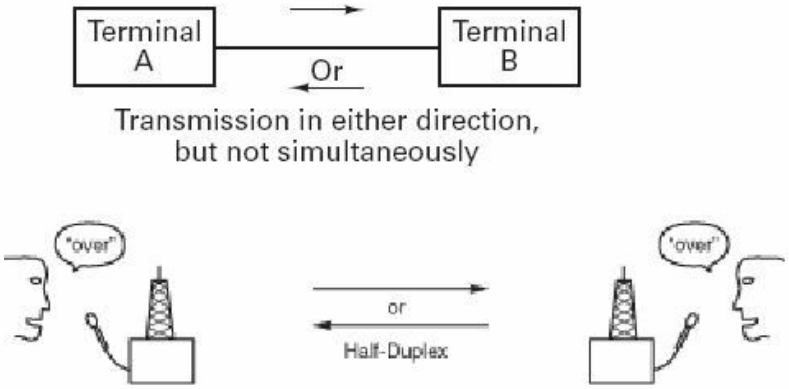

Fig. 2.5: Half Duplex Connection

When one device is sending data, the other device must only receive it and vice versa. Thus, both sides take turns at sending data. This requires a definite turnaround time during which, the device changes from the receiving mode to the transmitting mode. Due to this delay, half duplex communication is slower than simplex communication. However, it is more convenient than simplex communication as both the devices can send and receive data.

The difference between simplex and half-duplex refers to two-way communication where, only one party can transmit data at a time. Simplex refers to one-way communication where, one party is the transmitter and the other is the receiver. For example, a walkie-talkie is a half-duplex device because only one party can talk at a time. Let's try to establish an analogy with our real world regarding this communication mechanism. We can say that the half-duplex communication is something like rail tracks, where at one point of time only one train will pass through track. It can be used for both coming and going but not together.

Full Duplex

As the half duplex communication inherit the delay in data communication. Another mechanism of data communication mechanism is full duplex, refers to the transmission of data in two directions simultaneously. Here, both the devices are capable of sending as well as receiving data at the same time. As you can see from figure 2.6, that simultaneously bi-directional communication is possible, as a result, this configuration requires full and independent transmitting and receiving capabilities at both ends of the communication channel, one of its important examples is our network communication and Internet.

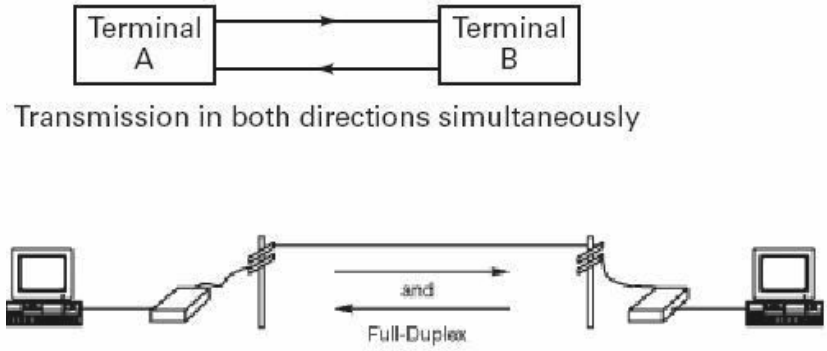

Fig. 2.6: Full Duplex Connection

Sharing the same channel and moving signals in both directions increases the channel throughput without increasing its bandwidth. For example, a telephone is a full-duplex device because both parties can talk to each other simultaneously. In contrast, a walkie-talkie is a half-duplex device because only one party can transmit at a time. It can also be view as bi-directional Road tracks. Most modems have a switch that lets you choose between full-duplex and half-duplex modes. The choice depends on which communications program you are running.

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) What is Digital Communication? How it is better than Analog Communication?

.....

.....

.....

.....

2) Bring out the difference between Synchronous, Asynchronous and Isochronous transmission.

.....

.....

.....

.....

2.4 COMMUNICATION HARDWARE

A smallest computer network should comprise minimum of at least two computers (sender and receiver), communication channel that connect the sender and receiver to each other, a network interface device on each computer which is also known as NIC, some intermediate communication devices like Switch, which is used to switch the data from one point to another, In this section we will cover all the hardware components used for designing a computer network.

2.4.1 Communication Channels

One of the most common ways to transport data from one computer to another is to write them onto magnetic tape or floppy disks, physically transport the tape or disks to the destination machine, and read them back in again. While, this method is not practical, imagine the data communication delay, cost require to transportation of data between countries and continents. Normally, Cable is the medium through which information usually moves from one network device to another. There are several types of cable, which are commonly used with LANs. In some cases, a network will utilize only one type of cable; other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size, these concepts of networks you will study in the next Unit. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

Twisted Pair

Twisted pair cable comes in two varieties: unshielded twisted pair and shielded twisted pair. Unshielded twisted pair (UTP) is the most popular and is generally the best option for small networks UTP cables contain four twisted-pairs (Orange, green, Blue & Brown) as shown in the figure 2.7, enclosed in a common sheath.

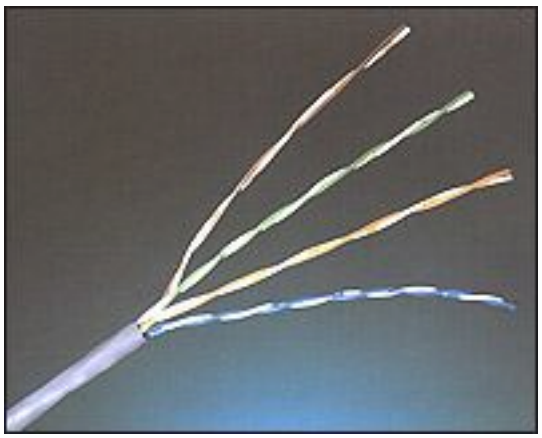

Fig. 2.7: Unshielded Twisted Pair Cable

The most common application of the twisted pair is in the telephone system. A twisted pair connects nearly all telephones to the telephone company office. Twisted pairs can run several kilometers without amplification, but for longer distances, repeaters are needed. Twisted pairs can be used for either analog or digital transmission. The bandwidth depends on the thickness of the wire and the distance traveled. A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

Coaxial Cable

Another common transmission medium is the coaxial cable. It has better shielding than twisted pairs, so it can span longer distances at higher speeds. A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often, as a closely woven braided mesh. The outer conductor is covered with a protective plastic sheath. A cutaway view of a coaxial cable is shown in figure 2.8.

Fig. 2.8: Coaxial Cable

The construction and shielding of the coaxial cable gives it a good combination of high bandwidth and excellent noise immunity. The bandwidth possible depends on the cable length. For 1-km cables, a data rate of 1 to 2 Gbps is feasible. Longer cables can also be used, but only at lower data rates or with periodic amplifiers. Coaxial cables used to be widely used within the telephone system but have now largely been replaced by fiber optics on long-haul routes. Coax is still widely used for cable television and some local area networks.Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are:

Thick coaxial: Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals.

Thin coaxial: Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals.

Optical Fiber

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials as depicted below in figure 2.9. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

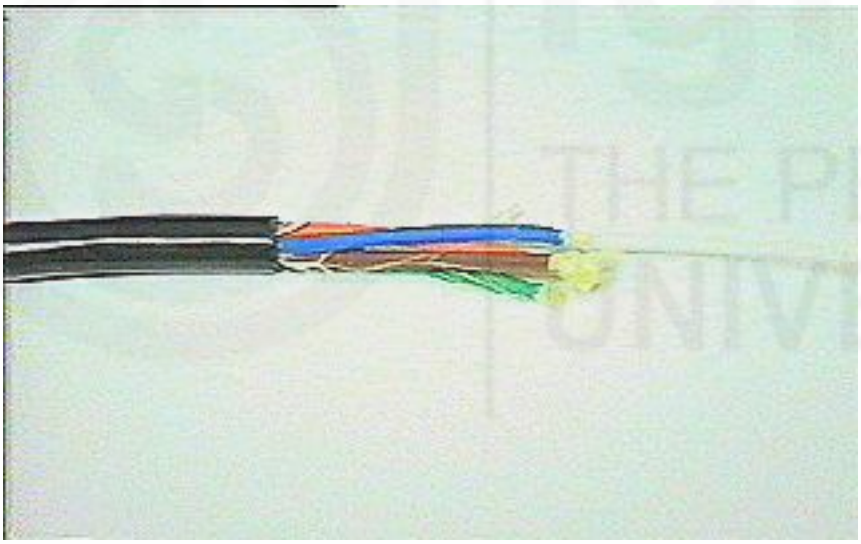

Fig. 2.9: Optical Fiber

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

2.4.2 Communication Devices

As discussed in previous section there are several communication devices used in data communication. In the sender and receiver computers, we should have Network Interface Card and Modem (which we have already studied in the Unit Basics of Computer Technology) before connected to the Internet connection. There are many

other devices being used at different levels and in different types of networks, those are explained in this section.

Network Interface Card (NIC)

A NIC is also known as a network card as shown in figure 2.10. It connects the computer to the cabling, which in turn links all of the computers on the network together as shown in figure. Each computer on a network must have a network card. Most modern network cards are 10/100 NICs and can operate at either 10 Mbps or 100 Mbps. It access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

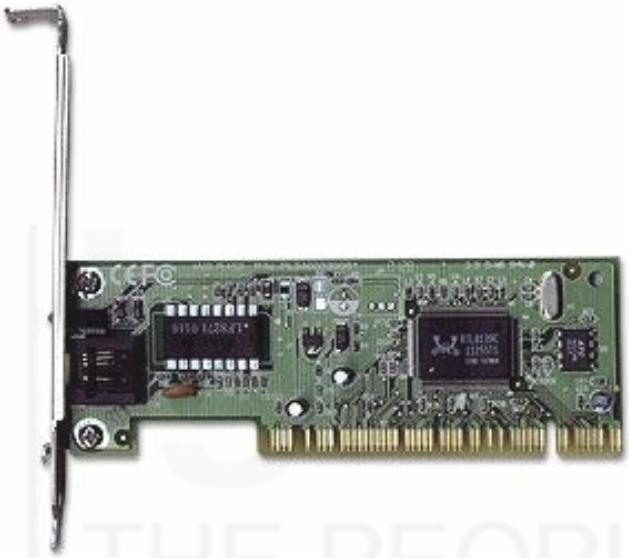

Fig. 2.10: A Network Interface Card (NIC)

Repeater

A **repeater** is an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances without degradation, an example is shown in the figure 2.11.

Fig. 2.11: Examples of Repeater

Hub

A hub is a device used to connect a PC to the network. The function of a hub is to direct information around the network, facilitating communication between all connected devices, means A hub contains multiple ports as shown in figure 2.12, which is used to connect devices in a star topology. When a packet arrives at one port, it is copied to all the ports of the hub.

Fig. 2.12: Example of Hub

Hubs can improve performance, especially for bursty traffic and large file transfers, it also enables optimum performance of computers. However, total bandwidth remains fixed; as network traffic grows, performance suffers and it does not reduce collisions.

Switch

A switch is a data-link layer network device that forwards frames using MAC addresses in the header of frames. A common type of switch is shown in the figure 13. It is used to improve network performance by segmenting the network and creating separate collision domains. It can also reduce competition for bandwidth.

Fig. 2.13: Switch

During new installations switches should be used instead of hubs as they are more effective and provide better performance. A switch, which is often, termed a 'smart hub'. Switches and hubs are technologies or 'boxes' to which computers, printers, and other networking devices are connected. Switches are the more recent technology and the accepted way of building today's networks. With switching, each connection gets "dedicated bandwidth" and can operate at full speed. In contrast, a hub shares bandwidth across multiple connections such that activity from one PC or server can slow down the effective speed of other connections on the hub. It Supports VLAN's (virtual local area network (VLAN) is a logical grouping of hosts on one or more LANs that allows communication to occur between hosts as if they were on the same physical LAN.

Howver, switches are not as good as a router in limiting Broadcasts, also for handling Multicast packets needs quite a bit of configuration & proper designing.

Bridges

The main network device found at the data link layer is a bridge, mainly used for connecting two network or local area networks. This device works at a higher layer than the repeater and therefore is a more complex device. It has some understanding of the data it receives and can make a decision based on the frames it receives as to whether it needs to let the information pass, or can remove the information from the network. This means that the amount of traffic on the medium can be reduced and therefore, the usable bandwidth can be increased. Bridges are store and forward devices to provide error detection; a common type of bridge is shown in the figure 2.14.

Fig. 2.14: A Common Bridge

Routers

Router is a device which is use to create an internetworking in our WANs and LANs. The main purpose of router is routing, which means taking a packet from one device and sending it through the network to another device on a different network. Packet is often a confusion term; it is nothing but the unit of data at any layer of the protocol stack, prior to, or after transmission.

A packet normally contains Data Type, Packet Count, Recipient's IP address, Sender's IP address, and Data. Actually routers need to transfer the data from source machine to destination machine but other information in packets it need during its transportation process. A common type of router is shown in the figure 2.15.

Fig. 2.15: A Common Router with its Front and Back View

Router has nothing to care about the host machine; it need to care about networks and the best path to each network. The logical network address of the destination host is used to get packets to a network through a routed network, and then the hardware address of the host is used to deliver the packet from a router to the correct destination host.

2.5 COMMUNICATION PROTOCOLS/STANDARD

Before going through the origin of the Internet, let us examine what is communication. **Communication** is a process of sharing ideas, information, and messages with others at a particular time and place. Communication is a vital part of personal life and is also important in business, education, and any other situation where people encounter each other. Communication between two people is an outgrowth of methods developed over centuries of expression. Gestures, the development of language, and the necessity to engage in joint action all play a part. Communication, as we see it today, has evolved a long way. We will discuss the primitive modes of communication briefly.

2.5.1 Communication Systems

Early societies developed systems for sending simple messages or signals that could be seen or heard over a short distance, such as drumbeats, fire and smoke signals, or lantern beacons. Messages were attached to the legs of carrier pigeons that were released to fly home. Further,

The postal system are being developed to transfer written documents to destinations around the world. Even after implementing different electronic communication mediums, postal system is still one of the popular communication systems available. The first truly electronic medium for communication was developed first in the form of telegraph, which sent and received electrical signals over long-distance wires. After telegraph the most important invention is telephone systems use to transmitting human speech. The telephone network has also provided the electronic network for new computer-based systems like the Internet facsimile transmissions, and the World Wide Web.

The development of computer networks was started when computers became faster, more-powerful and smaller. In the 1960's the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defence, along with researchers working on military projects at research centres and universities across the country, developed a network called the ARPANET, for sharing data and processing time of uniform computer connection over specially equipped telephone lines and satellite links. The network was designed to survive the attack or destruction of some of its parts and continue to work. Soon, however, scientists using the ARPANET realised that they could send and receive messages as well as data and programs over the network.

Today, the Internet is the widely known computer network. It uses interconnection of computer system by both wired and wireless. Smaller networks of computers, called Local Area Networks (LANs), can be installed, in a single building or for a whole organisation. Wide Area Networks (WANs) can be used to span a large geographical area. LANs and WANs use telephone lines, computer cables, and microwave and laser beams to carry digital information around a smaller area, such as a single college campus. Internet can carry any digital signals, including video images, sounds, graphics, animations, and text, therefore it has became very popular communication tool.

Need of Internet

The main reason is that each computer network is designed with a specific purpose. For example, LAN is used to connect computers in a smaller area, and it provides fast communication. As a result, networks become specialised identify. In many cases, these networks do not use the same hardware and software technology. It means that, a computer can communicate with the computers attached to the same network, because they are inter-compatible. As more and more organisations had multiple computer networks, this became a major issue. As a result, the concept of internetworking (internet)

came into being. This means that there should be a network of all physically separate networks.

Need of Protocols/Standards

All methods of communication described above follow a protocol. Protocol is nothing but a convention or standard. To signify that "Everything is ok and the train can start by a green flag is also a protocol. When we write a letter we follow a protocol. If we look at them carefully, we will find that protocols normally have hidden layers. A good example is human conversation over the phone which can be used as an analogy for communication using computers.

Assume that X and Y, want to have conversation over the telephone about a cricket match. We call this an idea. Assume that each person is taking down what other has to say. Thus, the conversation takes place in the form of several messages. A message is a block of sentence. It could also consist of one world such as OK, yes denoting a positive **acknowledgement** (ACK). It could also mean a **negative acknowledgement** (NAK) or a request to repeat such as come again, pardon me. All this happens both ways.

At the level of idea, X and Y feel that they are discussing a cricket match. However, in reality, the conversation consists of a number of messages.

A message could be too long. It may not be wise for X to speak for half an hour, only to receive a request to repeat. It is therefore necessary to send/receive acknowledgements after each sentence like 'ok', 'come again' etc. A sentence is analogous to a packet in computer world. The sender X will not speak until s/he hears some form of acknowledgement, or will repeat the sentence if s/he receives a negative acknowledgement. An alternative is timeout strategy. The speaker speaks a sentence and waits for some time for any acknowledgement. If s/he does not hear anything, s/he repeats the sentence.

Apart from this **error control** we take care of **flow control**. Flow control refers to the speed mismatch between the listener and speaker. If the speaker speaks too fast, the listener will say go-slow. In computer world, if the receiving computer is not fast enough, and cannot hold any more data, it requests the sender to wait or control the transfer by slowdown.

Therefore, in computer communication, both speaker and listener should agree on the communication language/syntax, scheme of acknowledgement, during flow control, machine error control mechanism, etc. Thus, we can say that the conversation is governed by some set of rules known to both the parties. This set of rules is called protocol and it necessary for disciplined manner of conversation/communication.

2.5.2 TCP/IP Layers and Protocols

To provide the set of rules and standardization among the different computer networks, the International Standards Organization (ISO) in 1984 defined the Open System Interconnection (OSI) model. OSI model is a set of protocols that attempt to define and standardize the data communications process; we can say that it is a concept that describes how data communications should take place. The OSI model has the support of most major computer and network vendors, many large customers, and most governments in different countries. The following are the seven layers of the Open System Interconnection (OSI) reference model, depicted in the figure 2.16:

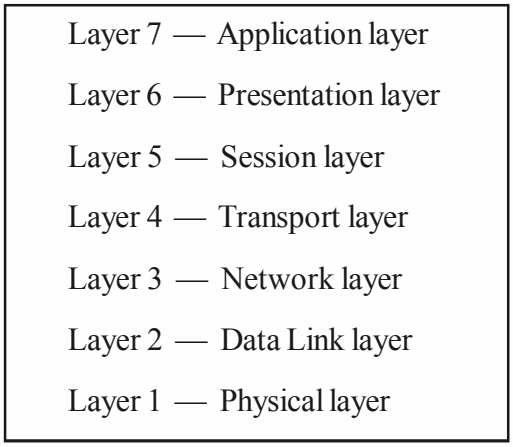

Fig. 2.16: OSI Layers

The OSI model is modular. Each successive layer of the OSI model works with the one above and below it. Although, each layer of the OSI model provides its own set of functions, it is possible to group the layers into two distinct categories. The first four layers i.e., physical, data link, network, and transport layer provide the end-to-end services necessary for the transfer of data between two systems. These layers provide the protocols associated with the communications network used to link two computers together. Together, these are communication oriented. The top three layers i.e., the application, presentation, and session layers provide the application services required for the exchange of information. That is, they allow two applications, each running on a different node of the network to interact with each other through the services provided by their respective operating systems. Together, these are data processing oriented.

Though OSI model is very important for data communication but multiple layers slow down the communication process. Practically OSI was never fully implemented; to provide robustness and better efficiency another but similar model was implemented named as TCP/IP model (its named was given because of its two most important protocols in it). The TCP/IP model is made up of four layers: interface layer, network, transport, and application. The first layer of TCP/IP (Application layer) is similar to the first three layers (Application, presentation and Session layer) of the OSI model. The services of transport layers of both the models are similar. Further, the services of network layers in both models are also similar, while some time network layer is also known as Internet layer. The last layer of TCP/IP is interface layer, which includes the services of data link layer and physical layer of OSI model. In OSI model, each layer takes the services of the lower layer. Whereas the layers of TCP/IP protocol suite contain relatively independent protocols as shown in figure 2.17.

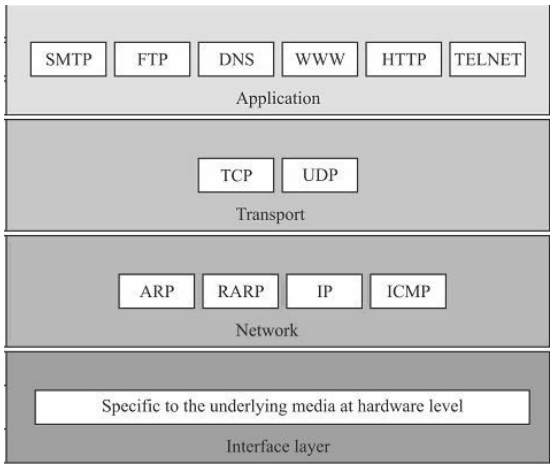

Fig. 2.17: TCP/IP and its Protocols

Layers of TCP/IP Protocol Suite

As we know TCP/IP contains four layers and each layer has its specific functions, in the following section lets find out the functions of each layer of TCP/IP.

Interface layer or (Physical + Data Link Layer)

The physical layer deals with the hardware level like, transmission media, connections and the voltage for digital signals. The data link layer deals with media access and control strategies, frame format etc.

Internet Layer or Network Layer

The Internet layer is an important layer in the protocol suite. At this layer, TCP/IP supports Internetworking Protocol (IP). IP is a host-to-host protocol. This layer is responsible for the format of datagrams as defined by IP, and routing a datagram or packet to the next hop, but is not responsible for the accurate and timely delivery of datagrams to the destination in proper sequence. IP allows raw transmission functions allowing user to add functionalities necessary for given application. Ensuring maximum efficiency, TCP/IP supports four other protocols: ARP, RARP, ICMP and IGMP in this layer.

1) **Address Resolution Protocol (ARP)**

On a LAN, each machine is identified with a unique physical address imprinted on the network interface card. ARP is used to find the physical address of a machine when its IP address is known.

2) **Reverse Address Resolution Protocol (RARP)**

It is used to find the IP address of a machine when its physical address is known. It is used when a diskless computer is booted or a computer is connected to the network for the first time.

3) **Internet Control Message Protocol (ICMP)**

IP is unreliable are best effort delivery. In case of failures ICMP is used to send notifications to the sender about packet problems. It sends error and query messages.

4) **Internet Group Message Protocol (IGMP)**

It is used for multicasting, which is transmission of a single message to a group of recipients.

Transport Layer

At this layer, TCP/IP supports two protocols: TCP, UDP, IP is host-to-host protocol, which can deliver the packet from one physical device to another physical device. TCP, UDP, are transport level protocols, responsible for delivering a packet from one process on a device to another process on the other device.

1) **User Datagram Protocol (UDP)**

It is simpler of the two protocols. It does not provide reliability. It is, therefore faster, and using for applications in which delay is intolerable (in case of audio and video).

2) **Transmission Control Protocol (TCP)**

TCP is reliable, connection-oriented protocol. By connection oriented, we mean that a connection must be established between both ends before either can transmit data. It ensures that communication is error-free and in sequence.

Application Layer

As said earlier, it is closer to combined session, presentation, and application layer of OSI model. It allows the user to run various applications on Internet. These applications are File Transfer Protocol (FTP), remote login (TELNET), email (SMTP), WWW (HTTP). The session layer of OSI model is almost dropped in TCP/IP. Whenever we work on the Internet we use most of these protocols. For example when use are surfing or browsing the Internet websites actually you are using WWW.

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.

3) Write any three important advantages of Optical fibers.

.....

.....

.....

.....

4) Differentiate between Switches and hubs.

.....

.....

.....

.....

2.6 SUMMARY

In this unit, we have studied the basic concepts of Data Transmission. As it is essential to know how data can be transmitted from the source to the destination, the different types of transmission were discussed like Asynchronous, Synchronous and Isochronous communication. Further we have explained different modes like Simplex, Half duplex and full duplex communication. How the network are designed and for this are the different components are required, to explain it we have discussed the characteristics and working of various communication channels and devices in this unit. Towards the end, we have focused about the communication protocols and standards used for communication in the networks and Internet.

2.7 ANSWERS TO SELF CHECK EXERCISES

1) Digital communication is information transmitted electronically and is encoded digitally. Digital signals are signals that are represented by binary numbers, "1" or "0". It is stored and processed by computers. The main difference between analog and digital signals is that an analogue signal is continuous and a digital signal is discrete. Analog technologies record waveforms as they are, while digital technologies convert analog signals into numbers. Digital communication systems offer much more efficiency, better performance, and much greater flexibility than analog.

2) Asynchronous communication sends individual characters one at a time framed by a start bit and 1 or 2 stop bits. Transfer of large data sent in a group or block at once instead of sending single character or few bit at a time is known as synchronous communication. Isochronous communication combines both approaches.

3) Three advantages of Optical fibre are: a) since it transfer light instead of electronic signal, it eliminates electrical interference, b) it is able to transmit signals over much longer distance compared to coaxial or twisted pair cable, and c) cost is much lower compared to copper cabling.

4) A hub is a device used to connect a PC to the network whereas a switch is a data link layer network device.

2.8 KEYWORDS

Coaxial Cable : A type of electric cable that is used to send telegraph, telephone, and television signals.

MAC Addresses : A media access control address is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet.

Open System Interconnection (OSI) Reference Model : A set of seven layers that define the different stages that data must go through to travel from one device to another over a network. OSI model is a set of protocols that attempt to define and standardize the data communications process.

Shielded Twisted Pair (STP) : Cable construction that includes an external grounded shield as well as twisting on a regular basis to help minimize noise interferences.

Unshielded Twisted Pair (UTP) : Copper wiring used in small-to-large networks to connect host devices to hubs and switches.

2.9 REFERENCES/FURTHER READING

Tenenbaum, Andrew S. *Computer Networks*. PHI: New Delhi, 2006. Print

Stalling, William. *Data and Computer Communication*. PHI: New Delhi, 2007. Print

Godbole, Achyut S. *Web Technoligies*. New Delhi: TATA McGrawHill, 2009. Print

Forouzan, Berhouz. *TCP/IP Protocol Suite*. New Delhi: TATA McGraw Hill, 2003. Print

Websites:

http://compnetworking.about.com/lr/

http://en.wikipedia.org/w/index.php

http://www.cisco.com

http://www.tcpipguide.com

UNIT 3 BASICS OF NETWORK TECHNOLOGY

Structure

3.0 OBJECTIVES

After going through this Unit, you will be able to:

- explain the concept of computer networks;
- understand different application of networks;
- differentiate between different types of computer networks based on size, connection and functioning;
- compare the different network topologies used in LAN and WAN;
- understand the working of LAN access methods;
- explain the working of networking devices used in WAN;
- know the importance of using networked system; and
- understand the concept of wireless technologies and standards.

3.1 INTRODUCTION

With the ICT revolution the functioning of organisations has changed drastically. In a networked scenario organisations often need several people (may be at different locations) to input and process data simultaneously. In order to achieve this, a computer-networking model in which a number of separate but interconnected computers do the job has replaced the earlier standalone-computing model. By linking individual computers over

a network their productivity has been increased enormously. A most distinguishing characteristic of a general computer network is that data can enter or leave at any point and can be processed at any workstation. In this unit you will be learning about the basic concepts regarding Computer Networks. Here, you will learn about different types of Networks, their applications, and various network topologies used in LAN and WAN. Also, the networking devices and access methods in LAN and WAN will be discussed. At the end of the Unit we will discuss the wireless communication technologies and standards (Wi-Fi and WiMAX) used in wireless communications.

3.2 NETWORK CONCEPT AND CLASSIFICATION

As we have seen in the last unit that a computer network consists of two or more computers that are linked (connected) together to share resources, application, allow communication. In Fig. 3.1 a networked environment is illustrated. The Computers on a network may be linked through cables, telephones lines or wireless points.

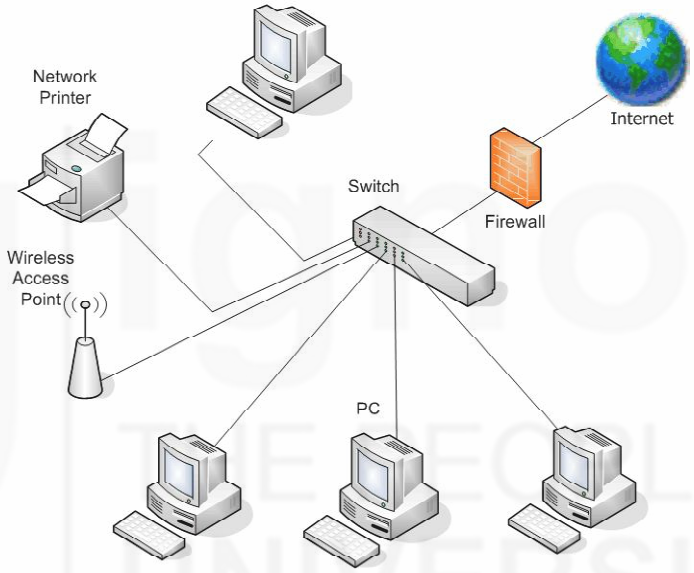

Fig. 3.1: A Simple Computer Network

A Computer network includes the network operating system in the client and server machines, the cables, which connect different computers and all supporting hardware in between such as bridges, routers and switches. In wireless systems, antennas and towers are also part of the network. As you can see in Figure 3.1, between Internet and network a firewall is depicted which provides the security to the network.

3.2.1 Advantages of Networks

Computers in a networked environment provide numerous advantages when compared to computers in a stand-alone environment. The immense benefits that the computer networks provide are in the form of excellent sharing of computational resources, computational load, increased level of reliability, economy and efficient person-to-person communication. Following are some of the major advantages of using computer networks.

Sharing: The main aim of a computer network is to make all programs, equipment, and data available to anyone on the network without regard to the physical location of the resource and the user.

Reliability: Reliability is always an important requirement of all system but especially for military, banking, air traffic control, nuclear reactor safety, and many other applications,

the ability to continue operating in the face of hardware problems is of utmost importance. Computer networks provide high reliability by having alternative sources of supply. For example, all files could be replicated on two or three machines, so, if one of them is unavailable (due to hardware failure), the other copies could be used.

Saving Money: Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ten faster than personal computers but they cost much more. This imbalance has caused many systems designers to build systems consisting of personal computers, one per user, with data kept on one or more shared file server machines. In this model, the users are called clients, and the whole arrangement is called the client-server model.

Scalability: The ability to increase the system performance gradually as the workload grows just by adding more processors. With centralised mainframes, when a system is full, it must be replaced by a larger one, usually at great expense and even greater disruption to the users. With client-server model, new clients and new servers can be added when needed.

Communication Medium: A computer network can provide a powerful communication medium among widely separated users. Using a computer network it is easy for two or more people who are working on the same project and who live far apart to write a report together. When one worker, makes a change to an online document, others can see the change immediately, instead of waiting several days for a letter. This facilitates real time collaboration among far-flung groups of people which was previously impossible.

Increased Productivity: Networks increase productivity as several people can enter, share, evaluate and process data at the same time cutting down on the time. Networks facilitate handling of multiple tasks simultaneously from different locations increasing productivity and cutting down cost and time.

3.2.2 Network Classification

We see different types of networks available like mobile networks, computer networks and TV networks around us. Let us now learn about different types of computer networks available around us and try to classify them. Table 3.1 shows classification of computer networks based on size, type of connection and functional relationships.

Table 3.1: Classifications of Networks

According to the size of the Network	LAN
	MAN
	WAN
	PAN
According to the type of connection Used	Wired Network
	Wireless Network
According to the functional relationship (Network Architecture)	Peer to Peer network
	Client-Server Network

A) **Size of the Network**

According to size networks are classified as LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network) and Personal Area Network (PAN).

LAN (Local Area Network)

The network that spans a relatively small area that is, in the single building or campus is known as LAN as depicted in Fig. 3.2. For example, a library will have a wired or wireless LAN for users to interconnect local devices (e.g., printers and servers). Local area networking uses switches, bridges and/or repeaters, and hubs to interconnect LANs and increase overall size.

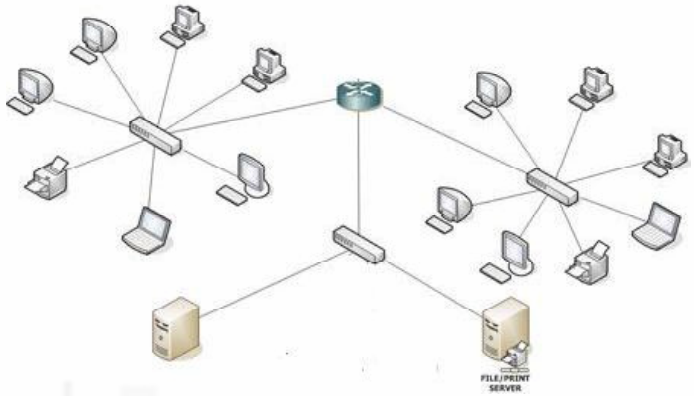

Fig. 3.2: An example of LAN

MAN (Metropolitan Area Network)

Metropolitan Area Network is a Computer network connecting two or more Local Area Networks or Campus Area Networks together but within a town or city as shown in Fig. 3.3. In terms of geographic area MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MANs are usually characterised by very high-speed connections using fiber optical cable or other digital media. MAN can range anywhere from 5 to 50km in diameter.

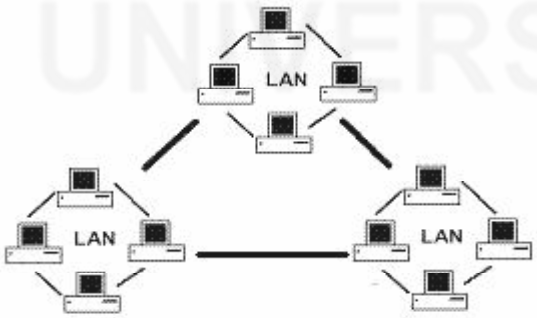

Fig. 3.3: An example of MAN

WAN (Wide Area Network)

Wide Area Network is a computer network that spans a relatively large geographical area. Typically, a WAN consists of many local-area networks (LANs), which are depicted, in Fig. 3.4. They can connect networks across cities, states or even countries. Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. They are generally connected with each other using routers. They have main characteristics like multiple interconnected LANs are used, generally more expensive technology are used for implementation.

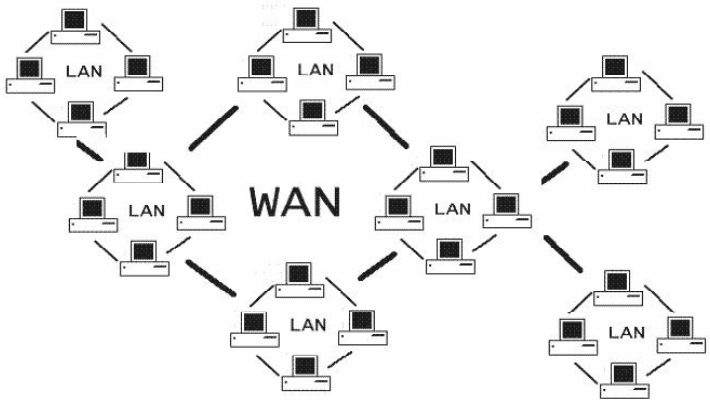

Fig. 3.4: An Example of WAN

Personal Area Network (PAN)

A personal area network (PAN) is a computer network used for communication among computer devices close to one person. Some examples of devices that may be used in a PAN are printers; fax machines, telephones, Personal Digital Assistants (PDAs) or scanners.

Fig. 3.5: An Example of PAN

The reach of a PAN is typically within about 20-30 feet (approximately 6-9 Meters) as depicted in the Figure 3.5. PANs can be used for communication among the individual devices (intrapersonal communication), or for connecting to a higher-level network and the Internet.

B) Type of Connection

According to the connection-type, networks can be classified as using wire connection or wireless connection:

- **Wired Network:** A network that connects devices using cables (wires) like Coaxial Cable, Twisted pair Cable, Optical Fiber Cable etc.
- **Wireless Network:** A network that connects devices using wireless technologies like Bluetooth, infrared, radio frequency etc.

C) Functional Relationship

Functional Relationship or Network architecture could be another important criteria to classify the networks:

Peer to peer network

Peer-to-peer networks are more commonly implemented where less than ten computers are involved and where strict security is not necessary (see Fig. 3.6). Generally, computers in this kind of network are configured to share common resources and responsibilities**.** Workgroups provide easy sharing of files, printers and other network resources.

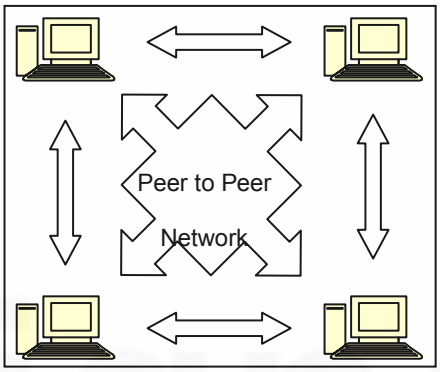

Fig. 3.6: Peer to Peer Networking

It is designed for small LANs in homes, schools, and small businesses. As the number of computers in a workgroup grows, workgroup LANs eventually become too difficult to administer and should be replaced with alternative solutions like client/server approaches.

Client-Server Network

In this architecture each computer or process on the network is either a client or a server. **Client/server networks** are more suitable for larger networks as shown in Figure 3.7. A central computer, or 'server', acts as the storage location for files and applications shared on the network. Usually the server is a higher than average performance computer. Clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

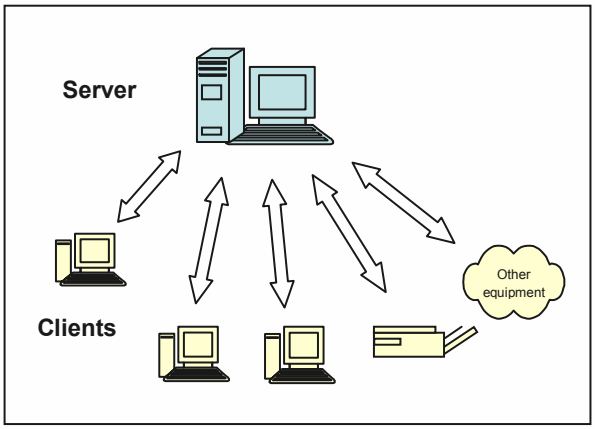

Fig. 3.7: Client - Server Networking

It provides high-level security features through server, which controls the network access of the other computers and processes.

3.3 LOCAL AREA NETWORK (LAN) OVERVIEW

As you know the computer network that spans a relatively small area that is, in the single building or campus is known as LAN, according to standard it can be in 1-kilometer radius. We have studied above the classifications of network based on different criteria. Now in this section we are going to explain about the various LAN topologies and access methods through which network computers can be arranged and configured to communicate.

3.3.1 LAN Topologies

Topology refers to the shape of a network, or the network's layout. How different nodes in a network are connected to each other and how they communicate with each other is determined by the network's topology. Topologies are either physical or logical. Some of the most common network topologies are: Bus, Star, Ring, Tree and Mesh topology. These are explained further in this section.

Bus Topology

In Bus topology, all devices are connected to a central cable, called the bus or backbone. The bus topology connects workstations using a single cable. Each workstation is connected to the next workstation in a point-to-point fashion. All workstations connect to the same cable. Fig. 3.8 shows computers connected using Bus Topology.

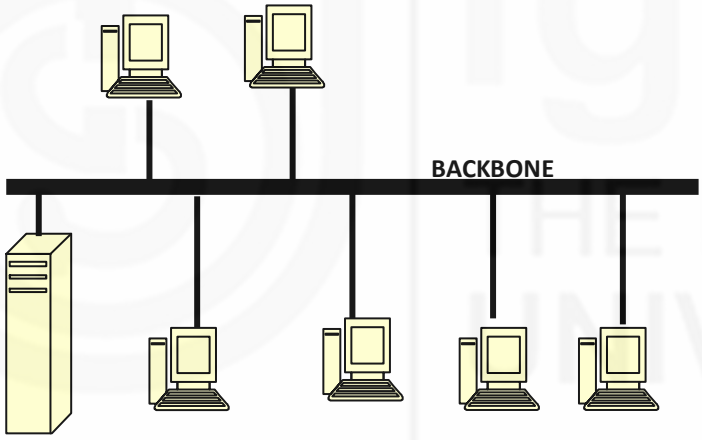

Fig. 3.8: Bus Topology

In this type of topology, if one workstation goes faulty all workstations may be affected as all workstations share the same cable for sending and receiving of information. The cabling cost of bus systems is the least of all the different topologies. Each end of the cable is terminated using a special terminator. The common implementation of this topology is Ethernet. Here, message transmitted by one workstation is heard by all the other workstations. Bus installation is simple, easy and cheap in comparison to other topologies also it requires less cable. But, this topology is used only in comparatively small networks. As all computers share the same bus, the performance of the network deteriorates when we increase the number of computers beyond a certain limit. Also, fault identification is difficult and if it occurs in the cable all transmission can be stopped.

Star topology uses a central hub through which, all components are connected. In a Star topology, the central hub is the host computer, and at the end of each connection is a terminal as shown in Fig. 3.9.

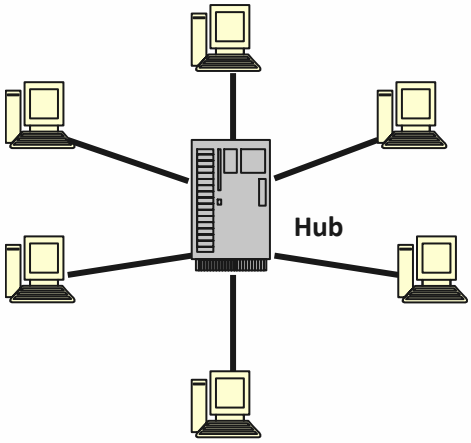

Fig. 3.9: Star Topology

Nodes communicate across the network by passing data through the hub. A star network uses a significant amount of cable as each terminal is wired back to the central hub, even if two terminals are side by side but several hundred meters away from the host. The central hub makes all routing decisions, and all other workstations can be simple.

An advantage of the star topology is that, failure in one of the terminals does not affect any other terminal; however, failure of the central hub affects all terminals. This type of topology is frequently used to connect terminals to a large time-sharing host computer. It is less expensive to mesh topology. Compared to bus topology, faults in this type of network can be easily traced. One of the main advantage of star network is that expansion and modification is easy and it can support multiple cable types like shielded twisted pair cable, unshielded twisted pair cable, ordinary telephone cable etc. However, if central hub fails it brings the entire network to a halt.

Ring Topology

In Ring Topology all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it, i.e., the ring topology connects workstations in a closed loop, which is depicted in Figure 3.10. Each terminal is connected to two other terminals (the next and the previous), with the last terminal being connected to the first. Data is transmitted around the ring in one direction only; each station passing on the data to the next station till it reaches its destination.

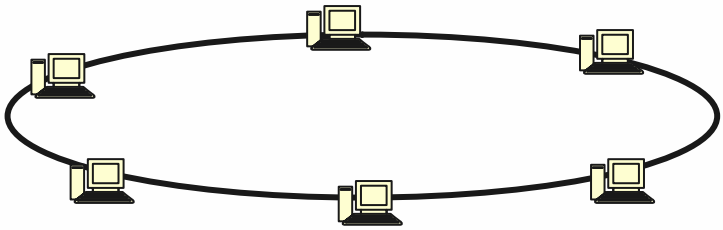

Fig. 3.10: Ring Topology

Information travels around the ring from one workstation to the next. Each packet of data sent on the ring is prefixed by the address of the station to which it is being sent. When a packet of data arrives, the workstation checks to see if the packet address is the same as its own, if it is, it grabs the data in the packet. If the packet does not belong to it, it sends the packet to the next workstation in the ring.

Faulty workstations can be isolated from the ring. When the workstation is powered on, it connects itself to the ring. When power is off, it disconnects itself from the ring

and allows the information to bypass the workstation. The common implementation of this topology is token ring. A break in the ring causes the entire network to fail. Individual workstations can be isolated from the ring. In this topology fault isolation is simplified. Unlike Bus topology, there is no signal loss in Ring topology because the tokens are data packets that are re-generated at each node. But Adding or removing computers disrupts the entire network. A break in the ring can stop the transmission in the entire network.

Tree Topology

Tree topology is a LAN topology in which only one route exists between any two nodes on the network. The pattern of connection resembles a tree in which all branches spring from one root. Figure 3.11 shows computers connected using Tree Topology.

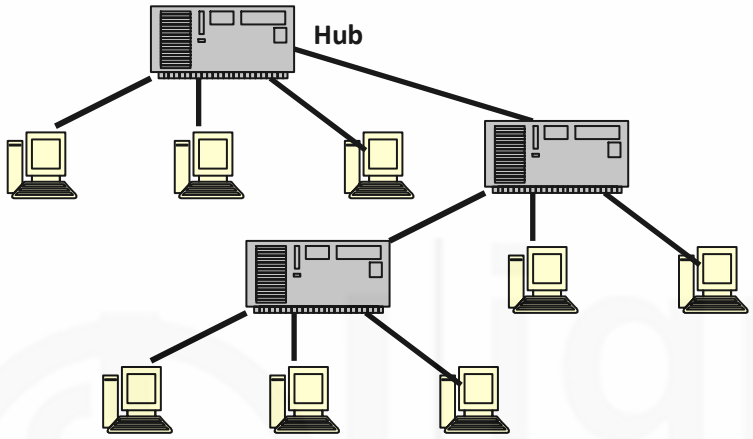

Fig. 3.11: Tree Topology

Tree topology is a hybrid topology, it is similar to the star topology but the nodes are connected to the secondary hub, which in turn is connected to the central hub. In this topology groups of star-configured networks are connected to a linear bus backbone. Similar to star topology Installation and configuration of network is easy and Supports multiple cable types like shielded twisted pair cable, unshielded twisted pair cable, ordinary telephone cable etc. However, failure in the central hub brings the entire network to a halt. Also it needs more cabling when compared to bus topology.

Mesh Topology

Devices are connected with many redundant interconnections between network nodes. In a well-connected topology, every node has a connection to every other node in the network. The cable requirements are high, but there are redundant paths built in. Failure in one of the computers does not cause the network to break down, as they have alternative paths to other computers.

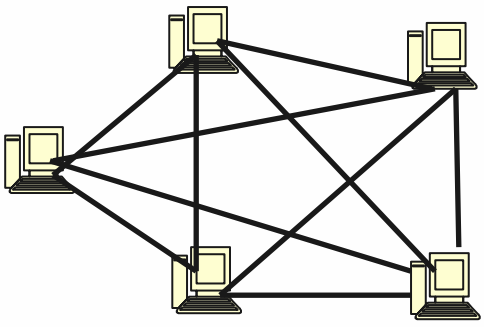

Fig. 3.12: Mesh Topology

Mesh topologies are used in critical connection of host computers (typically telephone exchanges). Alternate paths allow each computer to balance the load to other computer systems in the network by using more than one of the connection paths available. A fully connected mesh network therefore, has n (n-1)/2 physical channels to link n devices. To accommodate these, every device on the network must have (n-1) input/output ports. The main advantage of this topology is its robustness and use of dedicated links eliminates traffic and security problems. Failure in one of the computers does not affect the entire network. However, due to each dedicated cabling it requires high cost, time and I/O (input/output) ports for configuration.

3.3.2 LAN Access Methods

Access Method means how network devices will handle data transmission with one another. For data transmission in LAN, various protocols/standards are defined by IEEE (Institute of Electrical and Electronics Engineers) called IEEE 802, to enable intercommunication between equipment from a variety of manufacturers. It has set IEEE 802.3, 802.4 and 802.5 standards alternatively named as Ethernet, Token bus and Token Ring for LAN. This section will explain you about these methods and their importance in the LAN.

Ethernet

The term Ethernet refers to the family of local-area network (LAN) protocol defined by the IEEE 802.3 standard that is commonly known as the CSMA/CD protocol. Among the other technologies and protocols Ethernet is widely used in LAN-connected PCs and workstations because it is easy to understand, implement, manage, and maintain. Along with that it allows low-cost implementations and provides topological flexibility.

As you know general standard for the data link layer defined by the OSI Model. The IEEE divides this layer into two sub-layers, the logical link control (LLC) layer and the media access control (MAC) layer. IEEE 802.3 supports a LAN standard originally developed by Xerox and later extended by a joint venture between Digital Equipment Corporation, Intel Corporation and Xerox. This was called Ethernet.

IEEE 802.3 defines two types of data transmissions Broadband and Baseband. Broadband transmissions enable two or more communication channels to share the bandwidth of the transmission media. Broadband networks can simultaneously accommodate video, voice and data. Most cable modem providers use broadband communications. On the other hand, Baseband transmissions enable digital signals over a single frequency. With Baseband transmission, the entire communication channel capacity is used to transmit a single date signal. Most LAN's today use Baseband technology.

The MAC layer has two primary responsibilities first is Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception and second is Media access control, including initiation of frame transmission and recovery from transmission failure. Let's discuss MAC frame structure for IEEE 802.3 with the help of following Figure 3.13.

Preamble	Start Delimiter of frame	Destination Address	Source Address	Length of Data Field	Data	Pad	Frame Check Sum

Fig. 3.13 : Ethernet Frame Format

Each frame has seven fields explained as follows:

Preamble: The first field of 802.3 frame is 7 byte (56 bits) long with a sequence of alternate 1 and 0 i.e., 10101010. This pattern helps the receiver to synchronise and get the beginning of the frame.

Starting Delimiter (SD)/ Start-of-Frame (SOF): The second field start delimiter is 1 byte (8 bit) long. It has pattern 10101011. Again, it is to indicate the beginning of the frame and ensure that the next field will be a destination address. Address, here, can be a single address or a group address.

Destination Address (DA): This field is 6 byte (48 bit) long. It contains the physical address of the receiver.

Source Address (SA): This filed is also 6 byte (48 bit) long. It contains the physical address of the sender. These source and destination addresses are actually MAC address to uniquely identify Each Ethernet network interface card (NIC) that is assigned by the card manufacturer. Each manufacturer that complies with IEEE standards can apply to the IEEE Registration Authority for a range of numbers for its cards. Each MAC address is a 48-bit number, of which the first 24 bits identify the manufacturer. This part of the MAC address (manufacturer ID or organizational unique identifier is assigned by the registration authority. The second half of the address (extension of board ID) is assigned by the manufacturer. The number is usually programmed into the hardware so that it cannot be changed.

Length of Data Field: It is 2 byte (16 bit) long. It indicates the number of bytes in the information field. The longest allowable value can be 1518 bytes.

Data: This field size will be a minimum of 46 bytes long and a maximum of 1500 bytes as will be explained later.

Pad: This field size can be 0 to 46 bytes long. This is required if, the data size is less than 46 bytes as a 802.3 frame must be at least 64 bytes long.

Frame Checksum (FCS): This field is 4 bytes (32 bit) long. It contains information about error detection. This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames. The FCS is generated over the DA, SA, Length/Type, and Data fields. Here it is CRC-32.

Minimum and Maximum Length of Frame

Minimum frame length is 64 bytes and Maximum frame length is 1518 bytes. Minimum length or lower limit for frame length is defined for normal operation of CSMA/CD. This is required so that, the entire frame is not transmitted completely before its first bit has been received by the receiver. If, this happens then the probability of the occurrence of collision will be high (the same has been explained earlier in the previous section CSMA/CD).

Hence, Ethernet frame must be of 64 bytes long. Some of the bytes are header and trailer parts of the frame. If, we consider 6 bytes destination address, 6 bytes source address, 2 bytes length and 4 bytes FCS (6+6+2+4=18) then, the minimum length of data will be 64-18= 46 bytes. If, frame is less than 46 bytes then, padding bits fill up this difference. As per 802.3 standard, the frames maximum length or upper limit of frame is = 1518 bytes (excluding preamble and SD). If we subtract 18 bytes of header and trailer then, the maximum length will be 1500 bytes.

Frame Transmission

Whenever the end station MAC receives a transmit frame request with the associated address and data information from the LLC layer, the MAC starts the transmission sequence by transferring the LLC information into the MAC frame buffer. First, the preamble and start delimiter are inserted in the PRE and SD fields, next both destination and source addresses are inserted into the address fields. Similarly, LLC data bytes are counted, and the number of bytes is inserted into the Length/Type field. Next, the LLC data bytes are inserted into the Data field. If the number of LLC data bytes is less than 46, padding is added to bring the Data field length up to 46. An FCS value is generated over the DA, SA, Length/Type, and Data fields and is appended to the end of the Data field. After the frame is assembled, actual frame transmission will depend on whether the MAC is operating in half-duplex or full-duplex mode. The IEEE 802.3 standard currently requires that all Ethernet MACs support half-duplex operation, in which the MAC can be either transmitting or receiving a frame, but it cannot be doing both simultaneously. Full-duplex operation is an optional MAC capability that allows the MAC to transmit and receive frames simultaneously.

Token Bus

In a token passing system, a small data frame is passed from device to device across the network in pre-determined order. The device that has control of the token frame has the ability to transmit data across the network. When a device has data to send, it must wait until it has the token and then sends its data. When the data transmission is complete, the token is released so that other devices may use the network media. The main advantage of token-passing networks is that they are deterministic. In other words, it is easy to calculate the maximum time that will pass before a device has the opportunity to send data. Both IEEE 802.4 (token bus) and 802.5 (token ring) are based on this approach. However, token bus is suitable in few situations instead of token ring (token ring we will discuss in next section of this unit).

As we know LANs are implemented in a factory automation and process control situation, where the nodes are computers controlling the manufacturing process. In this type of application, real-time processing with minimum delay is needed. Processing must occur at the same speed as the objects moving along the assembly line. Ethernet is not a suitable protocol for this purpose because the number of collisions is not predictable and the delay in sending data from the control center to the computers along the assembly line is not a fixed value. Token ring is also not a suitable protocol because an assembly line resembles a bus topology and not a ring.

Token bus combines features of both Ethernet and token ring. It combines the physical configuration of bus topology and the predictable delay feature of token ring.

Token bus is a physical bus that operates as a logical ring using tokens. Stations are logically organised into a ring. When a device wants to transmit across the bus, it has to determine whether the media is in use. If no other device is transmitting, the signal is sent. Each device receives the signal and then determines whether its address matches that of the recipient. Messages that weren't addressed to the device are disregarded. When dealing with bus networks, it is important to pay careful attention to termination. Each end of the trunk cable needs to be properly terminated. Without termination the signal will bounce back down the cable causing collisions. Generally, bus topologies use coaxial cable.

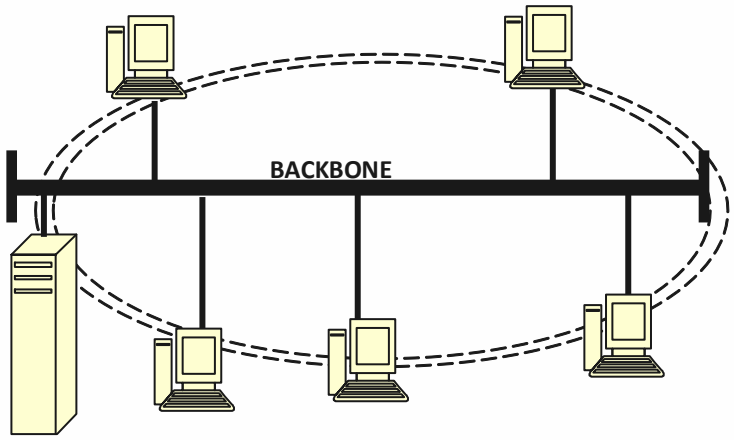

Fig. 3.14: Token Bus

Token bus is limited to factory like automation and process control and has limited commercial application in data communication. It has some other disadvantages like it lead to network performance degradation, weakened signal and difficult troubleshooting.

Token Ring

Token Ring uses a logical ring topology whereby the data is sent from one machine to the next and so on around the ring until it ends up back where it started. It also uses a token passing protocol, which means that a machine can only use the network when it has control of the Token; this ensures that there are no collisions because only one machine can use the network at any given time.

The computers on the LAN are connected so that data is passed around the network in a logical ring (see Figure 3.15). The token ring configuration calls for the computers to be wired to a central hub, where physically it might not look like a ring, but the hub is wired so that the data passes from one computer to the next in a circular motion. The computers pass a packet of data called a token around the network. Only the computer that holds the token can transmit a message on to the ring. At the start, a free Token is circulating on the ring, to use the network, a device first has to capture the free Token and replace the data with its own message. It should write its data and the recipient's address onto the Token and pass it to the next machine in the ring. Next machine that reads the address, realises it is not its own, so passes it on to another machine in the ring sequence. The same process continues till the token reaches to the intended machine.

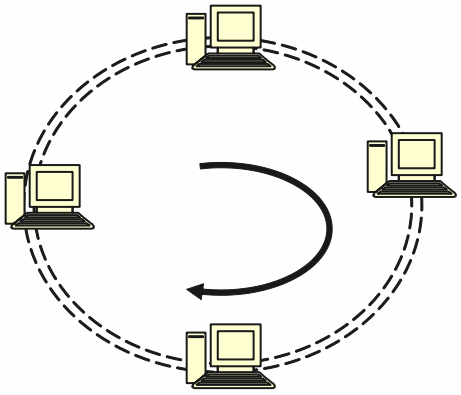

Fig. 3.15: Token Ring

The intended machine read the message and first sends the message back with an acknowledgement to say that it has received the data. This acknowledgement receipt is then sent to machine next in the ring sequence (in the same direction) who checks the address, realises that it is not it's own and so forwards it on to the next machine in the

ring, consequently it is forwarded to sender machine. Sender Machine recognises the address, reads the acknowledgement from number 4 (represented by the purple flashing screen) and then releases the free Token back on to the ring ready for the next machine to use. It is basics of Token Ring and it shows how data is sent, received and acknowledged, but Token Ring also has a built in management and recovery system that makes it very fault tolerant. Token ring is technically more sophisticated than Ethernet, and it includes a number of built-in diagnosis and correction mechanisms that can help troubleshoot network problems. Also, because data is transmitted in a more orderly fashion, token ring does not suffer as badly under heavy data traffic. Almost everything about token ring is more expensive than Ethernet by comparison he cable, the network adapter cards, and the other components as well.

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) How computer networks provides reliability and scalability? Explain.

2) What is a main limitation of peer-to-peer networking?

3) In real time processing environment Token Bus should be preferred over Token Ring. Justify the statement.

.....

.....

.....

.....

.....

.....

.....

.....

3.4 WIDE AREA NETWORK (WAN) OVERVIEW

As we know wide area network (WAN) is a network linking geographically distinct locations, which may or may not belong to the same organisation. Over the last few years the web-based applications and wireless networking have changed our outlook about computer networks. Today's corporate networks are accessible virtually anytime from anywhere, and these remote access solutions typically involve a combination of varied WAN services.

In this section we will explain the WAN connection methods, recognize the various WAN physical topologies and hardware devices used for building WANs.

3.4.1 WAN Topologies

WAN topologies use both LAN add enterprise-wide topologies as building blocks, but add more complexity because of the distance they must cover, the larger number of users they serve, and the heavy traffic they often handle. Here we will explain about the WAN topologies. These are almost similar like LAN. However, instead of single node

or machine in WAN we connect one network (which may or may not be LAN). These networks may be based on different types of technologies, connections and topologies. Also, the different network may use different types of connections to interconnect with the WAN.

Single link

As Bus topology may not be possible in case of WAN or very costly to implement WAN. We can have another technique similar to peer-to-peer connection to design WAN, where single interconnection points for each location is arranged as depicted in Figure 3.16. Each network site depends on every other site in the network to transmit and receive its traffic. However, the peer-to-peer LANs use computers with shared access to one cable, whereas the WAN peer-to-peer topology uses different locations, each one connected to another one through dedicated channel.

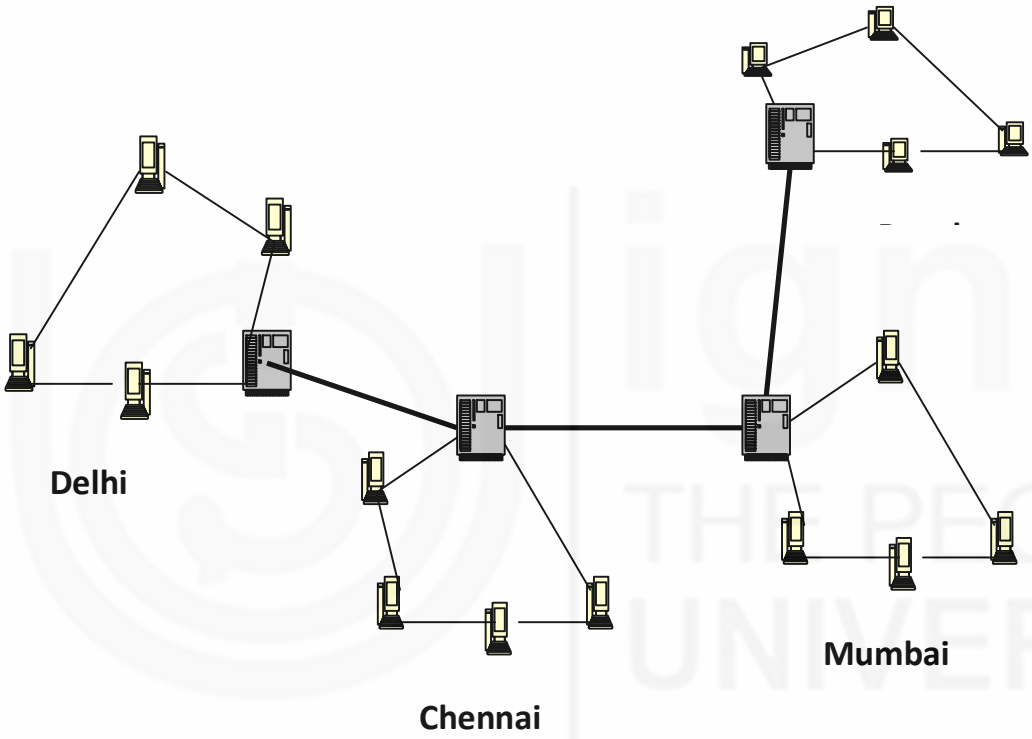

Fig. 3.16: Single Link WAN

Ring

Similar to LAN Ring topology, in WAN Ring topology, each site is connected to two other sites so that the entire WAN forms a ring pattern (see Figure 3.17), except that a ring WAN topology connects locations rather than local nodes. Unlike the Single-Link WAN, routers at any network site can redirect data to another route if one route becomes too busy, however a single cable (as in single link WAN) can break the interconnect of entire network.

Also, the single Link WAN at the time of expanding requires at least one additional link. Therefore, WANs that use the ring topology are only practical for connecting less than four or five network sites.

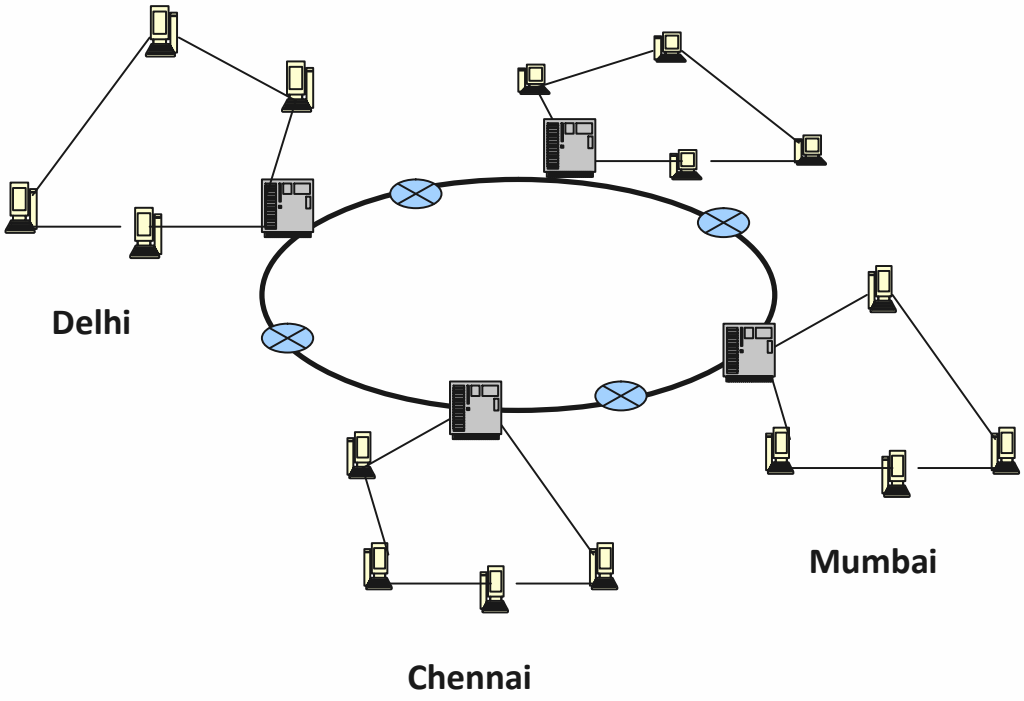

Fig. 3.17: Ring based WAN

Star

The star WAN topology also follows the arrangement of a star LAN. A single network site acts as the central connection point for several other points as shown in figure 18. This arrangement provides separate routes for data between any two sites. As a result, star WANs are more reliable than the Single link or Ring WANs. Another advantage of a star WAN is that when all of its dedicated circuits are functioning, a star WAN provides shorter data paths between any two sites.

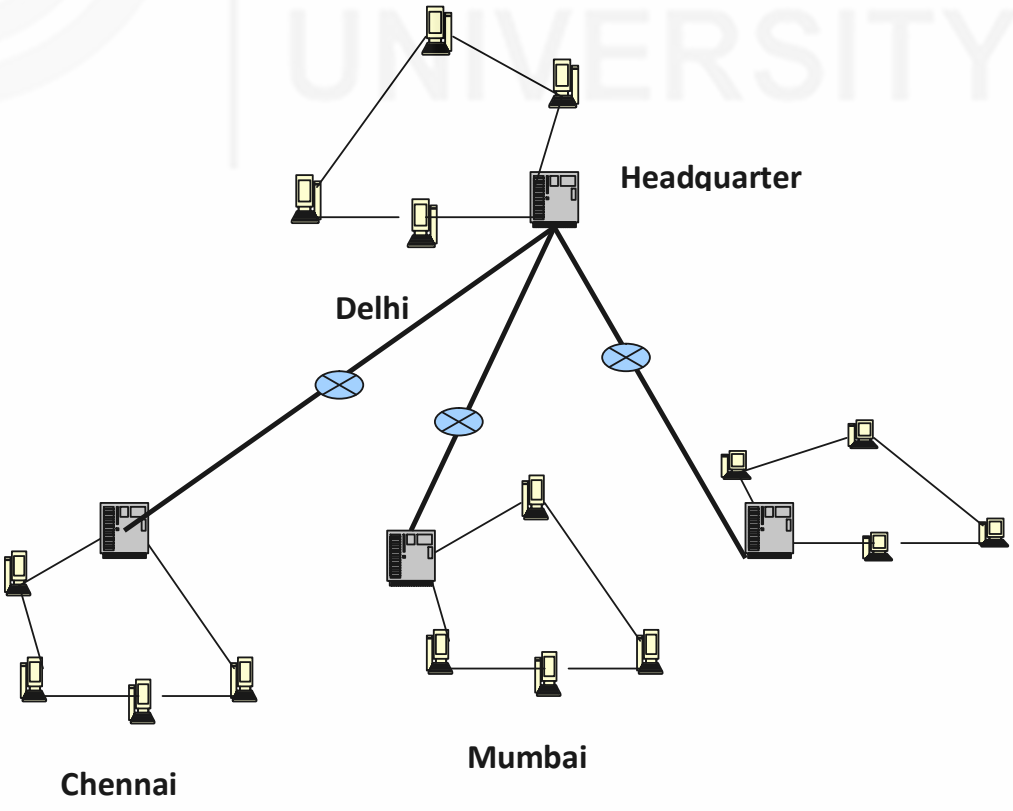

Fig. 3.18: Star WAN

Mesh

As shown in Figure 3.19, Mesh WAN topology incorporates several directly interconnected network sites. Because every site is interconnected, data can be transferred directly from its source to its destination. If one connection suffers a problem, routers can redirect data easily and quickly. One disadvantage to a mesh WAN is the implementation cost; connecting every network site on a network to every other involves leasing a large number of channels. To decrease costs, we can choose to implement a partial mesh, in which critical WAN networks are directly interconnected.

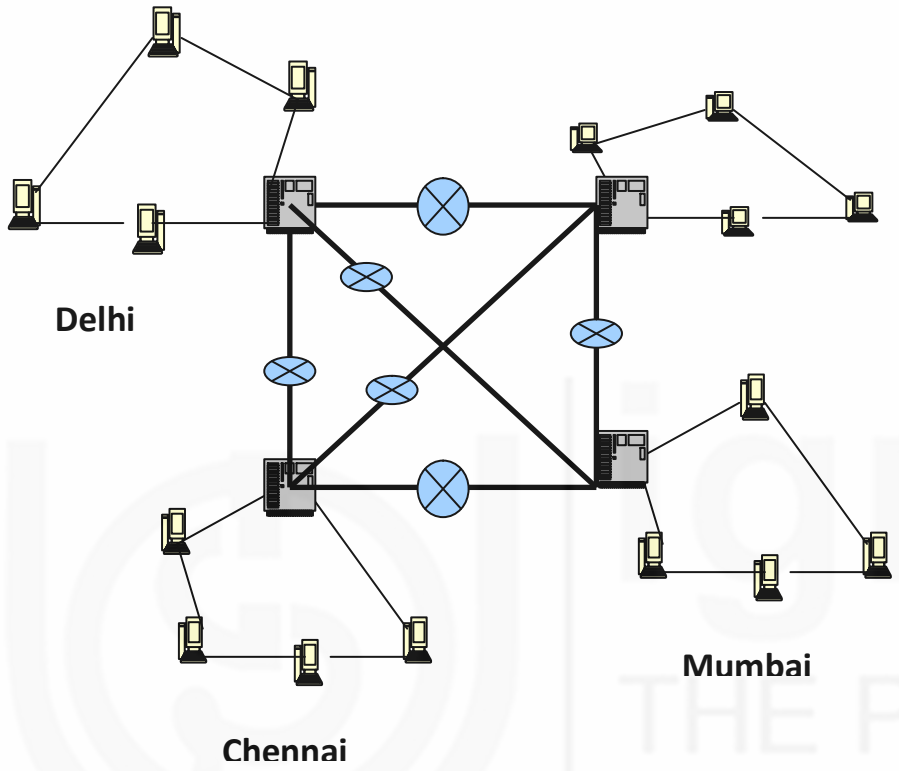

Fig. 3.19: Mesh WAN Topology

3.4.2 WAN Switching Methods

In a WAN, two computing devices are not connected directly. A network of switching nodes provides a transfer path between the two devices. The process of transferring data blocks from one node to another is called data switching. There are three switching techniques commonly employed and these are Circuit, Message and packet switching.

Circuit Switching

In circuit switching there is a dedicated communication path between the sending and receiving devices as discussed above in single link WAN. The dedicated path is a connected sequence of links between switching nodes. A conventional telephone network, where a dedicated path is set between the caller and the called party for the duration of a telephone call is an example of circuit switching. Communication in. circuit switching involves three steps-circuit establishment; data transfer; and circuit termination. Circuit switching is mainly for voice telephone network, but is not all that effective for data communication networks, as channel capacities are not fully utilised, as data communication equipments do not generate data continuously.

Message Switching

Message switching is an alternative switching technique, where it is not necessary to establish a dedicated path between the sending and receiving devices. In Message Switching, the sending device appends the destination address to the message and passes it to the network; the message is then passed through the network from one node to another till it reaches the intended destination. Each switching node receives a message, stores it briefly and then transmit it to the next node. Examples of a message are electronic mails, computer files, telegrams and transaction queries and responses. A complete exchange may consist of several messages. The basic disadvantage of message switching is the variable delay at intermediate switching nodes.

Packet Switching

Packet Switching combines the advantages of message and circuit switching. Packet Switching is functionally similar to message switching, in which data is transmitted in block, stored by the first switching node it meets in the network and is forwarded to the next and subsequent downstream nodes until it reaches the destination. The length of data block is Limited in a packet switching network. Typical maximum length of packets are between 128 bytes to 4096 bytes. There are two approaches to packet switching:

- Datagram
- Virtual circuit

In datagram approach, each packet is treated independently and may follow a different path through the network. Packets may be re-ordered, dropped or delivered in wrong sequence. The communication protocols provide the error recovery sequencing of packets at the receiving device.

In virtual circuit approach, a fixed logical path through the network from the sender to the receiver is established before any packets are sent. This path remains unchanged for the duration of the session. This is quite like circuit switching, but no resources are reserved along the path. Packets are buffered at intermediate nodes awaiting transmission.

3.4.3 WAN Devices/Hardware

The switching techniques utilise the routing technology for data transfer. Routing is responsible for searching a path between two computing devices that wish to communicate and for forwarding the data packets on this path. As we have already discussed about LAN devices like bridge and routers in the last unit, in this section briefly we have given the role of these devices in the WAN.

Bridges

Bridges are used to connect two LANs that use identical LAN protocols over a wide area as depicted in the Figure 3.20.

The bridge acts as an address filter, which picks up packets from one LAN that is intended for a destination on another LAN and passes these packets on the network. Bridges operate at the data link layer (layer 2) of the OSI model. As all devices use the same protocols, the amount of processing required at the bridge is minimal.

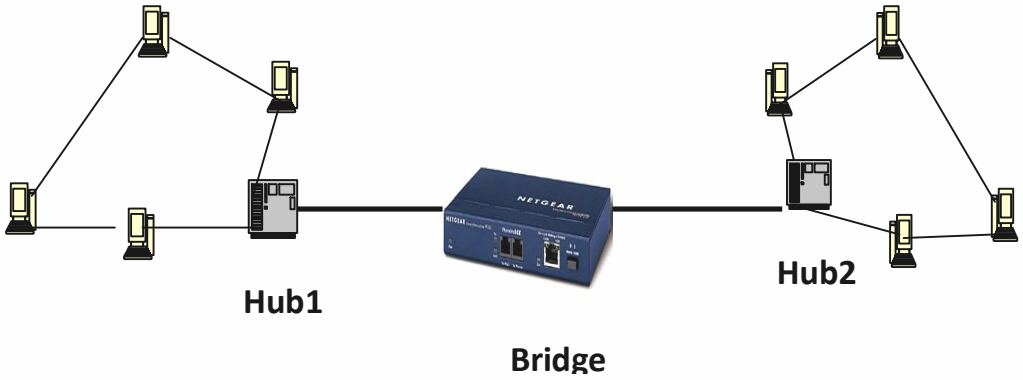

Fig. 3.20: Bridge Connectivity in a Network

If the distance between the two LANs is large, the user would require two identical bridges at either end of the communication link. Besides a point-to-point link, the intervening communication facility can be a network such as a wide area packet switching network in such cases the bridges need to add necessary header and trailer.

Routers

Routers can be used to connect networks that may not be similar. Routers provide connectivity between two LANs or two WANs over large geographical distances as shown in the Figure 3.21. Routers operate at the network layer 3 of the OSI model. All routers participate in a routing protocol to access the network, topology, and based on this information routers compute the best route from a sender to the receiver.

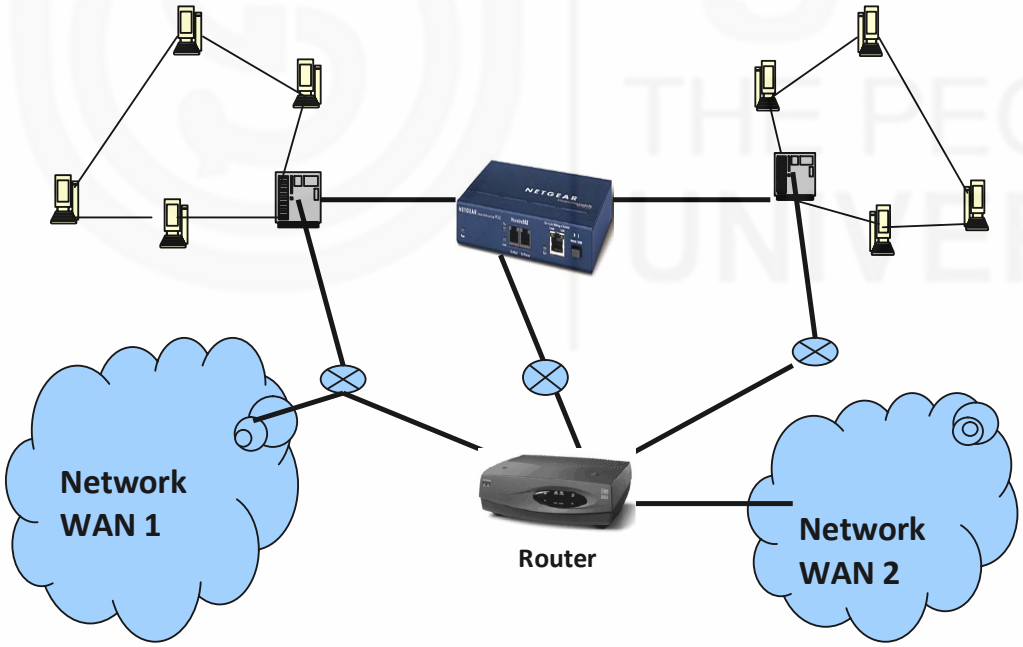

Fig. 3.21: Router Connectivity in a Network

For large Wide Area Networks spanning thousands of kilometers, the normal practice is to put network routers at suitable locations to minimize link costs for leased lines and provide adequate reliability from link failures. Networks and other system are then connected to the nearest router.

Gateways

Gateways are used to connect two dissimilar LANs as given the following Figure 3.22. The term gateways and routers are used interchangeably, though there is a subtle difference

between the two. A router operates at the network layer (layer 3) of the OSI model, whereas a gateway operates on the application layer 7 of the OSI model. A gateway is required to convert data packets from one protocol format to another before forwarding it as it connects two dissimilar networks.

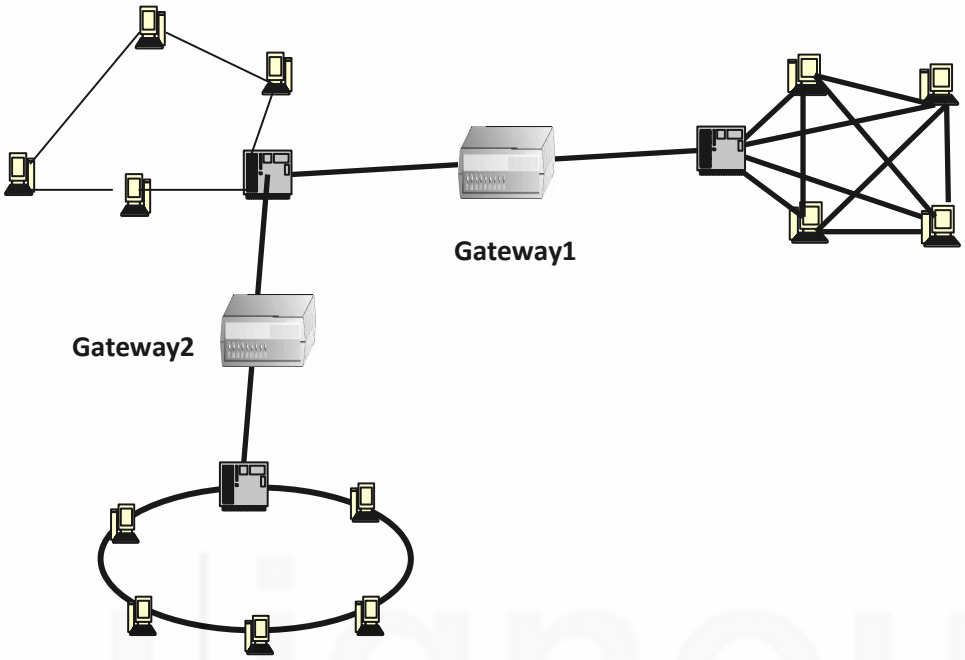

Fig. 3.22: Gateway Connectivity in a Network

3.5 WIRELESS TECHNOLOGY

As we know wireless transmission means where data transmission happen without wires. Here, there are no physical connectors between the two communicating devices. It is highly useful in difficult geographical areas (mountains, jungles, swamps, air, sea, etc.) where building wired networks and fixed devices is very difficult or not possible. In wireless transmission data is sent through the atmosphere or air. The three main types of Wireless Media are Radio, Microwave, and Infrared as explained below:

- The radio portion of the electromagnetic spectrum extends from 10 KHz to 1GHz. Within this range there are numerous bands or ranges of frequencies that are designated for specific purposes.
- Microwave is a radio system, which uses very high frequencies to send and receive data. Because of the high frequencies involved, microwave stations are located about 30 kilometres apart and in line of sight (visible to each other).
- Unguided infrared and millimetre waves are widely used for short-range communication. The remote controls used on televisions, stereos etc. all use infrared communication.

Wireless technologies represent a rapidly emerging area of growth and importance for providing wireless networking. Wireless networks are a system of portable computers that communicate using radio transmission. Nowadays everyone wants an uninterrupted omnipresent network access from everywhere and every time. There is interest in creating mobile computing labs utilizing laptop computers equipped with wireless Ethernet cards. Recently, wireless industry has made important progress in resolving some restraints to the widespread acceptance of wireless technologies. Some of the constraints have included disparate standards, low bandwidth, and high infrastructure and service cost. Wireless technologies can both support the institution mission and provide cost-effective

solutions. Wireless is being adopted for many new applications: to connect computers, to allow remote monitoring and data acquisition, to provide access control and security, and to provide a solution for environments where wires may not be the best solution.

Wireless networks are usually configured with the base stations strategically placed around the networking site. Optical fiber cable can be used to cable all base stations together. The transmission power of the base stations and portables must be properly adjusted, so that wireless access is omnipresent to the users. Here unlike the cellular telephone system, each cell has only one channel that covers the entire bandwidth, which is available. Typically its bandwidth is 1 to 2 Mbps.

3.5.1 Wi-Fi

Wi-Fi is a trademark of the Wi-Fi Alliance for certified products based on the IEEE 802.11 standards. It is often suggested that Wi-Fi means Wireless Fidelity (compared with the long-established audio recording term High Fidelity or Hi-Fi.). However, officially the term Wi-Fi does not mean anything.

This certification warrants interoperability between different wireless devices. Actually, when wireless networking technology first entered the market, due to lack of standardization interoperability problem arose between different products from different vendors, consequently IEEE 802.11 standards were developed to guide the vendors. But it is important to note that not every IEEE 802.11 compliant device is certified by the Wi-Fi Alliance, which may be because of certification costs that must be paid for each certified device type. Also, that the lack of the Wi-Fi logo does not imply that a WLAN-device is incompatible to certified Wi-Fi devices.

Wi-Fi Enabled Devices

Nowadays we see that most of the personal computer operating systems, many game consoles, laptops, smart phones, printers, and other peripherals support Wi-Fi. Many consumer devices use Wi-Fi. Amongst others, personal computers can network to each other and connect to the Internet, mobile computers can connect to the Internet from any Wi-Fi hotspot, and digital cameras can transfer images wirelessly.

In addition to restricted use in homes and offices, Wi-Fi can make access publicly available at Wi-Fi hotspots provided either free of charge or to subscribers to various providers. Organizations and businesses such as airports, hotels and restaurants often provide free hotspots to attract or assist clients. Wi-Fi technology is also used to set up mesh networks. Wi-Fi also allows connectivity in peer-to-peer (wireless ad-hoc network) mode, which enables devices to connect directly with each other. This connectivity mode can prove useful in consumer electronics and gaming applications. Wireless routers which incorporate modem and a Wi-Fi access point, often set up in homes and other premises, provide Internet-access and internetworking to all devices connected (wirelessly or by cable) to them.

Advantages and Limitations

In addition to resolving the implementation problems of wired networking at difficult geographical areas, wireless networks typically reduce the costs of network deployment and expansion also. You may be thinking about the wireless networking cost, but gradually it will be more economical. As you can see wireless network adapters are now built into most laptops soon it will be with other networking devices.

Wi-Fi now extensively used in corporate infrastructures. At a basic level of services most of the vendors and brands of access points and client network interfaces has

interoperability. Wi-Fi has a global set of standards some time interchanged with name of IEEE 802.11. Any standard Wi-Fi device will work anywhere in the world. One of the major concerns of wireless technology is security; to address the security requirements current version of Wi-Fi Protected Access encryption (WPA2) is considered as secure. It can defeat many security threats, provided strong passwords are used.

Another important limitations of wireless technology are slow data rate and poor quality of services. However, some new protocols for Quality of Service (WMM) make Wi-Fi more suitable for latency-sensitive applications (such as voice and video), and power saving mechanisms (WMM Power Save) improves battery operation.

3.5.2 WiMAX

The meaning of WiMAX is Worldwide Interoperability for Microwave Access, the name "WiMAX" was created by the WiMAX Forum, which was formed to promote conformity and interoperability of the standard.

It is a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile Internet access. Less data rate is major problem of wireless technology however through WiMAX we can reach up to 3 Megabits/second broadband data rate. The IEEE standard available for WiMAX is 802.16 standard. The WiMAX technology can be used for connecting different Wi-Fi hotspots to the Internet and to enable the wireless broadband access. It can also support all data and telecommunications services through portable connectivity. As it can provide broadband wireless transmission of data using a variety of transmission modes it can be highly useful in the disaster management. It is interesting to note that WiMAX is a possible replacement candidate for cellular phone technologies such as GSM and CDMA, or can be used as an overlay to increase capacity. It has also been considered as a wireless backhaul technology for 2G, 3G, and 4G networks in both developed and poor nations.

IEEE 802.16 (WiMAX)

WiMAX is a term coined to describe standard, interoperable implementations of IEEE 802.16 wireless networks, similar to the way the term Wi-Fi is used for interoperable implementations of the IEEE 802.11 Wireless LAN standard. However, WiMAX is very different from Wi-Fi in the way it works.

Data Link Layer

In Wi-Fi the media access controller (MAC) uses contention access, all subscriber stations that wish to pass data through a wireless access point (WAP) are competing for the WAP's attention on a random interrupt basis. This can cause subscriber stations distant from the WAP to be repeatedly interrupted by closer stations, greatly reducing their throughput. In contrast, the 802.16 MAC uses a scheduling algorithm for which the subscriber station needs to compete only once (for initial entry into the network). After that it is allocated an access slot by the base station. The time slot can enlarge and contract, but remains assigned to the subscriber station, which means that other subscribers cannot use it.

Physical Layer

The original version of the standard on which WiMAX is based (IEEE 802.16) specified a physical layer operations and frequency range. The operating frequency range was updated and modified afterwards in new versions to 2 to 11 GHz range. More higher

versions, including 802.16e, also provides multiple antenna support, which are expected to fetch possible benefits in terms of coverage, self installation, power consumption, frequency re-use and bandwidth efficiency.

WiMAX subscriber or client units are available in both indoor and outdoor versions from different manufacturers. Self-install indoor units are suitable, but radio losses mean that the subscriber must be significantly closer to the WiMAX base station than with professionally installed external units. Indoor units are comparable in size to a cable modem. However, outdoor units are roughly the size of a laptop PC, and their installation is comparable to the installation of a residential satellite dish.

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.

4) How Ring based WAN is better than single Link WAN?

.....

.....

.....

.....

3.6 SUMMARY

In this unit we have learned about networking concept and its utilisation. Here we discussed the different types of networks and the difference between them. We have seen the immense benefits that the computer networks provide in the form of excellent sharing of computational resources, computational load, increased level of reliability, economy and efficient person-to-person communication. Computer networks are basically classified based on size like LAN, MAN, WAN, based on connection like wired and wireless and based on functional requirements like peer-to-peer and client-server. Network topologies means ways of geographical interconnecting in networking nodes like Star, Bus, Ring, Tree, and Mesh topologies, these topologies are discussed for LAN and WAN. The access methods, techniques and networking devices used for developing LAN and WAN are also discussed. In the last of this unit wireless technology is discussed briefly with its two important standards Wi-Fi and WiMAX .

3.7 ANSWERS TO SELF CHECK EXERCISES

1) Computer networks provide high reliability by having alternative sources of supply. For example, all files could be replicated on two or three machines, so, if one of them is unavailable (due to hardware failure), the other copies could be used. Scalability can be achieved by increasing the system performance gradually as the workload grows just by adding more processors. With centralised mainframes, when a system is full, it must be replaced by a larger one, usually at great expense and even greater disruption to the users. With client-server model, new clients and new servers can be added when needed.

2) Peer to peer network is designed for small LANs in homes, schools, and small businesses. As the number of computers in a workgroup grows, workgroup LANs eventually become too difficult to administer and should be replaced with alternative solutions like client/server approaches.

3) Token bus combines features of both Ethernet and token ring. It combines the physical configuration of bus topology and the predictable delay feature of token ring. LANs are implemented in a factory automation and process control situation, where the nodes are computers controlling the manufacturing process. In this type of application, real-time processing with minimum delay is needed. Processing must occur at the same speed as the objects moving along the assembly line. Token ring is not a suitable for this purpose because the number of collisions is not predictable and the delay in sending data from the control center to the computers along the assembly line is not a fixed value. Token ring is also not a suitable protocol because an assembly line resembles a bus topology and not a ring.

4) A ring WAN topology connects locations rather than local nodes. Unlike the Single-Link WAN, routers at any network site can redirect data to another route if one route becomes too busy, however a single cable (as in single link WAN) can break the interconnect of entire network. Also, the single Link WAN at the time of expanding requires at least one additional link.

3.8 KEYWORDS

Ethernet : A system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.

MAC Address : A media access control address is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet.

Routers : Small physical devices that join multiple networks together. Technically, a router is a Layer 3 gateway device.

WAP : Short for the **W***ireless* **A***pplication* **P**rotocol, a secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios, smartphones and communicators.

Wi Fi : 1. A facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

WiMAX : WiMAX is a wireless communications standard designed to provide 30 to 40 megabit-per-second data rates, with the 2011 update providing up to 1 Gbit/s for fixed stations.

3.9 REFERNCES ANDFURTHER READING

Forouzan, Berhouz. *TCP/IP Protocol Suite.* TATA McGraw Hill. Print

Godbole, Achyut S. *Web Technoligies*. TATA McGrawHill. Print

Stalling, William. *Data and Computer Communication*. PHI: New Delhi. Print

Tenenbaum,Andrew S. *Computer Networks*. PHI: New Delhi. Print

Websites

http://en.wikipedia.org/w/index.php

http://www.angelfire.com/mech/phattony/

http://technet.microsoft.com/en-us/library/

UNIT 4 TECHNOLOGY CONVERGENCE

Structure

4.0 OBJECTIVES

After going through this Unit, you will be able to understand and appreciate:

- what is meant by convergence;
- convergence as a phenomenon;
- the goal of convergence;
- important convergence objectives;
- organisations responsible for convergence standardisation;
- the origin and progress of convergence;
- the factors that drive convergence phenomenon;
- connectivity, capacity and content as the main focus of convergence;
- layered convergence architecture;
- convergence in different layers of the architecture;

- technology and techniques convergence;
- network, access and services convergence; and
- convergent applications like internet radio and interactive TV.

4.1 INTRODUCTION

As students of BLIS, you must be aware that the world has witnessed the phenomenon of information explosion in the last century. The advent of industrial age accompanied by an increase in world population has brought about significant growth in information generation and dissemination. All round developments in areas like transportation, power, communications, entertainment and education have led to exponential growth in information. Today, information generated doubles every five years. By the middle of last century, computers were pressed into service to store and manage large volumes of information in electronic form. The electronic storage media is capable of storing large volumes of data while occupying small physical space. When a complete document is stored in electronic form, we call it as **electronic document**. We use digital technology to store information electronically. Hence, an electronic document is also known as **digital document**. Digital technology is very rugged and reliable and uses only two signal values to represent information. Numerically, we represent the two signal values by binary digits (bits) '1' and '0'.

The world is evolving towards a Networked Electronic Information Society (NEIS). As you know, a networked society means one in which a large proportion of the world population is interconnected or networked by some form of telecommunication system and the people carry out their day-to-day activities using the network predominantly. Day-to-day activities may involve tasks such as banking, ticket booking for travel or entertainment programmes, product ordering, financial transactions, exchange of mails, retrieving of information from a database, downloading of music files, simple telephone conversation etc. Electronic information is central to all these tasks. Activities that are carried out in the electronic domain using networks are usually denoted with a prefix 'e-' such as e-banking. We now list some of the e-activities that are evolving in the networked society:

- e-education
- e-governance
- e-library
- e-health
- e-banking
- e-commerce
- e-mail
- e-entertainment
- e-journal
- e-newspaper
- e-marketing
- e-procurement

E-activities are often referred to as online-activities. Examples include online-ticketing, online-banking etc. To illustrate what e-activities mean, we elaborate two of the above activities. First, we illustrate e-education. This means sign up with a university, pay fees, obtain lessons, submit assignments give examination and obtain results, all via network without having to visit the university actually. Counselling is also available via network. A student may book time with a counsellor and interact with him/her via Internet. In India, IGNOU is offering e-education in many areas. Second, we look at an e-library. The resources and services of an e-library can be accessed on the network without having to physically go to the library. For this purpose, it is necessary to store all the

library resources in digital form. A library whose resources are available in digital form is known as **digital library**. When accessed over networks from remote places, a digital library becomes an **e-library**. What is underlying the NEIS or the so-called e-world? It is the concept of convergence.

4.2 WHAT IS CONVERGENCE?

Last few decades have witnessed significant development in the field of telecommunications, computer networking, information technology and Internet. Optical fibre, wireless and satellite communications have seen many advances. Communication satellites and remote sensing satellites are used extensively today. Mobile communication has become a common place with close to half of the world population connected by mobile networks. Internet has grown leaps and bounds from a few interconnected computers in 1980 to over a billion computers in 2009. This is often termed as Internet Revolution. Usefulness of these developments to the society increases significantly when there is a synergy of purpose amongst different technologies and techniques. In other words, the use of technologies, the design of networks and the development of services must all be directed towards a common goal. Such a common goal is NEIS. The process of bringing together different technologies, techniques, networks and services to realise the common objective of evolving towards NEIS is known as **convergence**. E-activities are central to NEIS. And, convergence is a fundamental requirement to make e-activities possible in a networked society. Without convergence no networking or e-applications are possible. It is because of convergence concept the networked society is becoming a reality. We study the goal and objectives of convergence in detail in Section 4.3.

In fact, convergence is not limited to NEIS. It is much wider phenomenon covering many technologies and even human resource. For example, convergence is much talked about in automobile industry. There it refers to the use of electronics, communications and computers in automotive controls and operations. For example, use of radar to sense vehicles or other obstacles ahead on the road and automatically adjusting the speed is possible only when the relevant technologies converge. Another interesting example is the use of intelligence in air conditioners. Conventional air conditioners maintain the room ambience according to certain set parameters. Air conditioners with intelligence determine the ideal room ambience and maintain the same. They take into account factors like human biological rhythm, the present heat load, atmospheric temperature etc. in determining the ideal ambience. Artificial intelligence, biological science, instrumentation and computer engineering are some of the disciplines that contribute to producing such an air conditioner. There is little doubt that the world is witnessing a phenomenon of convergence in almost all the fields.

Convergence was born when the computer and communication engineers realised the tremendous potential of bringing the two technologies together. From then on, every development relating to technology, switching techniques, protocols, services and applications has kept in mind the convergence aspect. We trace the genesis and development of convergence in Section 4.4. Connectivity, inter-operability, content access and capacity of communication and computer systems lie at focus of convergence. We discuss this in Section 4.5. The fact that the convergence principle is applicable from basic communication systems that move bits and bytes to sophisticated network applications has led to the study of convergence architecture. We cover this in Section 4.6. The individual components of the architecture are discussed in Sections 4.7 – 4.10. Convergence applications are becoming commonplace these days. These days, we hear a lot about access to Internet from mobiles in third generation (3G) mobile

communication systems. This is an excellent example of convergence between mobile communications and Internet. With this, we would have a host of new applications like mobile banking, m-commerce etc. Literally, every application that is emerging today is based on the convergence concept. We discuss convergent applications in Section 4.11.

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) Define convergence.

.....

.....

.....

.....

4.3 GOAL AND OBJECTIVES OF CONVERGENCE

As discussed earlier, convergence is an essential fundamental requirement for NEIS to emerge. The degree of success of convergence phenomenon would determine the speed with which mankind would move towards NEIS. In the context of NEIS, the goal of convergence may be stated as:

To achieve the capability wherein any network can deliver any service to any platform, and any user with an appropriate consumer device can access any application that runs on the networked world.

In some sense, the goal as stated above is reflection of the famous idiom "Unity in Diversity" in the context of NEIS. Multiplicity of networks and computer platforms make up the basic infrastructure of the networked world. For example, we have landline and radio networks. We have PCs, servers and mainframe computers. These networks and platforms are designed by using a variety of different technologies. For example, two different technologies, viz. GSM and CDMA are used for designing mobile networks. GSM stands for Global System for Mobile communications and CDMA for Code Division Multiple Access. Landline networks may use copper cables or optical fibres. There would be a multiplicity of applications and a multiplicity of consumer devices. In the midst of all these multiplicity, there exists the unity of purpose that any user connected to any network is given the capability for accessing any application that runs on any platform anywhere in the networked world. Of course, the user must have the appropriate consumer device that is required by an application. Obviously, a user cannot expect to access an application that delivers pictures by using a plain telephone set. Integrated consumer devices are capable of transmitting and receiving audio, video and data. Such devices enable the users to access multimedia applications on the global network. We are witnessing the concept of integrated consumer device being applied in mobile handsets extensively. As you may be aware, we have mobile handsets that have built-in camera, FM radio, MP3 audio player, Internet access feature download facility etc.

There are only three generic forms of information in NEIS: Audio, Video and Data. Audio includes speech and music. Video includes television, movies pictures, photos etc. Data includes all computer-generated information such as text, computer graphics, computer animation, digitised documents etc. Every application in NEIS is built around these three fundamental forms of information.

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.

2) What is an integrated consumer device?

3) What are the fundamental constituent components of information?

.....

.....

.....

.....

4.4 GENESIS OF CONVERGENCE

The genesis of convergence can be traced to mid 1950s. At that time, the computers were expensive resources and required highly controlled environment for their operations. They were housed in big computer centres that were air-conditioned with temperature, humidity and dust control. Entry was restricted to these centres and people were required to remove their shoes and wear aprons to work inside the centres. Computer centres were few in numbers and often located in faraway places. Users had to travel long distances to reach the centres. India had only three or four computers in the first half of 1960s located in the major cities like Kanpur, Delhi, Kolkata (the then Calcutta) and Mumbai (the then Bombay). In effect, working with computers was difficult for prospective users.

Around the same time, computer manufacturers were keen on increasing the clientele for their computers for economic reasons. Being expensive resources, high usage was essential to justify the cost associated with the establishment of computer centres. On the one hand, the prospective users could not get easy access to computers and on the other, computer resource was being under utilised. A solution was needed to resolve this issue for the benefit of both users and the owners of the computer systems.

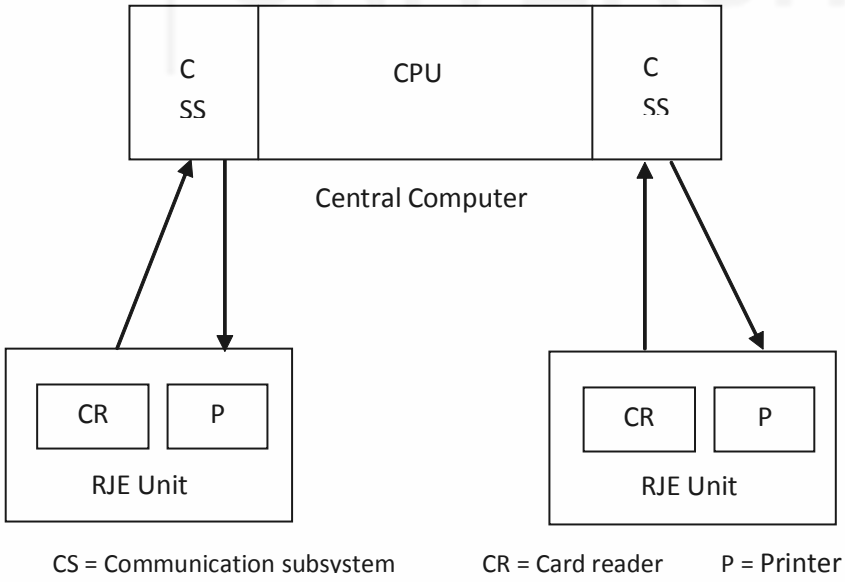

Fig. 4.1: Remote Computing Set-up

The solution was found in the famous saying that goes as: If Prophet Mohammad cannot go to the mountain, the mountain comes to him. Computer manufacturers took an

approach reflected by this saying in solving the problem of low usage of computers. They decided to take the access to computers to the doorsteps of users. The approach is known as **remote computing**, i.e. the users could access a computer and perform computations from a remote location. Implementation of remote computing required a suitable communication link between the remote site and the computer centre as shown in Fig. 4.1.

In those days, computer programs were used to be prepared on cards by punching holes and submitted to a computer centre for execution. A program thus submitted was called a job. Accordingly, in remote computing, the equipment at the remote site was called Remote Job Entry (RJE) terminal. This usually consisted of a card reader as an input device and a printer as output device suitably interlinked to the main central computer via dedicated communication lines. Many RJE terminals could be connected to one central computer thus allowing users from different locations to access the same central computer. This solution turned out to be win-win solution for both users and the computer owners. Users could access the computer easily and at the same time the utilisation of the computer went up significantly. Remote computing is the first application that brought computer and communication technologies together laying the foundation for technology convergence. Thus, the genesis of convergence lies in remote computing that started in late 1950s.

RJE centres were non-interactive online centres. They were permanently connected to the main computer centre via communication lines; i.e. online. They were non-interactive because users could not access the computer online. They submitted their jobs on cards and their outputs became available many hours later. Thus, RJE centres were offline as far as the users were concerned. However, RJE centres demonstrated the successful remote online connectivity.

Once remote computing was successful, suitable software systems were developed to allow user interact directly with the computer giving birth to what is known as **interactive computing.** In interactive computing, the users interact directly with the main computer. I/O is done via visual display units (VDU) or **monitors,** as they are popularly known, with keyboard acting as the input device and the screen as the output device, a configuration that we are very familiar with these days. The VDUs, i.e. the monitors are connected online to the computer. It was just a matter of time that a cluster of VDUs was placed in RJE centres, laying the foundation for network computing.

The idea of sharing data, information and other resources emerged in the late 1960s. Focus shifted from communication between terminal and computer to communication between computers, which marked the emergence of **computer networks**. In fact, the ideas developed in remote computing form the basis of access to Internet even today. The convergence of computer and communication technologies took deep roots by the end of 1960s. This was most aptly summarised in the words of a famous information scientist R. M. Fano as quoted in the following:

The marriage of computers and communications has been celebrated and consummated. The honeymoon is over and the two partners are realising the hard realities of inter-dependence on each other. - R.M. Fano, 1972.

After 38 years of this marriage, the bond is growing from strength to strength and today we are witnessing the phenomenon of convergence in a variety of areas to realise the common goal of networked society.

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.

4) Why is remote computing a win-win solution for users and computer owners?

.....

.....

.....

.....

4.5 CONVERGENCE FOCUS

Quite often, a question arises as to what should be the focus of convergence efforts? There are three important aspects towards which convergence efforts in NEIS may be directed:

- Connectivity
- Capacity
- Content

At present, less than one-sixth of the world population is connected to telecommunication infrastructure for some service or the other. Over five billion people in the world still have no network connectivity. The existing connection may be for a simple service like telephone, dial-up Internet access or a multitude of services offered by ISDN. Should the convergence efforts be directed towards increasing the connectivity level and thereby make a larger percentage of the world population as part of NEIS? Bringing in more people on the network has been considered important by major international organisations. In fact, International Telecommunication Union (ITU) has suggested that every village in the world be brought on to the connectivity map by the end of year 2015 as part of its global multi-stakeholder initiative called Connect the World launched in June 2005.

As mentioned earlier, interactive services are likely to be dominating NEIS. Interactive services, restricted to text transfer like e-mail, information access and simple graphics transfer can be supported by limited bandwidth connections that exist today. The current information transfer rates are in the range of 64-128 kbps. The rates are proving to be inadequate even for the current level of usage. For example, Internet response for Web access at times becomes so slow that it made someone to expand the acronym WWW as World Wide Wait! Multimedia interactive services envisaged in NEIS demand transmission and distribution of high fidelity voice, high quality video, 3-D graphics and other forms of information. This calls for a broadband communication pipe supporting data rates of the order of 100 Mbps or more to be extended to customer premises. Broadband services have the potential of increasing the revenue earnings for the network operators as the users may be prepared to pay high charges for the services. Should then the convergence efforts be directed towards enhancing the capacity of the existing communication pipes instead of increasing the connectivity?

A network infrastructure without contents and applications to run on it is like 5-star hotels without guests to occupy them. The importance of content creation has been

emphasised by many experts. For example, a CEO of a networking company once remarked something to the following effect "We do not want to build dumb pipes. If we make only racks and servers, that is dumb. What we should do is to meld contents and networks" Norio Ohga, an ex-chairman of Sony once remarked "Without content, network is nothing". Yet the debate of content versus connectivity is hot. One of the main reasons for this is that the statistics show that consistently connectivity applications earn much more revenue than content delivery systems. In connectivity applications like telephone, the end users create the content. The highest revenue is earned from voice conversation in both landline and mobile networks. The other source of major revenue is the fax usage, which is again a connection-oriented service. Another pointer is a comparison between Small Messaging System (SMS) and Wireless Access Protocol (WAP) on the mobile networks. SMS is connectivity oriented where the end user creates the content. WAP is a content delivery protocol for wireless devices. Statistics show that SMS is more widely used than WAP and brings in more revenue. On the Internet too, it is the e-mail that is the 'killer' application and not the wide area information system (WAIS). In fact, it appears that even historically the connectivity has been more important for people. For example, in the postal system the main revenue earner is the letter communication rather than the newspaper distribution. It appears that the people prefer to create their own content and all that they need is an efficient connectivity infrastructure that is affordable.

So, the debate goes on. In the opinion of this author, all the three aspects, viz. connectivity, capacity and content are important. Small and medium network operators must concentrate on connectivity. Large operators must focus on capacity. Content creation must be left to end users and specialists like movie producers.

4.6 CONVERGENCE ARCHITECTURE

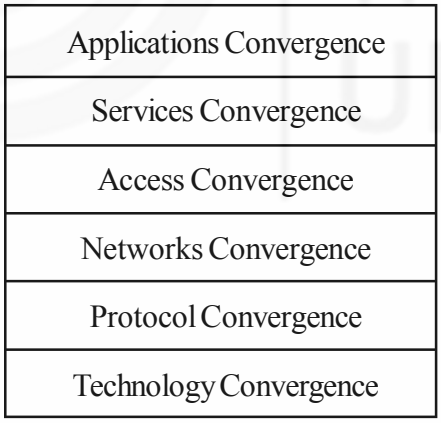

Fig. 4.2: Convergence Architecture

The phenomenon of convergence in the context of networked society is occurring at many levels. Different levels of convergence may be represented in the form of a layered architecture as shown in Fig. 4.2. At a very broad level, convergence is seen at sectoral level of infrastructure such as telecommunication sector, power sector, automobile sector, air conditioning sector etc. At the second level is the convergence in technology. Technology convergence is studied at two levels. First, how different technologies in the same sector exhibit synergy to achieve certain common goals? Second, how technologies in different sectors come together to produce better products? Our main concern is the first question in Information Communication Technology (ICT) sector to achieve the goals of NEIS. Technology convergence is fundamental to the entire process

of convergence in NEIS. Without technology convergence, other layers of convergence are not possible. Once the technologies are able to interwork, techniques that can be applied across all technologies need to be evolved. In particular, switching and signalling techniques need to converge in ICT. Techniques convergence layer deals with this aspect. Once converging techniques are available, the different networks and systems can be made to interwork with each other. Then comes the need for access convergence. From any one interface, the user must be able to access all the services available in NEIS. In the architecture shown in Fig. 4.2, a distinction is made between services and applications. Services are provided by the network operators and the applications are designed and run by end users. Applications make use of the network services.

4.7 TECHNOLOGY CONVERGENCE

There are four major communication technologies that form part of modern telecommunications:

1) Electrical communication system

2) Optical communication system

3) Radio or wireless communication system

4) Satellite communication system.

Now, let us see how each one of these technologies converges to support the emergence of NEIS. The four communication technologies complement each other to improve **connectivity** and **capacity**.

Electrical communication uses copper cables of different types that have different information carrying capacities. Copper cables have been in use for a long time for establishing networks worldwide. Information carrying capacity of copper cables is being continuously improved and even today copper cable is a favourite medium in communication systems. Optical fibres are replacing the copper wires in certain segments of telecommunications because of their extremely high information carrying capacity. However, laying copper or optical cables to every village, home and office in the world is a formidable task and it may take many centuries if this were to be achieved. The enormity of the task becomes clear when we realise that we have been able to connect via landline only about 16% of the world population in the last 130 years. Further, laying optical fibres is more difficult than laying copper cables because of special considerations required for optical fibres in bending and routing. With such constraints, large-scale connectivity cannot be achieved in a short time frame by using cables. However, only high speed copper cables and optical fibres can offer high bandwidths. The bandwidth capacity of optical fibres is, of course, orders of magnitude higher than that of copper cables.

Our interest in wireless communication lies in short-haul radio technology that may be placed under four categories: mobile communication, wireless LANs, piconet, and wireless in local loop (WLL or WILL). Since the introduction of cellular mobile telephony in 1990, over one billion mobile subscriptions have been registered throughout the world as of 2004. There is a discernible trend that indicates that new users prefer mobile connectivity to landline connectivity. Today over 90% of the countries in the world have mobile networks and over 100 countries have more mobile subscriptions than fixed landline subscriptions. Clearly, mobile communication is raising connectivity levels significantly. Data and video carrying capacity of mobile systems are very limited.

Wireless LANs are useful in such cases of office and home networks where wired infrastructure may not be available. They can also provide high capacity. Their main problem is in electromagnetic interference and lack of privacy and security. Wireless LANs may be affected by or cause interference from/to neighbouring networks. Eavesdropping is very easy on wireless LANs.

WLL short-haul radio technology has the excellent potential of making interactive services a reality. Residential premises may be connected to nearby communication centres via WLL radio technology. The centres may be equipped to offer large bandwidth using optical fibres. This principle may be extended to provide limited interactive facility to individual users via mobile communication technology. However, WLL is capable of providing much higher capacity than mobile technology. The use of short haul radio implies the establishment of radio network, which can be done more easily in urban areas than in rural areas.

In the context of remote area connectivity, satellite communication presents a practical solution for connecting remote areas. Establishing connectivity via satellite links is by far the quickest. Even remotest villages can be brought on to the world network map in a matter of few hours by using satellite links. Local cabling may be used to carry information between the satellite terminal and the houses in the village. Satellite links do not need any landline infrastructure except for local distribution. At present, efforts are on to develop satellite mobile systems wherein a hand-held device may connect to a satellite directly without the help of a terminal. This also offers an elegant solution to rural area connectivity even though the capacity of the hand-held terminals may be very limited. As mentioned earlier, the main problem with the satellite is the limited capacity. The bandwidth of a typical present day communication satellite is at least a few hundred times lower than that offered by a single optical fibre. Limited bandwidth of satellites does not permit high-capacity two-way interactive communication to individual homes.

Trained manpower is an important consideration in selecting technologies. Copper cable communication is well known and a large number of trained technicians are available to install and maintain such systems. This is the reason why a large number of cable operators have sprung up in the market. Optical fibres are new and satellite communication is highly specialised. Manpower is limited in both areas. Radio communication is well understood but mobile communication involves new concepts that are not taught extensively at present.

Table 4.1 summarises the strengths and limitations of different technologies that we have discussed so far. The convergence of the four communication technologies, inter-operating with each other, can provide a suitable solution to the problems of connectivity, capacity and trained manpower in the networked information society of tomorrow.

Table 4.1: Technology Convergence

Technology	Connectivity	Capacity	Manpower
Copper cables	Fair	Reasonable	Very Good
Optical fibres	Difficult	Very High	Limited
Satellite	Rural areas	Limited	Limited
Short haul radio	Urban areas	Limited	Low

We now have a paradoxical situation. Short-haul radio and satellite communication enhance connectivity but have limited bandwidth capabilities. High speed copper cables and optical fibres can offer very high bandwidth but have serious connectivity limitations. Hopefully, these technologies are poised to play complementary roles in shaping the

networked information society of tomorrow. Clearly, the goal of telecommunications in the years to come is to establish a wide band multi-services network reaching out as large a population of the world as possible.

4.7.1 Bluetooth Technology

Bluetooth is the codename for a short-range wireless convergent technology. It is a low power radio technology covering a small range of distances up to 10 metres. The purpose of the technology is to make bluetooth enabled devices that are in the vicinity of a master device to communicate in a wireless mode. The technology is very simple to use. All that one needs to do is to bring a bluetooth device close to bluetooth-enabled computer and a communication can start. There is no cable or modem or driver to be installed. The simplicity of its use is very attractive to users. For example, a mobile phone may connect to a laptop computer and send and receive electronic mail if the two devices have bluetooth interface incorporated in them. Bluetooth communication calls for no additional infrastructure like mobile communication that calls for a radio network to be in place. Bluetooth devices can communicate directly without any network support.

Bluetooth functions in master-slave configuration. Usually a bluetooth-enabled computer acts as a master. Slave devices are dumb, basically doing whatever the master tells them to do. Typical slave devices include digital cameras, mobile handsets, scanners and personal digital assistants (PDA). Up to 7 slave devices can be active at a time. If more than seven slave devices come in the vicinity, the master computer can place these devices in 'parked' mode. There can be up to 255 parked nodes in the net. The master can wake up a parked node and allow it to communicate with it. All communication is between the master and the slave. Direct slave-to-slave communication is not possible. The technical name for the Bluetooth network is **piconet**. Multiple piconets can be interconnected to form what is called a **scatternet**.

Bluetooth has potential for many interesting applications. These include:

- Receiving and sending email from mobiles
- Check in at airports
- Check in at movie theatres
- Sending and receiving fax from PDAs and mobiles
- Digital walkie-talkie
- Make e-payments
- Transferring picture files from digital cameras to computers
- Connecting a scanner to a computer without a cable.

In general, wherever there is a queue-based activity, bluetooth technology can be used. In other words, bluetooth technology has the potential of eliminating queues from this world!

4.7.2 3G and WiMAX Technologies

Mobile communication has undergone three generations of development. The first generation (1G) mobile communication was basically analog voice communication. The second (2G) generation systems are designed for digital voice communication and low

speed data transmission. In India, we have mainly 2G mobile systems prevalent and 3G is picking up fast. There are two technologies and standards associated with 2G systems: GSM and CDMA. GSM stands for Global System for Mobile communications. CDMA stands for Code Division Multiple Access systems. Both technologies operate in India. Low speed data feature of 2G systems supports SMS (Small Messaging System) service. Since higher data rate can support services like MMS (Multimedia Messaging System), the 2G technology was enhanced using two techniques: General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE). The resulting systems were called 2.5G mobile systems. Much higher-level services can be offered in 3G systems. These include video telephony, Internet browsing, mobile television and high quality music. The main difference from one generation to the next is the amount of bandwidth available for services. Higher the bandwidth, the larger is the variety of services that can be offered. 3G systems offer voice, video and high-speed data services taking convergence one step further.

4.8 PROTOCOL CONVERGENCE

Wi Max is the wideband wireless data access technology. This technology permits mobile operator to offer very high-speed data services to users. The data rates may vary from 2 Mbps to 100 Mbps.

Switching, signalling and transmission techniques are the main ones in networks. Signalling includes addressing and routing apart from monitoring sessions and connections. In this section, we shall bring out the divergence that exists in these areas and the convergence efforts that are currently being pursued.

As you are aware, the principle of switching is central to all networks. The switching technique adopted by data networks is different from the one used by telephone networks. Telephone networks use the technique of **circuit switching** whereas data networks use **packet switching**. In circuit switching, a communication path is established between the source and destination before the actual information transfer takes place. This path and the associated resources remain dedicated to the communicating pair until any one of the two entities initiates a disconnect request. The path is used effectively if there is continuous traffic during the service period. However, if the traffic between the source and destination is not continuous, the path remains partly idle during the service, leading to inefficient use of network resources. In packet switching, information transfer takes place in a store and forward fashion from node to node in the form of packets. At every node, the destination address is processed before the next forward move is made. The packets move from one location to another in the general direction of the destination. There is no connection between the source station and the destination station.

In the context of multi services network, it is recognised that packet switching is not suitable for real time services like telephony and video distribution. And, circuit switching is not efficient for bursty non-continuous traffic from the point of view of utilising network resources. The realisation that both circuit switching and packet switching are required for different purposes on a common digital network led to the search for new switching techniques. The two techniques have now converged and a new switching technique called **cell switching** is now accepted as the standard switching technique for future broad band infrastructure. Cell is a small-sized packet that moves very fast on a digital infrastructure. Cell switching is capable of supporting both real time and non-real time services efficiently. However, it is foreseen that for sometime to come, all the three switching techniques would co-exist.

The importance of signalling in networks is reflected by statements such as 'If we cannot signal, we cannot make a call' and 'If we cannot signal, we cannot transfer a packet'. Attempts to convert existing single-service networks to multi-service ones has led to the emergence of a plethora of signalling techniques. Specific convergence questions are how do we support real time services like telephony on IP-based packet networks and how do we transport packets efficiently on circuit switched networks? Circuit-switched and packet-switched networks use entirely different forms of signalling. The signalling protocols are also very different. Convergence signalling protocols on the IP-based packet networks include media gateway control protocol (MGCP), session initiation protocol (SIP) and real time control protocol (RTCP). These are protocols brought out by the Internet Society. ITU-T has brought out recommendation H.323 that allows interworking of circuit switched networks and IP-based packet networks. H.323 refers to a number other signalling protocols used in circuit switched networks. H.323 is the key convergence protocol that is used at present to offer real time services like IP Telephony on IP-based packet networks.

At the transmission level, two transmission hierarchies are emerging. One is ITU recommendation known as synchronous digital hierarchy (SDH) and the other evolved by U.S. in the context of optical networks known as optical carrier (OC) hierarchy. OC transmission systems run on synchronous optical networks (SONET). SDH is applicable to both copper and optical networks. Luckily, the transmission speeds are identical in both SDH and OC at different levels of hierarchy. The speeds at which SONET runs are specified as OC1, OC2, OC3 etc. The lowest speed of SONET is OC1 at 51.84 Mbps. SDH speeds start at OC3 level that corresponds to 155.52 Mbps. The basic speed of ATM network is also OC3.

4.9 ACCESS CONVERGENCE

The economic considerations do not apply only to network providers. It is equally important for the users. A user may not invest in different types of access interfaces for different services. A single telecommunication connection should fetch all types of services to a user subject only to the limitations of speed and capacity of his interface. It is this philosophy that has led to the idea of access convergence. The trend of access convergence is being seen in the following:

1) Access to Internet from mobile handset and vice versa

2) Access to global satellite services from mobile and vice versa

3) Access to Internet from telephone network and vice versa

4) Access to global satellite services from telephone network and vice versa

5) Automatic access among bluetooth devices

6) Access to Internet via television cables and vice versa.

Access convergence provides tremendous flexibility to end-users. They are able to access a variety of services from whatever device they have on hand. For example, a person with a mobile, a tablet or a laptop can literally access all Internet services without physically having a connection to the Internet. Satellite telephony allows telephone conversations directly via satellites from anywhere in the world.

4.10 SERVICE CONVERGENCE

The idea of convergence in different areas that we have discussed so far is to carry multiple services using one common infrastructure. The trend of service convergence, i.e. offering multiple services in one interface, is seen in the following:

1) Real time services like telephony on the Internet

2) E-mail via mobile phones

3) Web access via bluetooth interface and mobile phones

4) E-mail and Web access via television cables

5) Internet services delivered on TV sets

6) Broadcasting radio and TV programmes on the Internet

7) Normal telephone services via cable TV networks.

Broadcasting on the Internet is sometimes called webcasting. The above are examples of some of the recently introduced services using the concept of convergence. For the future, ISDN and broadband ISDN are being designed to carry every conceivable service. Let us now see how service convergence issue is being addressed in broadband ISDN. In broadband ISDN, the services are placed under some generic categories as shown under:

- Audio services
  - Telephone quality (speech)
  - Broadcast quality (music)
- Motion video services
  - Studio quality
  - Broadcast quality
  - High definition television (HDTV)
- Still video services
  - Low resolution (fax)
  - High resolution (pictures and photographs)
- Text services
- Computer graphics services
- Computer animation services
- Satellite imageries

Each of the above services, when digitised, demand different communication capacities, i.e. different speeds. To carry a variety of services with different capacity requirements, the architecture of broadband ISDN uses the ATM information transport mechanism. ATM is structured in a layered manner with different functionality stacked one over another. One of the layers is known as **ATM adaptation layer**. It has a sublayer called **convergence sublayer**. This sublayer has been designed to multiplex a variety of

services and carry them on the underlying network infrastructure. The underlying infrastructure for ATM is by and large an optical network like SONET.

4.11 CONVERGENT APPLICATIONS

In this section, we shall discuss some important upcoming convergence applications: Music on demand, Internet radio, Internet telephony and Interactive Television.

Music on demand, known as streaming audio in technical terms deals with listening to music on Internet. As you know, Internet is a data network capable of transporting 1s and 0s. Once digitised, music is in the form of 1s and 0s. Therefore, theoretically digital music can be transported over Internet. Listening to music happens in real time. But, the Internet is not designed to provide real time services. Therefore, the convergence question is 'how to deliver music in real time on Internet?'

Digital sound is compressed before storage. One of the most popular standards used for digitisation and compression is MP3 standard and format. There are many web sites on the Internet that store music in MP3 digital form. The most popular application architecture on the Internet is client-server architecture. The server runs web server software and the client web browser software. The interaction between the web browser and the web server takes place via the application protocol HTTP that runs on TCP. HTTP is not a real time protocol. One way to listen to music under HTTP is to download the entire music file and play it from the client machine. A typical song in MP3 format takes about 4MB and it would take about 8 minutes to download the entire file at 64 kbps speed. Internet rarely runs at that speed. It could sometimes take as much as 15 minutes to download the entire file. The user will have to sit idle during download of each song. This clearly is an unacceptable solution. Streaming audio overcomes this deficiency and provides a near real time solution.

Streaming audio application is designed under client-server architecture supplemented with a media server on the server side and a media player on the client side. The media server and the media player interact via the real time protocol (RTP) that runs on UDP. Initially, the user interacts with the server via the browser for selecting the music bit. Thereafter, the media server and the media player come into picture to play the music in real time. The streaming audio configuration is depicted in Figure 4.3.

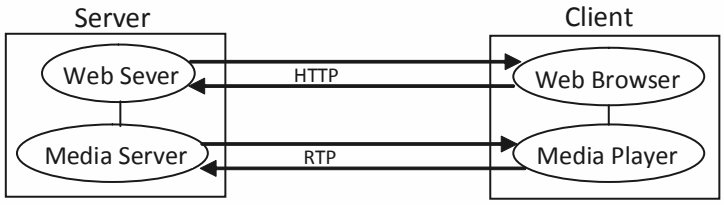

Fig. 4.3: Streaming Audio Configuration

RTP runs on UDP. UDP runs on IP which is a packet protocol. A packet in the case of streaming audio comprises an accumulation of digital samples of music/speech for certain duration, usually 5-8 msec. In other words, each sample is not transmitted in real time but about 40-64 samples are grouped together and transmitted. The grouping of samples and making them available in bursts lead to unnatural audio. However, grouping up to 6 msec is not noticeable by the human ear. As you know, in packet switching, each packet takes a different time to reach the destination depending on the traffic conditions on the network. While an average delay is computable, a packet may arrive much later than the average delay or even be lost on the way. Such delay variation from packet to packet causes jitters in the music affecting the quality. Streaming audio takes care of

these problems by providing a music buffer at its input. At the start of a listening session, the buffer is filled with music samples before the music is played out to the user. The buffer holds about 15-20 seconds of music. The user has to wait only for a short while until the buffer is full before he can start listening to music. The music packets continue to arrive from the server while the media player is playing out the music and emptying the buffer contents. This is a streaming operation and hence the name streaming audio. On the one side the buffer is being emptied and on the other it is being filled. The provision of the buffer ensures that continuous music is available even in the presence variable packet delays.

In order to provide flexibility to user in listening, certain control functions as available in a cassette player need to be implemented by the media player-server combination. The control functions include controls like pause, resume, stop, fast forward and fast backward. Some flow control feature is also required. For example, if the packets arrive too fast from the server, then the buffer would become full and the packets would be discarded at the player end. To prevent this from happening, the media player may ask the media server to pause the flow momentarily. All such control functions are implemented using a protocol known as real time control protocol (RTCP) which is used in conjunction with RTP. There are two other protocols associated with streaming services. They are protocols used for establishing a real time session before streaming operation starts. The protocols are real time streaming protocol (RTSP) and session initiation protocol (SIP).

Internet radio is based on the same principles as streaming audio. There are some differences between music-on-demand and Internet radio. In music-on-demand, the music bit is selected by the user whereas in Internet radio, the programme is played out by the station. There is no user interaction for selection. This means that HTTP interaction is absent. User also has no control like pause, resume etc. Some radio stations play a second channel which is delayed by about 10 minutes to allow the users to take a break. After the break, the user may switch over to the delayed channel and listen to the programme from where he/ she left. Another important difference is that music-on-demand is a unicast service whereas Internet radio is a multicast service. Many persons listen to Internet radio at a time. Hence, the same audio stream has to be sent to different destinations.

The architecture of streaming audio is the building block of **streaming video** too. Video bandwidth is much larger and hence requires higher speeds of transmission on the Internet. The buffer size on the client side is also much larger as the sampling rate for digitisation of video is much higher. For example, 10 seconds of audio requires 80 kB of buffer whereas video for the same duration would require 2 MB of buffer. Another important requirement of video streaming is the synchronisation required between the video signal and the accompanying audio signal. Video streaming is the basis for a variety of applications such as distance learning, digital libraries, home shopping and video-on-demand.

Internet telephony is also known as **Voice over Internet Protocol** or simply **Voice over IP** (VoIP). Internet telephony is built around a set of protocols and standards defined by ITU. IT also uses the set of protocols we discussed as part of streaming audio. It was in 1996 that first attempts were made to build Internet telephony gateways when ITU first proposed architecture suitable for voice services in LANs in its standard H 323. This standard was revised in 1998 and forms the basis for Internet telephony. The architecture is depicted in Figure 4.4. Basically, the Internet and the telephone network are interconnected by a gateway. The gateway implements H.323 protocols on the Internet side and PSTN protocols on the telephone network side. The end

devices on the Internet are terminals and on the PSTN they are telephones. H.323 refers to a number of other ITU protocols. The telephone speech is digital and should conform to G.711 ITU recommendation that specifies 64 kbps PCM stream. G.711 conformity is mandatory for VoIP. Some other compressed audio streams that run at lower speeds like 6.4 kbps or 5.3 kbps are permitted optionally. The digital stream is transported over RTP under the supervision of RTCP. Both RTP and RTCP run on UDP. Since multiple compression schemes are permitted optionally, there is a need to negotiate and agree on the scheme before start of the session. This is done by call control protocol specified in H.245. Call establishment and release and call signalling, like sending out ring tone etc. are done according to ITU signalling protocol Q.931. The call control and call signalling protocols run on TCP. On the LANs, ITU suggests the use of a gatekeeper device that organises telephone call for LAN terminals. A protocol, named registration, admission and status (RAS) has been defined for the gatekeeper to interact with LAN terminals. The RAS protocol runs on UDP.

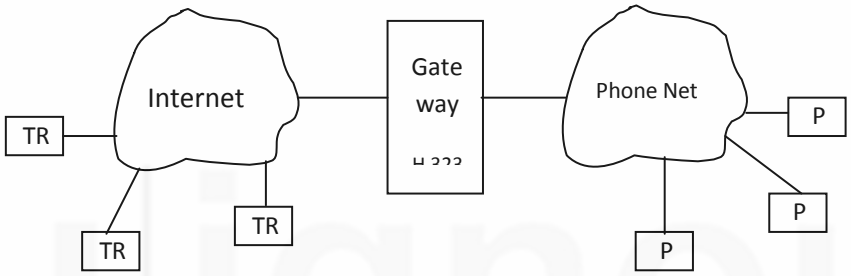

Fig. 4.4: Internet Telephony Architecture

Interactive television (ITV), also called two-way television is a convergence application where a one-way video broadcasting system is turned into a two-way system capable of handling media, i.e. voice, video and data. ITV is a television set with a return path to the broadcaster or the ITV service provider. The return path makes it interactive. Information flows not only from the ITV service provider to the viewer but also from the viewer to the ITV service provider and/or his computer. When fully developed, ITV would offer video-on-demand service. For the present, ITV systems are providing broadcast programmes with facility for interaction. ITV is evolving in three stages:

1) Programmes are broadcast and the return path is provided via PSTN.

2) Programmes are broadcast and the return path is provided via set-top box.

3) Video-on-demand programmes and return path via set-top box.

The set-top box is more than a TV tuner. It has a computer with a phone, coaxial cable or satellite link to the ITV service provider and the Internet. There is a phone modem or a cable modem or a network card, which connects the set-top box to a public network. Unlike broadcast service where the viewer can only watch one of the many programmes currently being broadcast, ITV gives the viewer an individual choice of content that may be exclusive to that viewer.

The potential use of ITV is enormous. To name a few, ITV may be used for marketing, advertising, child counselling, public relations, education and even politics. For the user, there is the promise of choice, fun, convenience and empowerment. Sitting at home, one will be able to get literally any product or service delivered at the touch of a button. This is known as t-commerce, television commerce. Users may click on advertisements

to know more about the product. Viewers may choose camera angles while watching their favourite sport events. This indeed is exciting. Users may pause and resume programmes that they are viewing, provided the programmes are not live. With live programmes, the users may record the programmes for later viewing. And, of course, e-mail can be sent through ITV.

There is one serious aspect of ITV, which is now spreading to Internet. All ITV systems have a feature called click stream analysis. This feature creates a complete record of the clicks that a user performs on his/ her set-top box. This record is later analysed to build profiles of users. In a positive sense, the purpose is to provide the user information that he/she is interested in. The negative aspect is that the service provider is actually treading into the private life of individuals.

ITV systems call for wide band infrastructure to transport individual programmes to different viewers. This infrastructure is an ATM network with synchronous optical network (SONET) as the transport infrastructure.

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) Differentiate between streaming audio and Internet radio.

.....

.....

.....

.....

4.12 SUMMARY

In this Unit the convergent aspects in the context of NEIS have been discussed. It introduces you to the concept of convergence and discusses the driving factors viz. societal need, economics of operation and technology support. The convergent phenomena in technology, network, access and service areas are explained in detail. The Unit finally covers the convergent applications like internet radio and interactive TV.

4.13 ANSWERS TO SELF-CHECK EXERCISES

1) The process of bringing together different technologies, techniques, networks and services to realise the common objective of evolving towards Networked Electronic Information Society (NEIS) is known as convergence.

2) Integrated consumer devices are capable of transmitting and receiving audio, video and data. Such devices enable the users to access multimedia applications on the global network. We are witnessing the concept of integrated consumer device being applied in mobile handsets extensively. As you may be aware, we have mobile handsets that have built-in camera, FM radio, MP3 audio player, Internet access feature download facility etc.

3) There are only three generic forms of information in NEIS: Audio, Video and Data. Audio includes speech and music. Video includes television, movies pictures, photos etc. Data includes all computer-generated information such as text, computer graphics, computer animation, digitised documents etc. Every application in NEIS is built around these three fundamental forms of information.

4) Remote computing has turned out to be win-win solution for both users and the computer owners as users could access the computer easily and at the same time the utilisation of the computer is optimised.

5) Internet radio is based on the same principles as streaming audio. However, there are some differences between them. In streaming audio, the music bit is selected by the user whereas in Internet radio, the programme is played out by the station. There is no user interaction for selection. This means that HTTP interaction is absent. User also has no control like pause, resume etc. Some radio stations play a second channel which is delayed by about 10 minutes to allow the users to take a break. After the break, the user may switch over to the delayed channel and listen to the programme from where he/ she left. Another important difference is that streaming audio is a unicast service whereas Internet radio is a multicast service. Many persons listen to Internet radio at a time. Hence, the same audio stream has to be sent to different destinations.

4.14 KEYWORDS

Bluetooth : A wireless networking technology that uses short-wave radio frequencies to interconnect cell phones, portable computers, and other wireless electronic devices.

Cell Switching : A convergent switching technique that combines the strengths of circuit and packet switching.

Circuit Switching : The process of establishing a dedicated connection between two end points via a network.

Distributive Services : Services that are broadcast or multicast in nature i.e. services that are distributed to a large number of users without a request from a user.

On- demand Services : Services that can be obtained by users by placing a demand on the network.

Packet Switching : The process of transferring information from a source to a destination on a node-by-node basis.

RJE Terminal : Remote job entry terminal, an equipment set up to use computers from remote places.

4.15 REFERENCES AND FURTHER READING

Douskalis, B. *IP Telephony*. New Delhi: Pearson Education Asia, 2001. Print

Hersent, O., Gurle, D. and Petit, J.P. *IP Telephony: Packet-Based Multimedia Communication System*s. New Delhi: Pearson Education Limited, 2001. Print

Johnston, C. B. Communication Conglomerates. In: *Encylopedia of Information Systems*, Volume 2, USA: Elsevier Science. Print

Pavlik J. V. And Powell, A. C. New Media. In: *Encylopedia of Information Systems*, Volume 2, USA: Elsevier Science. Print

Rao, K. R., Bojkovic, Z. S. and Milovanovic, D. A. *Multimedia Communication Systems*. New Delhi: Prentice Hall of India, 2002. Print

Viswanathan, T. *Convergence of the Telecommunications, Information Technology, Media and Power Sectors*. New Delhi: Centre of Publications, 2001. Print

Viswanathan, T. *New Telecom Policy*. New Delhi: Government of India, 1999. Print

ignou
THE PEOPLE'S
UNIVERSITY