BCA-15

Vardhaman Mahaveer Open University, Kota

Fundametnal of Computer Networks

Course Development Committee

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

Co-ordinator/Convener and Members

Convener/Co-ordinator

Dr. Anuradha Sharma
Assistant Professor,
Department of Botany, Vardhaman Mahaveer Open University, Kota

Members :

1. **Dr. Neeraj Bhargava**
   Department of Computer Science
   Maharshi Dyanand University, Ajmer
2. **Prof. Reena Dadhich**
   Department of Computer Science & Informatics
   University of Kota, Kota
5. **Dr. Nishtha Keswani**
   Department of Computer Science
   Central University of Rajasthan, Ajmer
3. **Dr. Madhavi Sinha**
   Department of Computer Science
   Birla Institute of Technology , Jaipur Campus
4. **Dr. Rajeev Srivastava**
   Department of Computer Science
   LBS College, Jaipur

Editing and Course Writing

Editor

Dr. Reena Dadhich
Department of Computer Science & Informatics
University of Kota, Kota

Unit Writers	Unit No.
1. Prof. Reena Dadhich Department of Computer Science & Informatics University of Kota, Kota	**(1,2,3)**
2. Dr. C.K. Jha Department of Computer Science Banasthali University	**(4,9)**
3. Mr. Vivek Dubey Department of Computer Science Govt. Engineering College, Ajmer	**(5,6)**
4. Mr. Vijander Singh Department of Computer Science Amity University, Jaipur	**(7,8)**
5. Mr. Surendra Choudhary Department of Computer Science Shri Balaji College of Engineering, Jaipur	**(10,11)**
6. Mrs. Anju Sharma Department of Computer Science BISR, Jaipur	**(12,13)**
7. Mr. Sanjay Department of Computer Science Govt. Engineering College, Ajmer	**(14,15)**

Academic and Administrative Management

Prof. (Dr.) Vinay Kumar Pathak	**Prof. (Dr.) B.K. Sharma**	**Prof. P.K. Sharma**
Vice-Chancellor	Director (Academic)	Director (Regional Services)
Vardhaman Mahaveer Open University, Kota	Vardhaman Mahvaeer Open University, Kota	Vardhaman Mahaveer Open University, Kota

Course Material Production

Mr. Yogendra Goyal
Assistant Production Officer
Vardhaman Mahaveer Open University, Kota

Vardhaman Mahaveer Open University, Kota

Fundamental of Computer Networks

Preface

This book attempts to provide a complete overview of the different aspects of data communication and computer networks. The book emphasizes basics of data communication and fundamentals of computer networks. It gives discussion of all related topics and elaborates the current technological terms related with computer networking.

The complete book is divided in to fifteen chapters. Each chapter contains the problems and references for further reading.

In the initial part of the book the fundamentals of data communication networks and types of data transmission are described, then the discussion about computer networks such as LAN, MAN and WAN is given in detail. The Computer Networks part of the book gives the complete idea about wired and wireless networks, their transmission & the applications. This part also includes the models used for establishing computer networks, routing techniques and various network services. There is a great need for network security as everyone is using and working on networks. So the book also includes the discussion about network security mechanisms in a seperate chapter.

The main feature of this book which is different from other books available in the market are the complete overview about Indian networks as well as impact of telemetric society. As a whole the book provides an immense knowledge to the readers about data communication and computer networks. Each chapter is designed to cover individual unit.

The book is intended for both an academic and a professional readers. As a textbook it can be used for the students of undergraduate level to provide them the whole idea about computer networking, the book serves as a basic reference and is suitable for self-study.

Unit-1
Computer Networks

Structure of Unit

1.0 Objective

On completion of this unit, we will be able to:

- Define Computer Networks.
- State the evolution of Computer Networks.
- Categorize different types of Computer Networks.
- Specify some of the application of Computer Networks.
- Multiplexing, Transmission Media and Signals

1.1 Introduction

A computer network, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information. Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. In other words more than one computer interconnected through a communication medium for information interchange is called a computer network.

This unit covers the very basics of networking history. We'll start with a little history that describes how the networking industry evolved. This unit is an overview only. It will familiarize you with much of the vocabulary you hear with regards to networking. Some of these concepts are covered in more detail in later units.

Before the advent of computer networks that were based upon some type of telecommunications system, communication between calculation machines and early computers was performed by human users by carrying instructions between them. Many of the social behaviors seen in today's Internet were demonstrably present in the 19th century and arguably in even earlier networks using visual signals. We begin with a brief history of the computer Networks.

• In September 1940, George Stibitz used a Teletype machine to send instructions for a problem set from his Model at Dartmouth College to his Complex Number Calculator in New York and received results back by the same means. Linking output systems like teletypewriters to computers was an interest at the Advanced Research Projects Agency (ARPA) when, in 1962, J.C.R. Licklider was hired and developed a working group he called the "Intergalactic Computer Network", a precursor to the ARPANET.

• Early networks of communicating computers included the military radar system Semi-Automatic Ground Environment (SAGE), started in the late 1950s.

• The commercial airline reservation system Semi-Automatic Business Research Environment (SABRE) went online with two connected mainframes in 1960.

• In 1964, researchers at Dartmouth developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a research group supported by General Electric and Bell Labs used a computer to route and manage telephone connections.

• Throughout the 1960s Leonard Kleinrock, Paul Baran and Donald Davies independently conceptualized and developed network systems which used packets that could be used in a network between computer systems.

• In 1965, Thomas Marill and Lawrence G. Roberts created the first Wide Area Network (WAN). This was an immediate precursor to the ARPANET, of which Roberts became program manager.

• The first widely used telephone switch that used true computer control was introduced by Western Electric in 1965.

• In 1969 the University of California at Los Angeles, the Stanford Research Institute, University of California at Santa Barbara, and the University of Utah were connected as the beginning of the ARPANET network using 50 kbit/s circuits.

• Commercial services using X.25 were deployed in 1972, and later used as an underlying infrastructure for expanding TCP/IP networks.

Computer Networks are the core of modern communication today. All modern aspects of the Public Switched Telephone Network (PSTN) are computer-controlled and telephony increasingly runs over the Internet Protocol, although not necessarily the public Internet. The scope of communication has increased significantly in the past decade and this boom in communications would not have been possible without the progressively advancing computer network. Computer networks, and the technologies needed to connect and communicate through and between them, continue to drive computer hardware, software, and peripherals industries.

1.2 Advantages of Networking

Computer Networks have highly benefited various fields of educational sectors, business world and many organizations. They can be seen everywhere they connect people all over the world. There are some major advantages which computer networks has provided making the human life more relaxed and easy. Some of them are described below.

1.2.1 Communication

When we communicate, we are sharing information. This sharing can be local or remote. Between individual communication is one of the biggest advantages provided by the computer networks. Different computer networking technology has improved the way of communications, people from the same or different organization can communicate in the matter of minutes for collaborating the work activities. In offices and organizations computer networks are serving as the backbone of the daily communication from top to bottom level of organization. Different types of software's can be installed which are useful for transmitting messages and emails at fast speed.

1.2.2 Data Sharing

Another wonderful advantage of computer networks is the data sharing. All the data such as documents, file, accounts information, reports multimedia etc can be shared with the help computer networks. Hardware sharing and application sharing is also allowed in many organizations such as banks and small firms.

1.2.3 Instant and Multiple Accesses

Computer networks are multiple processed, many users can access the same information at the same time. Immediate commands such as printing commands can be made with the help of computer networks.

1.2.4 Video Conferencing

Before the arrival of the computer networks there was no concept for the video conferencing.

LAN and WAN have made it possible for the organizations and business sectors to call the live video conferencing for important discussions and meetings

1.2.5 Internet Service

Computer networks provide the internet service over the entire network. Every single computer attached to the network can experience the high speed Internet, fast processing and work load distribution

1.2.6 Broadcasting

With the help of computer networks news and important messages can be broadcasted just in the seconds who saves a lot of time and effort of the work. People can exchange messages immediately over the network any time or we can say 24 hour.

1.2.7 Photographs and Large Files

Computer network can also be used for sending large data file such as high resolution photographs over the computer network to more than when users at a time.

1.2.8 Saves Cost

Computer networks save a lot of cost for any organizations in different ways. Building up links thorough the computer networks immediately transfers files and messages to the other people which reduced transportation and communication expense. It also raises the standard of the organization because of the advanced technologies that are used in networking.

1.2.9 Remote Access and Login

Employees of different or same organization connected by the networks can access the networks by simply entering the network remote IP (Internal Protocol) or web remote IP. In this the communication gap which was present before the computer networks no more exist.

1.2.10 Flexible

Computer networks are quite flexible thay all of its topologies and networking strategies supports addition for extra components and terminals to the network. They are equally fit for large as well as small organizations.

1.2.11 Reliable

Computer networks are reliable when safety of the data is concerned. If one of the attached system collapse same data can be gathered from another system attached to the same network.

1.2.12 Data Transmission

Data is transferred at the fast speed even in the scenarios when one or two terminals machine fails to work properly. Data transmission in seldom affected in the computer networks. Almost complete communication can be achieved in critical scenarios too.

1.3 Network Architecture

It is a network communication design in which the physical components of computers are arranged in a sequence so that they can communicate with each other. Network is a combination of hosts, applications, routers, hardware, software and links of media. Network architecture is a guideline and technology for designing, building and managing a network.

1.3.1 Purpose of Network Architecture

The purpose of network architecture is to provide assistance and guidance to implement high quality network. The network architecture not only helps you to deploy the network but also assists you in troubleshoot and maintaining architecture. Network architecture also helps you in security management and disaster recovery. Network architecture is composed of many layers. In the process of layering the communication tasks are divided into smaller parts, each part is further divided into sub tasks for accomplishing tasks. These subtasks interact with the other communication processes. The process of layering keeps the network design simple. There are many ways to design and set network architecture. There are many choices available to set up a network however every network must have three basic parts like network users, applications and devices. Network itself is operating at physical layer of the OSI model. The devices are operating mostly at data link layer or network layer. The application exists at the session layer of the OSI model. Lastly the user is at the last two layers of the model including presentation and application layer.

1.3.2 The Network Topologies

The network topologies play an important role in the formation of a network. Network architecture designs closely related to design of the network topology. There are many types of network topologies like star topology, bus topology, ring topology, mesh and tree topology. The choice of network topology is dependent upon the type and size of network architecture. Most commonly used network topology is mesh. However the application of topology depends upon the amount of space in which one has to establish network architecture. The network architecture which comprises of ten to twelve computers mostly is designed on using bus topology as a network. In a bus topology an array of computer terminals is connected to one after the other computer and a network is established. In order to establish larger networks Mesh topology is used. Mesh network architecture is a complex design and it involves the redundancy of interconnections attached to the routers and switches in a network.

1.3.3 Components of Network Architecture

There are six basic network architecture components such as server, proxy, client, command console, server module and core. The server is the backbone of any network. The role of servers in network architecture is to communicate with proxies and other peered servers. They are at the top layer of the network and they do not communicate directly with client. Moreover servers receive complete projects and tasks. Proxies can be termed as the focal point of the network because it facilitates the communication of the devices. Proxies usually perform buffering and they also communicate with the others of its type to share the loads of the network. The client systems are the workers of the network. They receive tasks, they interact with the users and perform user applications. Command consoles are the network guidelines which provide assistance to users about how to control the authorize network nodes. The core is the real work done in the system. The cores are verified within the network and with the clients to prevent bad cores. Server modules handle the particular tasks of the server. Server module is generally registered with the server libraries; this would help the server to perform the needed task.

1.4 Network Strategies

There are two types of network strategies. These are described below:

1.4.1 Node Connecting Strategies

Different types of networks can be characterized by the types of strategies they employ to connect computers. Three common types of relationships that exist among networks are:

- Hierarchical
- Client/server
- Peer-to-peer

1.4.1.1 Hierarchical Networks

Some networks, typically those based on mainframe computers, provide a host-to-terminal relationship between nodes. Very little processing, if any, is done by terminals, which simply enable users to enter and view information that is processed by the host. The host or primary device, initiates and manages all network communication.

1.4.1.2 Client/server Networks

Computers that perform a service on behalf of other network devices are called servers. There are several types of servers. For example, a computer that provides other network nodes with access to network storage devices is called a file server. Print servers provide other network nodes with access to network printers. Computers that use the services of a server are called clients. Networks in which servers control access to network storage and other network resources are called client/server networks.

In client/server networks, network users run programs and enter data at client stations (also called workstations). Typically (though not in all cases), the file server is reserved only for network-management functions and is not used as a workstation. Unlike the terminals used in hierarchical networks, workstations in client/server networks perform data-processing functions.

1.4.1.3 Peer-to-peer Networks

Computers that perform similar functions on a network are called peers. Networks in which no single, centralized computer controls network functions are called peer-to-peer networks. The idea of peer-to-peer networking is that each computer on the network can be both a server and a client. Users can configure their computers so that they can share directories or printers with other users on the network. Because any computer on the network can be a file server and a client concurrently, all computers are considered to have equal, or peer, status. Mixed relationships concepts, It is possible for a network to support a combination of relationships. For example, you might have a network that supports client/server and peer-to-peer access. In such an environment, a user would be able to access files and other shared resources from a file server and from another user's workstation.

1.4.2 Network Computing Strategies

Networks are sometimes also classified according to the way that processing is performed. A variety of processing schemes is possible. This section examines common network processing strategies. Networking technologies have developed over time because of the requirements of the following computing models:

1.4.2.1 Centralized Computing : It uses a large, centralized computer (mainframe) to store and organize large amounts of data. This data is entered by using local devices, or terminals. These terminals have an input device (keyboard) and some type of communications hardware so that a single mainframe could service requests from multiple remote users. With centralized computing, the mainframe provides all of the data storage and computational abilities; the terminal is simply a remote input/output device.

1.4.2.2 Distributed Computing : It uses a server, or servers, and multiple personal computers to achieve the same processing goals as a mainframe. Separate computers work on a subset of tasks without relying

on a single mainframe for processing. For example, applications designed for client/server networks are typically stored on the network. When a user runs the application from a workstation, the application is loaded into the workstation's memory. The application's processing occurs not at the server, but at the client workstations.

1.4.2.3 Collaborative Computing : It is a relatively new model and is becoming an important trend. This is a synergistic type of distributed computing where networked computers actually share processing abilities. Instead of simply communicating data between computers, collaborative computing uses the processing power of two or more computers to accomplish the same processing task.

1.5 Summary

In this unit, we have studied, the basic concepts of Computer Networks. To start, with, introduction and incurrent the basic advantage of Computer Networks like communicate, data sharing etc. After this to know the network Architecture and strategies.

1.6 Self-Assessment Questions

1. What is Computer Network?
2. What are the basic advantages of Computer Networks?
3. Which Network Strategy is best and Why?
4. Write short note on network architecture.

1.7 Reference

1. Behrouz A Forouzan, "Data communications and Networking", Fourth edition, McGraw-Hill companies, 2006.

Unit-2

Data Communications

Structure of Unit

2.0 Objective

After going through this unit, you should be able to:

- Understand the concept of Transmission Terminology
- Differentiate between Serial and Parallel communication
- Differentiate between Analog and Digital Data Transmission
- Have a broad idea about the different Transmission Impairments
- Compare the different Transmission Media and their characteristics and
- Understand Wireless Transmission and realise its importance.

2.1 Introduction

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.

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. At the very least, a communications protocol must define the following:

- Transmission media used.
- Rate of transmission (in baud or bps)
- Whether transmission is to be synchronous or asynchronous
- Whether data is to be transmitted in half-duplex or full-duplex mode

In order to understand this we need to learn about some of the basic concepts and terminologies related to data transmission, which we will be doing in this unit.

2.2 Data Communication Terminology

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.

2.2.1 Channel

In communications, the term channel refers to a path of communications between two computers or devices. A communication channel provides everything that is needed for the transfer of electronic information from one location to another. It may refer to the physical medium such as coaxial cable or to a specific carrier frequency (sub-channel) within a larger channel or a wireless medium.

The channel capacity of a transmission system is the maximum rate at which information can be transferred reliably over a given period of time.

Two basic types of channels that are used in voice and data communication. There are Analog and Digital.

The Analog type of channel transmits signals generally using sinusoidal waves as shown in figure 2.1. Non-sinusoidal waves can also be used for transmission. The commercial radio station and public telephone system are examples of this type.

The Digital type of channel transmits pulsed wave signals, such as, those shown in figure 2.2.

2.2.2 Baud

Baud is the number of signaling elements that occur each second. The term is named after J.M.E. Baudot, the inventor of the Baudot telegraph code.

At slow speeds, only one bit of information (signaling element) is encoded in each electrical change. The baud, therefore, indicates the number of bits per second that are transmitted. For example 300 baud means that 300 bits are transmitted each second (abbreviated 300 bps). Assuming asynchronous communication, which requires 10 bits per character, this translates in to 30 characters per second (cps). For slow rates (below 1,200 baud), you can divide the baud by 10 to see how many characters per second are sent.

At higher speeds, it is possible to encode more than one bit in each electrical change. 4,800 baud may allow 9,600 bits to be sent each second. At high data transfer speeds therefore data transmission rates are usually expressed in bits per second (bps) rather than baud. For example a 9,600 bps modem may operate at only 2,400 baud.

2.2.3 Bandwidth

The amount of data or signals that the transmission media can carry in a fixed amount of time is called *Bandwidth*. The Bandwidth depends upon the length, media and signaling technique used. A high bandwidth allows increased throughput and better performance. A medium that has a high capacity has a high bandwidth. A medium that has limited capacity has a low bandwidth. It is calculated using the difference between the highest and the lowest frequencies that the medium can carry. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz). Bandwidth is particularly important for I/O devices. For example, a fast disk drive can be hampered by a bus with a low bandwidth

2.3 Mode of Data Transmission

Data can be transmitted from source to destination in a number of ways.

The different modes of data transmission be outlined as follows:

• Parallel and Serial Communication.

• Asynchronous, Synchronous and Isochronous Communication.

• Simplex, Half duplex and Full duplex Communication

2.3.1 Serial and Parallel Communication

There is always a need to exchange commands, data and other control information between two communicating devices. There are mainly two options for transmitting data, commands and other control information from the sender to the receiver. These are:

• Serial communication.

• Parallel communication.

(a) Serial Communication

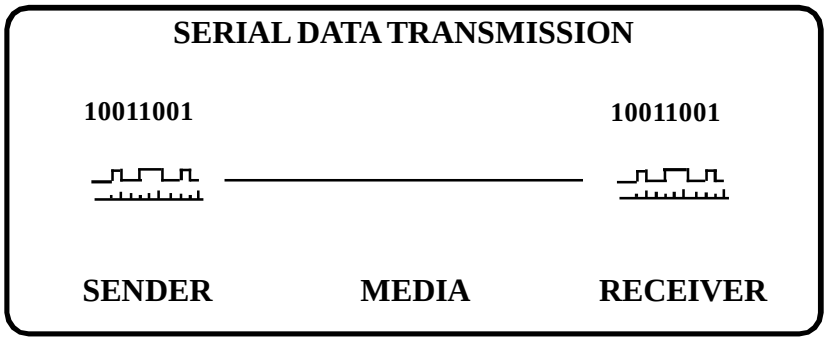


Figure 2.1 : Serial Communication

In serial data transmission, bits are transmitted serially, one after the other, as shown in figure 2.1. The Least Significant Bit (LSB) is usually transmitted first. While sending data serially, characters or bytes have to be separated and sent bit by bit. Thus, some hardware is required to convert the data from parallel to serial. At the destination, all the bits are collected, measured and put together as bytes in the memory of the destination. This requires conversion from serial to parallel.

As compared to parallel transmission, serial transmission requires only one circuit interconnecting the two devices. Therefore, serial transmission is suitable for transmission over long distances.

(b) Parallel Communication

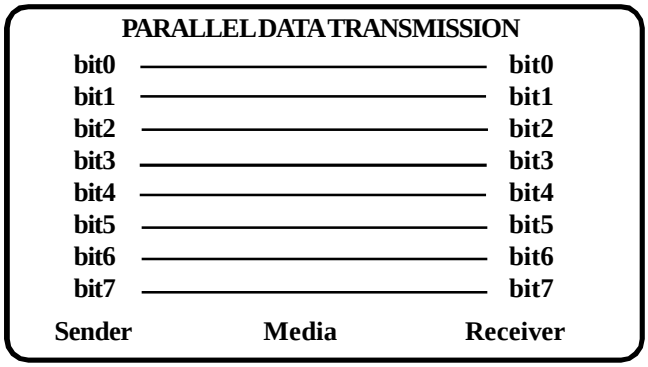


Figure 2.1 : Parallel Data Transmission

In parallel transmission, all the bits of a byte are transmitted simultaneously on separate wires as shown in the figure 2.3. Here multiple connections between the two devices are therefore, required. This is a very fast method of transmitting data from one place to another.

The disadvantage of Parallel transmission is that it is very expensive, as it requires several wires for both sending, as well as receiving equipment. Secondly, it demands extraordinary accuracy that cannot be guaranteed over long distances

2.3.2 Asynchronous, Synchronous and Isochronous Communication

One of the major difficulties in data transmission is that of synchronising the receiver (destination) with the sender (source). This is the main problem with serial communication. The receiver must be able to detect the beginning of each new character in the bit stream that is being presented to it and if it is not able to achieve this, it will not be able to interpret the incoming bit stream correctly.

The three mechanisms used for synchronisation are:

(a) Asynchronous Communication

(b) Synchronous Communication

(c) Isochronous Communication

(a) 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.

A typical frame used to transmit a character data has four components:

(i) A start bit: Signals the starting a frame and enables the receiving device to synchronise itself with the message.

(ii) Data Bits: Consists of 7 or 8 bits when character data is being transmitted.

(iii) Parity Bits: Optionally used as a crude method for detecting transmission errors.

(iv) A stop bit or bits: Signals the end of the data frame.

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.

Advantages of Asynchronous Communication

Asynchronous transmission is simple, inexpensive and is ideally suited for transmitting small frames at irregular intervals (e.g., data entry 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.

Disadvantages of Asynchronous Communication

As start, stop and parity bits must be added to each character that is to be transmitted, this adds a high overhead to transmission. This 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, hence as 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.

(b) Synchronous Communication

In synchronous communication the whole block of data bits is transferred at once, instead of one character at a time. 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.

Synchronous signals, generally utilise 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.

Serial synchronous transmission is used for high -speed communication between computers. It is used when high volumes of data are to be transmitted.

Advantages of Synchronous Communication

Synchronous transmission is more efficient because only 4 additional bytes (for start and end

frames) are required to transmit upto 64 kbits.

Synchronous transmission is not really prone to distortion, as a result, it can be used at high- speeds.

Disadvantages of Synchronous Communication

Synchronous transmission 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.

(c) Isochronous Communication

This method 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 it, 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.

Advantages of Isochronous Communication

- Isochronous transmission guarantees transmission rates, and it is almost deterministic.
- It has low overheads.
- It has high speed.

Disadvantages of Isochronous Communication

In isochronous transmission its necessary to ensure that the clocking device is fault tolerant.

2.3.3 Simplex, Half Duplex and Full Duplex Communication

This classification of data transmission is based on the which question of communication can send data and at what point of time.

The three basic ways in which this can be done are:

- *Simplex.*
- *Half Duplex*
- *Full Duplex,* sometimes called *Duplex.*

Simplex

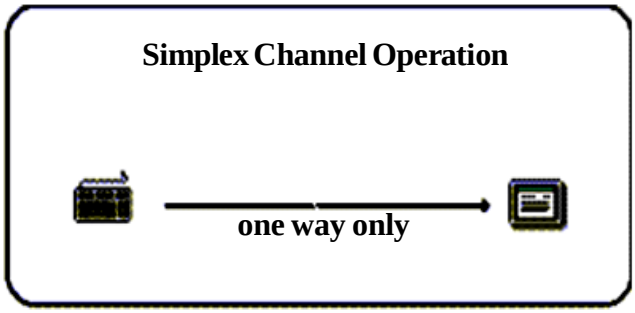


Figure 2.3: Simplex Connection

The simplest signal flow technique is the simplex configuration. In simplex transmission, one of the communicating devices can only send data, whereas the other can only receive it. Here, communication is only in one direction (unidirectional) where one party is the transmitter and the other is the receiver as shown in the figure 2.3. Examples of simplex communication are the *simple radio*, and *public broadcast television* where, you can receive data from stations but can't transmit data back. The television station sends out electromagnetic signals. The station does not expect and does not monitor for a return signal from the television set. This type of channel design is easy and inexpensive to set up.

Half Duplex

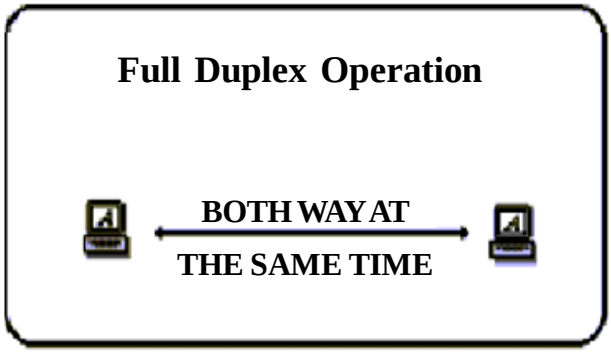


Figure 2.4: Half Duplex Connection

Half duplex refers to two- way communication where, only one party can transmit data at a time. Unlike, the simplex mode here, both devices can transmit data though, not at the same time, that is Half duplex provides simplex communication in both directions in a single channel as shown in figure 2.4. 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 turn around 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.

Note the difference between simplex and half-duplex. 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.

Most modems contain a switch that lets you select between *half-duplex* and *full-duplex* modes. The correct choice depends on which program you are using to transmit data through the modem.

Full Duplex

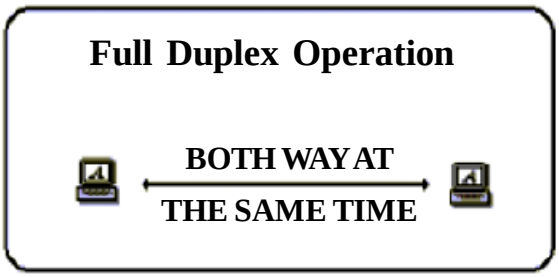


Figure 2.5: Full Duplex Connection

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 shown in figure2.5 . As you can see from figure 2.5, 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. 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.

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.

2.4 Analog and Digital Data Transmission

We know that the two major types of signals are Analog and Digital. The manner in which these two types of signals can be transmitted from source to destination is of the same two types that is ?

- *Analog data transmission.*
- *Digital data transmission.*

Analog Signal

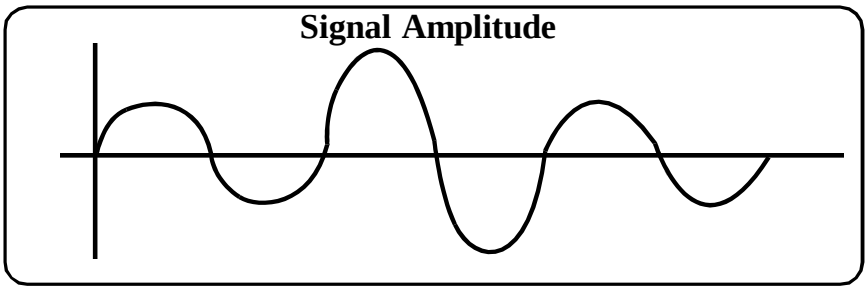


Figure 2.6 : Analog Signal

Analog signals vary constantly in one or more values; these changes in values can be used to represent data. An analog signal is continuous and can be represented by using sine waves. Human voice, video and music are all examples of analog signals, which vary in amplitude *(volume)* and frequency *(pitch).* Human voice generates an analog *(continuously varying)* signal containing multiple frequencies that is transmitted as an analog signal over the medium. Amplifiers are used to overcome the attenuation that the signal suffers on its way. The drawback is that 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 subtle 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. Third and fourth generations of audio and video recordings show marked deterioration.

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

Digital Data Transmission

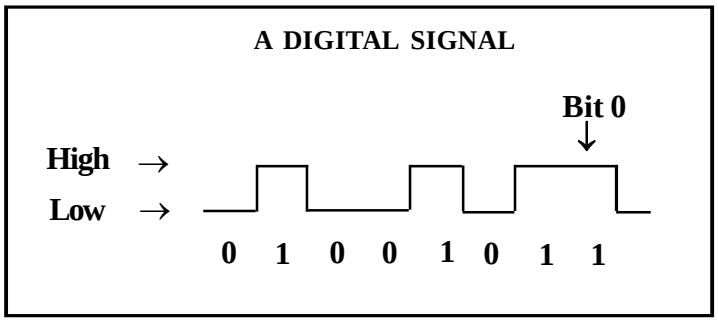


Figure 2.7: Digital Data Transmission

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. 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.

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 unrecognisable 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.

2.5 Tranmission Impairments

When data is transmitted from a transmitter to receiver, there is scope for transmission errors. If transmission media were perfect, the receiver would receive exactly the same signal that the transmitter sent. Unfortunately media are not perfect, so the received signal may sometimes not be the same as the transmitted signal.

Transmission lines suffer from three major problems:

- *Attenuation*
- *Delay distortion*
- *Noise*

2.5.1 Attenuation

Attenuation is the loss of energy as the signal propagates outwards. On guided media (e.g. wires and optical fibers) the signal falls off logarithmically with the distance. Attenuation is very small at short distances therefore, the original signal can be recognised without too much distortion. Attenuation increases with distance as some of the signal energy is absorbed by the medium. The loss is expressed in decibels per kilometer (db/km). The amount of energy lost depends on the frequency. Attenuation is also higher at higher frequencies.

If the attenuation is high, the receiver may not be able to detect the signal at all or the signal may fall below the noise level. In many cases, the attenuation properties of a medium are known, so amplifiers can be put in place to try to compensate for the frequency-dependent attenuation. This approach helps but can never restore the signal exactly back to its original shape.

2.5.2 Delay Distortion

Delay distortion is caused by the fact that the signals of varying frequencies travel at different speeds along the medium. Any complex signal can be decomposed into different sinusoidal signals of different frequencies resulting, in a frequency bandwidth for every signal.

One property of signal propagation is that the speed of travel of the frequency is the highest at the center of this bandwidth and lowest at both ends. Therefore, at the receiving end, signals with different frequencies in a given bandwidth will arrive at different times. If the signals received are measured at a specific time, they will not be exactly like the original signal resulting in its misinterpretation.

For digital data, fast components from one bit may catch up and overtake low components from the bit ahead, mixing the two bits and increasing the probability of incorrect reception.

2.5.3 Noise

Noise is unwanted energy from sources other than the transmitter. Thermal noise is caused by the random motion of the electrons in a wire and is unavoidable. Cross talk is caused by inductive coupling between two wires that are close to each other. Sometimes when talking on the telephone, you can hear another conversation in the background. That is crosstalk. Finally, there is impulse noise, caused by spikes on the power line or other causes. For digital data, impulse noise can wipe out one or more bits.

2.5.4 Concept of Delays

The average delay required to deliver a packet from source (origin) to destination has a large impact on the performance of a data network. Delay considerations strongly influence the choice and performance of network algorithms, such as routing and flow control. Because of these reasons, it is very important to understand the nature and mechanism of network delay and the manner in which it depends on the characteristics of the network.

A large delay is disastrous for data transfer. The total delay can be categorised into two types. The first type is fixed delay. This is the total delay which is always present due to buffering, link capacity etc. The second type is variable delay. This is the delay component which is caused by packets queuing in the routers, congestions etc. Among the different types of delays, here we shall discuss transmission delay and propagation delay.

Transmission delay

Transmission delay is the delay, which is present due to link capacities. When resource reservation methods are supported in routers, transmission delays can probably be kept low enough to satisfy the overall delay constraint of 200 ms.

When data is transmitted, there is always a minimal amount of delay, due to the capacity of the links along which the data travels. But the most significant part of the delay of transmission is usually due to queuing of packets inside routers. This delay is highly variable and depends both on the number of routers along the path and the load of the routers.

Propagation delay

Satellite microwave systems can reach remote places on the earth and can also communicate with mobile devices. As the signal travels a long distance *(around 36,000 km),* there is a delay of about 5 kms between, the transmission and the reception of the signal. This delay is known as the propagation delay. Such delays occur in all communication channels, however, small they may be.

Propagation delay is the time between the last bit transmitted at the head node of the link and the time the last bit is received at the tail node. This is proportional to the physical distance between the transmitter and the receiver; it can be relatively substantial, particularly for a satellite link or a very high-speed link.

The propagation delay depends on the physical characteristics of the link and is independent of the traffic carried by the link.

2.6 Summary

• In this unit, we have studied, the basic concepts of data transmission.

• To start with, we discussed the basic terms that are frequently used in data transmission like bandwidth, frequency, channel, baud etc.

• After this to know how data can be transmitted from the source to the destination and the different modes of data transmission.

• We also discussed the two major types of signals that is *analog* and *digital* and, the manner in which these two types of signals can be transmitted from the source to the destination and finally disurrneged about transimission impairments.

2.7 Self-Assessment Questions

1. What is data communication?
2. What is the difference between half-duplex and full duplex transmission modes?
3. What are some of the factors that determine in data communication terminology?
4. Categorize the hour basic impairments in term of data communication.
5. What is the difference between synchronous and Asynchronous data transmission modes?

2.8 References

1. Behrouz A forouzan, "Data communications and Networking", The Mc-Grow-Hill, Fourth Edition, 2006.

Unit-3

Bandwidth Utilziation

Structure of Unit

3.0 Objective

On completion of this unit, we will be able to:

- Define Bandwidth.
- Know channel, channel bandwidth, digital signals, bit interval, bit rate and band rate, which will help you in understanding the bandwidth utilization.
- Specify some of the multiplexiy like FDM, TDM & WDM.

3.1 Indtroduction

The data is generally in the form of pulses and pulse is a composite signal which contains may frequencies. Here, note that the peculiar shape of a pulse is due to the sum of specific frequencies at specific amplitudes and phases. If there is any change in the amplitudes or phases of these frequency components, then the shape of the pulse will not remain the same.

3.2 Medium (Channel)

The signal always travels over some medium or channel. The medium can be a coaxial cable or optical fiber etc. a medium does not pass all frequencies equally. It may pass some frequencies and weaken or block the other frequencies. Hence, when a composite signal is passed over such a transmission medium, at the receiving end, we get a wave, having a different shape as shown in figure 3.1.

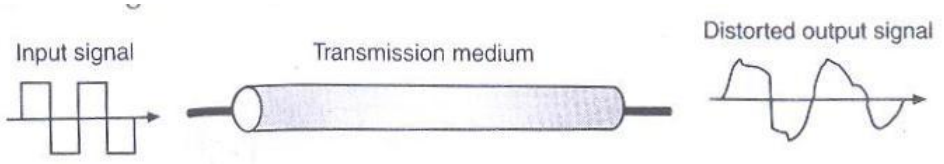


Figure 3.1 : Signal distortion on a transmission medium.

To avoid the signal distortion, the medium must pass all the frequencies present at the input without any change. However, no medium is perfect and hence some signal distortion always takes place.

3.3 Channel Bandwidth

The range of frequencies that contain the information is called as the *bandwidth*. However, the term channel bandwidth is used to describe the range of frequencies required to transmit the desired information. As an example, the *Amplitude Modulation* (AM) system requires a channel bandwidth of 10kHz to transmit a signal of 5kHz bandwidth. But the signal sideband system (SSB) only 5 kHz channel bandwidth to transmit the same signal. Actually, the efforts must be made to reduce the required channel bandwidth so that we can accommodate in more number of channels in the same available EM spectrum.

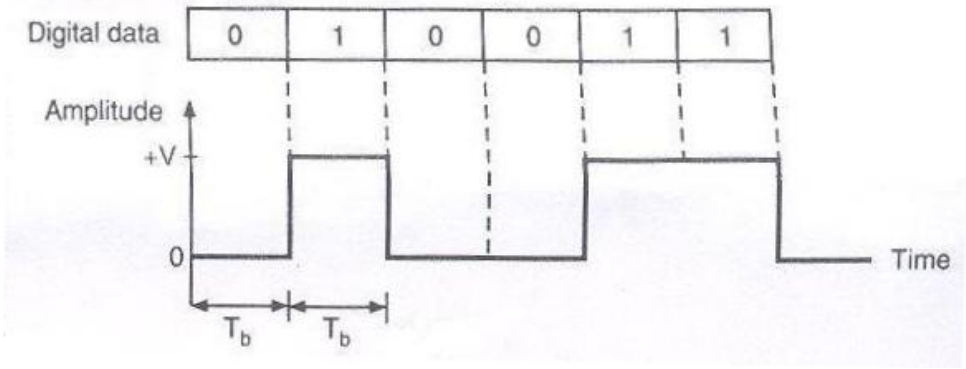


Figure 3.2 : Digital Signal.

3.4 Digital Signals

The data can also be represented by a digital signal. A digital signal is a discrete time signal having finite number of amplitudes. For example, let us consider he digital signal shown in figure 3.2. Here 0 is represented by zero volts and a 1 by some positive voltage.

3.5 Bit Interval

The bit interval is the time required to send one signal bit. As shown in figure 3.3 the time required to send a 0 or 1 is Tb which is the bit interval.

3.6 Bit Rate (Data Rate)

Bit rate is the number of bits transmitted or sent in one second. It is expressed in bits per send (bps). Relation between bit rate and bit interval may be expressed as under :

$$\text{Bit Rate} = \frac{1}{\text{Bit interval}}$$

Bit rate or significant rate is defined as the number of bits which can be transmitted in second. Ifthe bit duration is Tb1 then bit rate will be 1/ Tb. Let us consider figure 3.3. Here, we observe that the bit duration is necessarily equal to the pulse duration. In figure 3.3 the first pulse is of two bit duration.

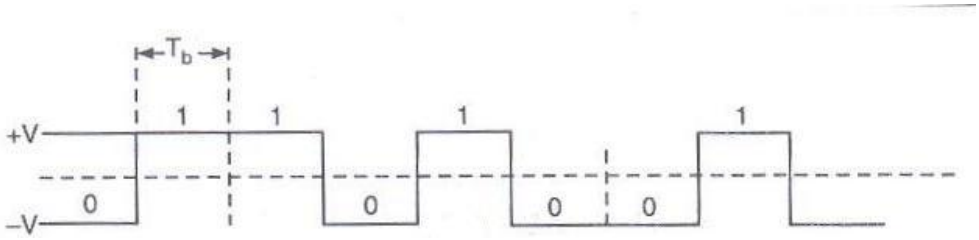


Figure 3.3 : A bit stream.

Bit rate also called as signaling rate and it must be as high as possible. However, with increase in bit rate, the bandwidth of transmission medium must be increased, in order to transmit the signal without any distortion.

3.7 Bauds (or Baud Rate)

Baud is the unit of signaling speed or modulation rate or the rate of symbol transmission. It indicates the rate at which a signal level changes over a given period of time. When binary bits are transmitted as an electrical signal with two levels 0 and 1, the bit rate and the modulation rate i.e., baud rate are same. This has been shown in figure 3.4.

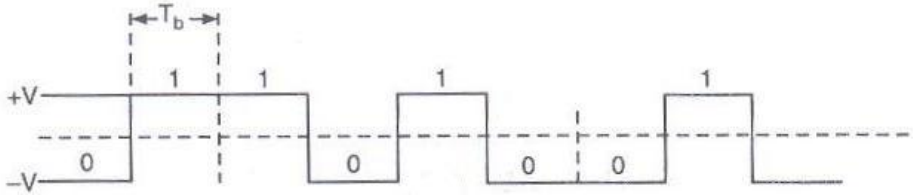


Figure 3.4 : Baud rate for two level modulation.

Here, it may be noted that for a two level signal, (binary signal) the bit rate and bauds are equal. Now, let us consider figure 3.5 where four different levels are used to represent the data.

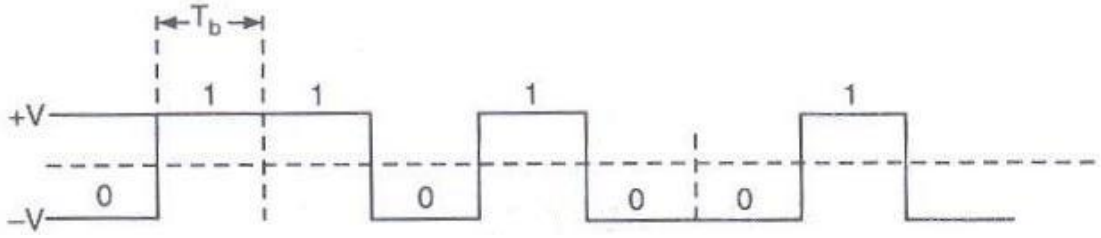


Figure 3.5 : Baud rate for a four level modulation.

Each level is being represented by a combination of two bits i.e. 00 or 01 etc. the bit rate is therefore not equal to the baud rate. The bit rate is 8 bits/sec, but, baud rate is only 4 bauds as there are 4-levels per second.

EXAMPLE 3.1 For a binary PCM system, the number of bits per transmitted word is 8 and the sampling frequency fs = 8 kHz. Calculate the bit rate and baud rate.

•Differentiate between bit rate and baud rate a modem constellation diagram has data point at coordinates : (1,1) (1,-1) (-1,1) and (-1,-1). How may bps can a modem with these parameters achieve at 1200 baud?

Solution: Given that N = 8, fs = 8 kHz

We have bit rate = N x fs = 8 x 8 kHz = 64 k bits/sec.

Boud rate = Bit rate = 64 kHz (since transmission is binary) Ans.

EXAMPLE 3.2 For the same data as in previous example, find the bit rate and baud rate if a QPSK system is used.

Solution: In a QPSK system, two successive bits are clubbed together to form one message. Hence, one symbol corresponds to 2 bit duration.

$$\text{Therefore, baud rate} = \frac{1}{2} \text{ x bit rate} = 32 \text{ k bits/sec.} \quad \text{Ans.}$$

EXAMPLE 3.3 A system sends a signal that can assume 8 different voltage levels. It sends 400 of these signals per second. What are the baud and bit rates?

Solution:

(i)As the signal assumes 8 different voltage levels, we required 3 bit digital signal to have 8 different combinations. Hence, the number of bit; per voltage level is 3. let each voltage level represent one symbol.

(ii)The system sends 400 signal/sec. Hence, the number of symbols transmitted per second is also 400.

Therefore, symbol rate = Number of symbols/sec.

= 400 symbols/sec.

(iii)The baud rate is define as the number of symbols per second.

Hence, Baud rate = Symbol rate.

or Baud rate = 400 symbols/sec.

(iv)We are using 3 bit to represent each symbol.

Therefore, bit rate = 3 x symbol rate = 3 x 400

= 1200 bits/sex Ans.

3.8 Multiplexing

1. Basic Concepts

The cost of maintenance of a high bandwidth trunk and a low bandwidth trunk is same. Hence telephone companies have developed elaborate schemes for multiplexing many lines into a signal physical trunk.

The multiplexing techniques used are as under :

(i) Frequency of Division Multiplexing (FDM)

(ii) Wavelength Division Multiplexing (WDM)

(iii) Time Division Multiplexing (TDM)

The multiplexing techniques can be broadly classified into two categories namely analog and digital. Analog multiplexing can be either FDM or WDM and digital multiplexing is TDM. Figure 3.6 shows the classification of multiplexing techniques.

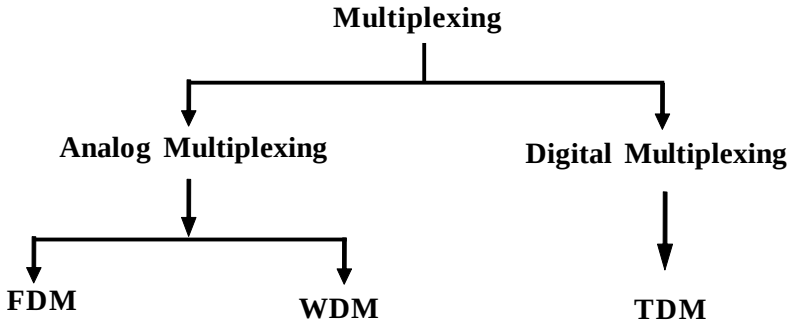


Figure. 3.6 : Classification of multiplexing techniques.

Generally, the FDM and WDM systems are used to deal with analog information whereas the TDM systems are used to handle the digital information.

In FDM, many signals are transmitted at a time, instead, they are transmitted in different time slots.

3.8.1 Frequency Division Multiplexing (FDM)

The FDM is based on the concept of sharing bandwidth of a common communication channel. The signal which are to be transmitted simultaneously will each modulate a separate carrier. The modulation can be AM, SSB, FM or PM. The modulated signals are then added together to form a complex signal which is transmitted over a signal channel.

Figure 3.7 shows the spectrum of FDM signal.

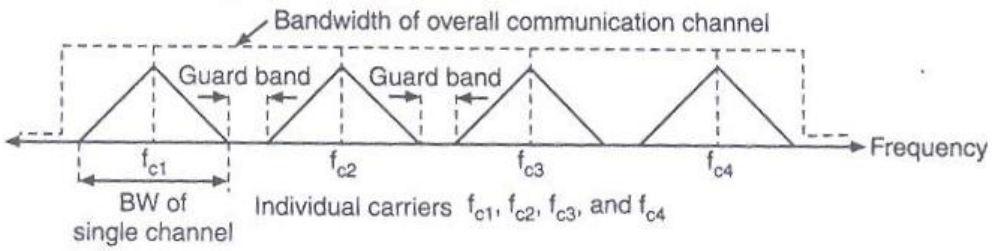


Fig. 3.7 Spectrum of FDM signal.

The guard bands are provided between the adjacent channel as shown in figure 3.7, in order to avoid the interference between them.

(i) A large number of signals (channels) can be transmitted simultaneously.

(ii) FDM does not need synchronization between its transmitter and receiver for proper operation.

(iii) Demodulation of FDM is easy.

(iv) Due to slow narrow band fading, only a signal channel gets affected.

(v) The communication channel must have a very large bandwidth.

(vi) Intermediation distortion takes place.

(vii) Large number of modulators and filters are required.

(viii) FDM suffers from the problem of crosstalk.

(ix) All the FDM channels get affected due to wideband fading.

Some of the important applications of FDM may be listed as under :

(i) Telephone systems.

(ii) AM *(Amplitude Modulation)* and FM *(Frequency Modulation)* ratio broadcasting.

(iii) TV broadcasting.

(iv) First generation of cellular phones used FDM

3.8.2 Wavelength Division Multiplexing (WDM)

WDM is the variation of FDM, for fiber optic channels.

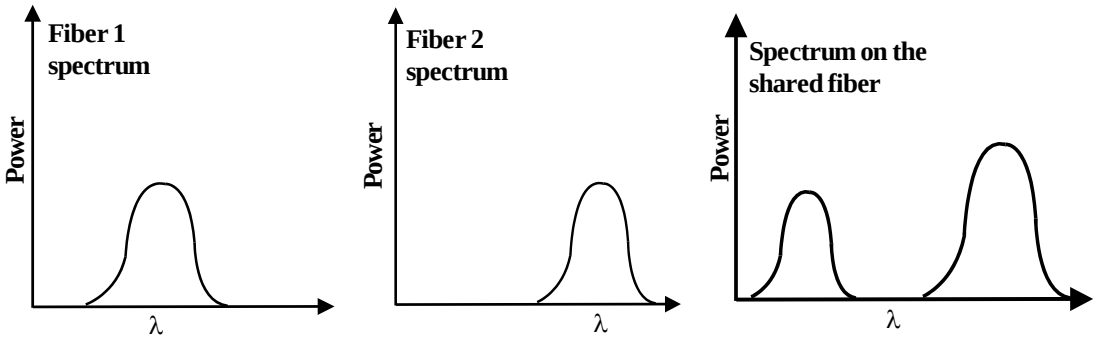


Figure 3.8 : Wavelength Division Multiplesing

As shown in figure 3.8 , 2 fibers come together at a prism, each having energy in a different band. After passing through the prism, beams are combined onto a single shared fiber, for transmission to a distant destination, where they are split again.

Channels having different frequency ranges can be multiplexed on a long fiber. The only difference with electrical FDM is that an optical system is completely passive and thus highly reliable.

Reason WDM is popular, is that the energy on a single fiber is a few gigahertz wide because it is impossible to convert between electrical and optical media any faster. Since BW of a single fiber band is about 25000 GHz, there is grate potential for multiplexing many channels together over long routes. Necessary condition is that incoming channels use different frequency.

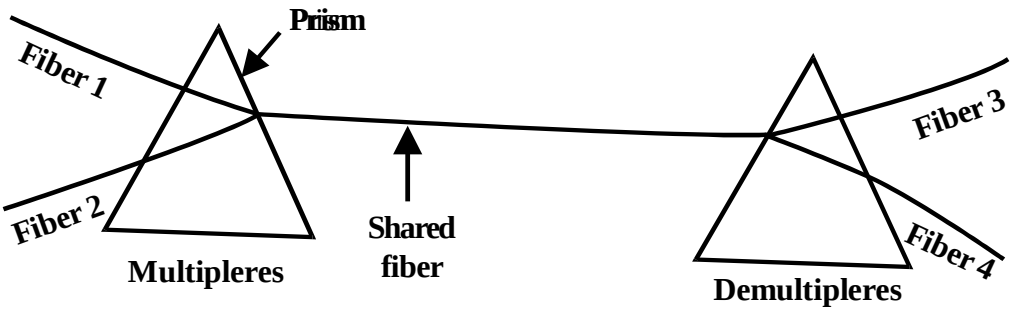


Figure 3.9 : Fixed Wavelength System

Potential application of WDM is in the FTTC (Fiber to The Curb) systems. In figure 3.9, we have a fixed wavelength system bits from fiber 1 go fiber 3 and bits from fiber 2 go to fiber 4. It is not possible to have bits go from fiber to fiber 4. It is also possible to build WDM systems that are switched, which contain many input and output fibers, switching data among themselves. Although spreading energy over n outputs dilutes it by a factor n1 such systems are practical for hundred of channels. If light from one of the incoming fibers have to go to any output fiber, all the output fibers need tunable filters.

Alternatively, input fibers could be tunable and output ones fixed. Having both to be tunable is unnecessary expense. A simple block diagram of WDM transmitter and receiver system with different channels has been shown in figure 3.10

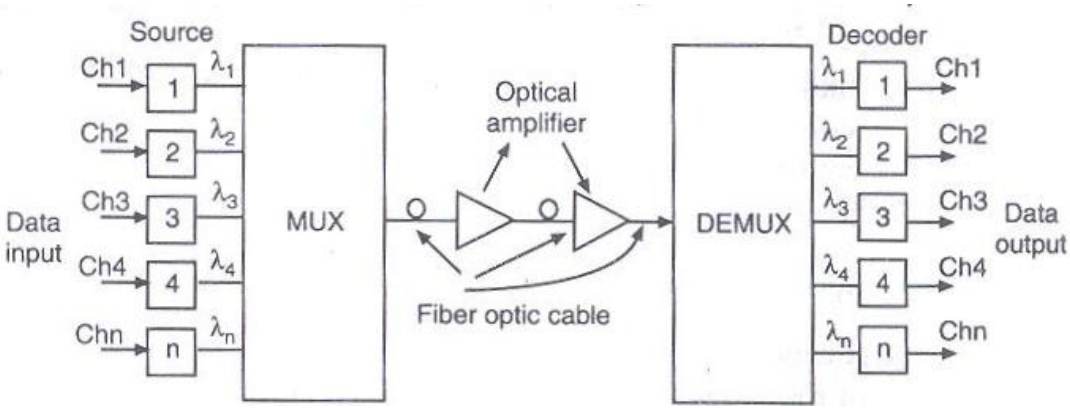


Figure 3.10 : WDM System.

One important application of WDM is the SONET network in which multiple optical fiber lines are multiplexed and demultiplexed. The long form of DWDM is dense WDM. It can multiplex a very large number of channels. The spacing between adjacent channels is small. Efficiency of DWDM is higher than that of WDM.

3.8.3 Time Division Multiplexing (TDM)

The process called *multiplexing* is used in order to utilize common transmission channel or medium to transmit more than one signal simultaneously. Two methods which are generally employed are Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM).

In TDM, all the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one. Thus, each signal will be transmitted for a very short time. One cycle or frame is said to be completed when all the signals are transmitted once on the transmission channel. The TDM principle is illustrated in figure 3.11.

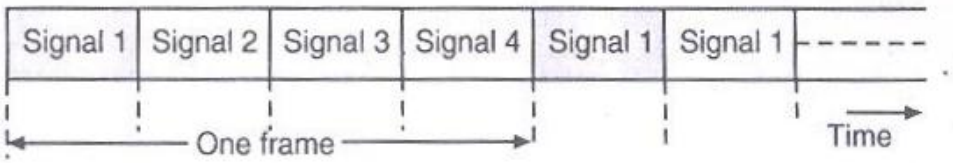


Figure 3.11 : Principle of TDM.

As shown in figure 3.11, one transmission of each channel completes one cycle of operation called as a *frame*. The TDM system can be used to multiplex analog or digital signals, however, it is more suitable for the digital signal multiplexing. The concept of TDM will be more obvious by considering figure 3.12.

The data flow of each source *(A, B or C)* is divided into units *(say A1, A2 or B1, C1 etc.)*. Then, one unit from each source is taken and combined to form one frame. The size of each unit such as A1, B1 etc. can be 1 bit or several bits.

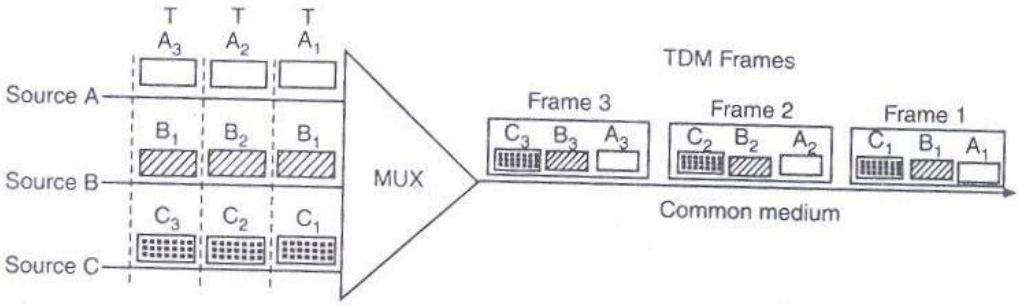


Figure 3.12 : TDN System

Figure 3.13 shows the frames of TDM signal. For 3 inputs being multiplexed, a frame of TDM will consist of 3 units i.e. one unit from each source. Similarly for n number of inputs.

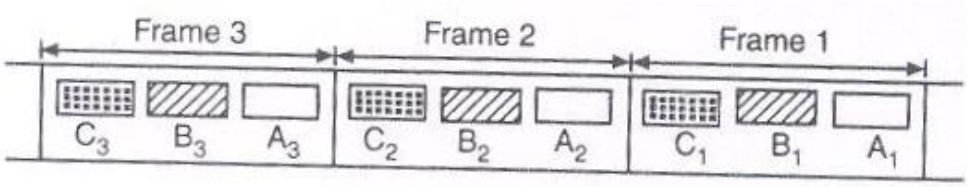


Figure 3.13 : TDM Frames

The TDM signal in the form of frames is transmitted on the common communication medium.

For TDM, the data rate of the multiplexed signal is always n times the data rate of individual sources, where n is the number of sources. Hence, if three sources are being multiplexed, then the data rate of the TDM signal is three times higher than the individual data rate. Naturally the duration of every unit *(A1 or B1 etc)* in TDM signal is n times shorter than the unit duration before multiplexing.

(i) Full available channel bandwidth can be utilized for each channel.

(ii) Intermediation distortion is absent.

(iii) TDM circuitry is not very complex

(iv) The problem of crosstalk is not severe

(v) Synchronization is essential for proper operation.

(vi) Due to slow narrow band fading, all the TDM channels may get wiped out.

Till now, we have assumed that the data rate of all the channels is the same. However, practically it will not be so. We will have to multiplex channels having different data rates. The data rates are not integer multiples of each other. But in order to multiplex them using TDM, they need to be integer multiples of each other. This can be achieved by a technique called bit padding. In the bit padding technique, the multiplexer adds extra bits to the bit stream of a source so as to force the integer relationship between all the sources to be multiplexed.

For example, if the bit rate of one source is 2.5 times the bit rate of the other source, then by using the bit padding, we can make it 4 times the bit rate of the other. These extra bits, however, do into contain any information. Therefore, they are discarded by the demultiplexer.

3.9 Summary

- Media are what the message is transmitted over.
- The signal always travels over some medium or channel.
- The range of frequencies is called bandwidth.
- Digital signals are represented in 0s and 1s.

3.10 Self-Assessment Questions

1. Define analog & digital Signals.
2. Define Channel and Channel bandwidth.
3. What is difference between bit rate and bandrate?
4. What is the basic concept of WDM?

3.11 Reference

1. Behrouz A Forozan, "Data Communications and Networking", Tata Mc-Graw-Hill Publication, Fourth adition, 2006 .

Unit- 4

Transmission Media

Structure of Unit

4.0 Objective

On the completion of this unit, we will be able to Know :

- The purpose of the physical layer.
- Various physical media can be used for the actual transmission.
- We will conver transmission media, guided and unguided.
- This materiel will provide background intermation on the key transmission technologies.

4.1 Introduction

Transmission media commonly refers to the physical interface or connections between two or more computers. These connections transfer data by using electricity, radio or microwaves, or light pulses. These pulses are formed by some part of the electromagnetic spectrum because they originate from electrical currents and can be amplified or controlled by semiconductors. Since electricity can either be on or off, it makes sense that electricity be used for binary communications. *Transmission media* is what actually carries a signal from one point to another. This may include copper wiring in the case of twisted pair cable or coax cable, or electronic waves in the case of microwave or satellite transmission.

Guided media or Bounded Media

A medium such as copper wiring is referred to as bounded media because it holds electronic signals. Fiber optic cable is said to be bounded media as well because it holds light waves. Bounded media includes the following:

- *Twisted Pair*
- *Coaxial Cable (Coax)*
- *Optical Fiber or Fiber Optic Cable*

Unguided or Wireless Media

Media that do not physically constrain signals are considered to be unbounded media. Unbounded media isn't really media at all, but a signal traveling through the air using microwave, laser or satellite transmission.

- *Transmission Microwave*
- *Infrared Transmission*
- *Radio Transmission*

4.1.1 Guided or bounded Media

For guided transmission media, the transmission capacity in terms of either data rate or bandwidth depends critically on the distance and on whether the medium is point to point or multipoint, such as in LAN. The three guided media commonly used for data transmission are *twisted pair, coaxial cable* and *optical fiber.*

1. Twisted Pair Cable

Twisted pair cabling is exactly what its name implies two wires twisted around one another. The least expensive and most widely used guided transmission medium is twisted pair. TP is merely copper wires twisted in a spiral along the length of the cable. It consists of two insulated copper wires twisted around each other. A twisted consists of two insulated wires arranged in a regular spiral pattern. A wire pares acts as a single communication link. Typically, a number of these pair is bundled together into a cable by wrapping them into a tough protective sheath over larger distances; cable may contain hundred of pairs.

Figure 4.1 : Twisted Pair Cabling

Twisted pair cabling is the current popular favorite for new LAN installations. The marketplace popularity is primarily due to twisted pair's *(TP's)* low cost in proportion to its functionality. Its usage has been justified through years of implementation by phone companies to connect world together. It is the most commonly used medium in the telephone network and is the workhorse for communication with buildings. In the telephone system individual residential telephone sets are connected to the local telephone exchange, or *"end office"* by twisted wire. These are referred to a as subscriber loops. For connection to a digital data switch or digital Private Branch Exchange [PBX] within a personal computer. Data rates for such products are typically in the of the order of 10 Mbps.

The twisting tends to decrease the crosstalk interference. The wires in a pair have the thickness of from 0.4 mm to 0.9 mm.

The construction of TP is simple. Two insulated wires are twisted around one another a number of times within one meter of distance. If properly manufactured, the twists themselves fall in no consistent pattern. This is to help offset electrical disturbances which can affect TP cable such as radio frequency interference (RFI) and electromagnetic interference (EMI). These pairs of wires are then bundled together and coated to form a cable.

When the signals from one pair migrate and interfere with the signals of another pair, it is called crosstalk. To reduce crosstalk and other EMI, such as noise, the wires are twisted. Twisting allows the EMI to be distributed more evenly between the wires. Twisting cancels out electrical noise from adjacent pairs (crosstalk) and external sources.

In effect, the voltage difference between the 2 wires carries the signal, so noise, equal on both wires, cancels itself out. Because twisting is so important in maintaining prescribed bandwidth (noise lowers bandwidth), great care must be taken not to untwist the wire along its cable run.

• There are five major categories of TP cable wiring.

• Generally inexpensive and easy to install.

• By far the most common transmission medium for both analog and digital signal. It is the most common medium used for digital signaling.

Twisted pair comes in two varieties:

- *Unshielded Twisted Pair*
- *Shielded Twisted Pair*

(i) Unshielded Twisted Pair (UTP)

Unshielded Twisted Pair is ordinary telephone wire. This is the least expensive of all the transmission media commonly used for total area network and easy to work with and easy to install.

The UTP Cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate, and the greater the cost per foot.

The UTP is subjected to external electromagnetic interference including interference from nearby twisted pair and from noise generated in the environment. A way to improve the characteristic of this medium is to use shielded twisted pair.

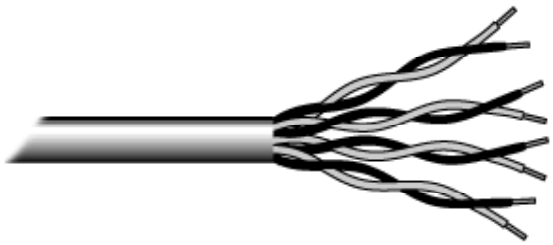


Figure 4.2 : UTP Cable

Installing UTP

Connecting UTP cable to a hardware device is accomplished by installing or "terminating" the cable ends with an RJ-45 connector. One end of the cable then plugs into the NIC and the other into a wall jack. The wall jack has cable that terminates to a 66 punch-down block. This punch-down block is then connected to a patch panel which in turn provides many RJ-45, RS-232, or RS-449 jacks. At the Patch panel, hubs, concentrators, or other devices can be connected.

Characteristics of UTP

UTP is low cost compared to other media types. It's relatively inexpensive and easy to install. It can handle data transfer rates from 1 to 100 Mbps. It rapidly attenuates when the cable run is over a few hundred meters. It is very susceptible to EMI.

• Maximum cable length is 100 meters or 328 feet (10BaseT).

Shielded twisted pair

Shielded Twisted Pair (STP) is often implemented with LocalTalk by *Apple* and by IBM's token ring systems. In the STP, the twisted pair are shielded with a metallic braid or sheathing, that reduces interference. STP is simply TP cabling with a foil or mesh wrap inside the outer coating. This special layer is designed to help offset interference problems. The shielding has to be properly grounded, otherwise it may cause serious problems for the LAN. Twisted pair cabling with no shielding is simply called *Unshielded Twisted Pair* (UTP).

This shielded twisted pair provides better performance at higher data rates. However it is more expensive and more difficult.

Connectors used with TP included RJ-11 and RJ-45 modular connectors in current use by phone companies. Uses RJ-45 telephone-type connectors (larger than telephone and consists of eight wires vs. telephone's 4 wires). Occasionally other special connectors, such as IBM's Data Connector, are used. RJ-11 connectors accommodate 4 wires or 2 twisted pairs, while RJ-45 houses 8 wires or 4 twisted pairs.

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. 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.

STP discourages EMI by encasing the twisted pair wires with a tin foil wrap that shields the wire pairs from interference.

Characteristics of STP

This cable is moderately expensive. It has to be grounded when it is installed, making installation more difficult. The capacity of STP can be up to 500 Mbps. The signal begins to attenuate at 100 m for 500 Mbps. Although STP is shielded, it still suffers from EMI, but not at the rate of UTP.

o Uses a braided copper jacket and a higher quality protective jacket.

o Less susceptible to interference and supports higher transmission rates than UTP.

TP cabling hasn't been able to support high speed data transmissions until relatively recently however. New development is focusing on achieving 100 Mbps throughput on UTP without costing the user an arm and a leg. A copper version of fiber optic's FDDI, called CDDI, will continue to mature while standardization is worked out for 100 Mbps Ethernet systems by the mid 90s. Copper cable will not allow the speeds attainable with fiber optic cable. However, the standard for fiber stipulates LAN speeds of only 100 Mbps, far below the fiber optic cable's actual capacity.

Twisted pair is grouped into certain classifications based on quality and transmission characteristics. The classifications are called *"types"* by IBM. UTP by itself is often grouped by *"grades"*.

Twisted Pair Cable Category Specifications or Types (IBM Standards)

The five major categories of TP cable are based on specifications designed by the Electronic Industries Association and the Telecommunications Industries Association (EIA/TIA). Please note that the EIA/TIA used only Unshielded Twisted Pair (UTP) when it defined the standard wiring categories for twisted-pair cables.

Category 1

Category 1 wiring is mainly used to carry voice. The CAT 1 standard was used primarily for telephone wiring prior to the early 1980s. Category 1 is not certified to carry data of any type and, in most cases, is not implemented as a cable type for data-grade wiring.

It is Voice grade telephone cable. It is Suitable for voice transmission and data transfer up to 1 Mbps. It has two pair, 22 gauge, solid conductors, braided-shield. It is traditional telephone wire that can carry voice; not data (2 pair)

Category 2

Category 2 wiring is used to carry data at rates up to 4Mbps. This type of wiring is popular for older token-based networks utilizing the 4Mbps specification of the token-passing protocol. It is rated to 1MHz.

Data grade up to 4 Mbps, four twisted pairs. It is capable of carrying data at 4 Mbps. It is Cat1 cable with additional four pairs of UTP

Category 3

Category 3 wiring is also known as voice-grade cable. It is used primarily in older Ethernet 10base-T LANs and is certified to carry data at 10Mbps. It is rated to 16MHz.

Data grade up to 10 Mbps, four pairs w/3 twists/ft (4 pair-3 twists per foot). It carries data at up to 10 Mbps. It is UTP, 22 or 24 gauge, 2 twists per foot, four pairs.

Category 4

Category 4 wiring is used primarily when implementing token-based or 10base-T/100base-T networks. CAT4 is certified at 16Mbps and consists of four twisted wires. It is rated to 20MHz.

Data grade up to 16Mbps, four twisted pairs

Category 5

Category 5 wiring is the most popular Ethernet cabling category. It is capable of carrying data at rates up to 100Mbps and is used for 100base-T and 10base-T networks. It is rated to 100MHz.

Data grade up to 100Mbps, four twisted pairs. It is Fiber optic cable used to link MAUs

2. Coaxial Cable (Coax)

Coaxial Cable is made up of two conductors that share the same axis. Coaxial cable, like twisted pair consists of two conductors but is constructed differently to permit it to operate over a wider range of frequencies. The center conductor is insulated by plastic while a second conductor, a foil wrap is covered by the external casing.

It consist of a hollow outer cylindrical conductor that surround a single inner wire conductor is held in place by either regularly spaced insulating rings or a solid dielectric material. The outer conductor is covered with a jacket or shield. A single coaxial cable has a diameter of from 1 to 2.5 cm. Because of it's shielded concentric construction, coaxial cable is much less susceptible to interference and crosstalk than is twisted pair. Coaxial cable can be used over longer distances and support more stations on a shared line than twisted pair.

Construction of coax is a little more complex then TP. It is typically composed of a copper conductor that serves as the *"core"* of the cable. This conductor is covered by a piece of insulating plastic, which is covered by a wire mesh serving as both a shield and second conductor. This second conductor is then coated by PVC or other coating. The conductor within a conductor sharing a single axis is how the name of the cable is derived.

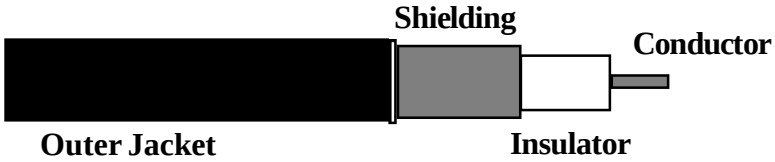


Figure 4.3 : Coaxial Cable's

Coaxial cable's construction and components make it superior to twisted pair for carrying data. It can carry data farther and faster than TP can. These characteristics improve as the size of the coax increases. There are several different types of coax used in the network world. Each has its own RG specification that governs size and impedance, the measure of a cable's resistance to an alternating current. One must be cautious in acquiring coax to make sure the right kind has been obtained. Different cable can differ widely in many important areas.

TP is less expensive than coax. In addition, TP is often already available on-site due to phone installation. TP is also extremely flexible and easy to work with, though it may not be as sturdy as coax.

Because of these factors, the current marketplace has migrated away from coax and it is no longer the "chic" cable to buy. Coax still has specific purposes, which means it won't go away, but its role as primary choice for cabling is no longer accepted in the marketplace.

Great caution should be used when selecting connectors for coax. There is standardly available about 4 different kinds of connectors.

Applications

Coaxial cable enjoys a huge installed base among LAN sites in the US. It has fit the bill perfectly for applications requiring stable transmission characteristics over fairly long distances. It has been used in ARCnet systems, Ethernet systems and is sometimes used to connect one hub device to another in other systems. This is due to coax's superior distance allowances.

All told, coax is an excellent medium for LANs, just expensive in comparison to UTP. Its wide-spread use will ensure that its existence is supported for quite some time.

Higher data rates over longer distances can be achieved with coaxial cable, and so coaxial has often been used for high speed LANs and for highly capacity long distances trunk applications.

Coaxial cable is perhaps the most versatile transmission and is enjoying widespread use of a wide variety of applications. The most important of these are as follows:

- Television distribution
- Long-distance telephone transmission
- Short-run computer system links
- Local area networks

Coaxial cable has traditionally been an important part of the long distance telephone network. Using frequently division multiplexing a coaxial cable can carry over 10,000 voice channels simultaneously.

For long distance transmission of analog signals, amplifiers are needed every few kilometers with closer spacing required if higher frequencies are used.

Common Coaxial Cable Types Used in Networking

Some common coaxial cable types are:

Type	Common Usage	Impedance	Name
RG-8	Thick Ethernet	50 ohms	10Base5 (Ethernet)
RG-11	Broadband LANs	75 ohms	Simple cable
RG-58	Thin Ethernet	50 ohms	10Base5 (Ethernet)
RG-59	Television	75 ohms	Cable TV
RG-62	ARCnet	93 ohms	ARCnet

Coax Characteristics

- Coax consists of a solid or stranded copper core surrounded by insulation, a braided shield and an insulating jacket
- Braided shield prevents noise and crosstalk. Hence Coax is fairly resistant to EMI and attenuation than twisted pair cabling
- It is bulky to handle and relatively expensive than TP

- Coax carries baseband or broadband signals
- With baseband, the cable carries a single signal at one time
- With broadband, multiple signals are multiplexed on to the wire or rather the multiple signals are forced onto it at different frequencies
- Broadband is sometimes used as a backbone cable to carry heavy traffic loads
- Both thin and thick cables can use BNC connectors, tees and terminators
- Plenum graded cable can be used in false ceilings of office space
- Can transmit data, voice and video
- Offers moderate security

3. Optic Fiber Cable (OFC)

OFC is a technology that uses glass threads to transmit data. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves.

Fiber consists of thin strands of glass or high grade plastic surrounded by a protective cladding and durable outer sheath. Light pulses are sent through the cable as on and off signals. The light signals are coded and decoded by equipment that converts the electrical on and off pulses to and from the light signals. The light is converted to electrical signals using photo diodes.

The glass core of a fiber optic cable is surrounded by and bound to a glass tube called "cladding". Cladding adds strength to the cable while disallowing any stray light wave from leaving the central core. This cladding is then surrounded by a plastic or PVC outer jacket which provides additional strength and protection for the innards. Some fiber optic cables incorporate Kevlar fibers for added strength and durability. Kevlar is the stuff of which bullet-proof vests are made, so it's tough.

An optical fiber cable has a cylindrical shape and consists of three concentric sections the core, the cladding and the jacket. The core is the inner most section and consists of one or more very thin strands of fiber, made of glass or plastic. The core has a diameter in the range of 8 to 100 um. Each fiber is surrounded by its own cladding, a glass or plastic coating that has optical properties difficult from those of the core.

Carrying data at dizzying speeds, fiber has come into its own as the premier bounded media for high speed LAN use. Because of fiber's formidable expense, however, we're not likely to see it at the local workstation any time real soon. Instead, fiber is used to link vital components (like file servers) in a LAN or multi-LAN environment together.

Fiber optic is unsophisticated in its structure, but expensive in its manufacture. The crucial element for fiber is glass that makes up the core of the cabling. The glass fibers may be only a few microns thick or bundled to produce something more sizable.

There are two kinds of fiber optic cable commercially available.

a. Single-mode Optical Fiber.

b. Multimode Optical Fiber.

a. Single Mode cable is a single stand of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission. Single Mode Fiber has relatively narrow diameter and carries higher bandwidth than multimode fiber. It provides higher transmission rate and up to 50 times more distance than multimode, but it also costs more.

b. Multimode cable is made of of glass fibers, with common diameters in the 50-to-100 micron range for the light carry component. Multimode fiber gives high bandwidth at high speeds over medium distances. It is cheaper than that of the single mode optical fiber.

Single mode is used in the telecommunications industry by companies like AT&T or US Sprint to carry huge volumes of voice data. Multimode is what we use in the LAN world.

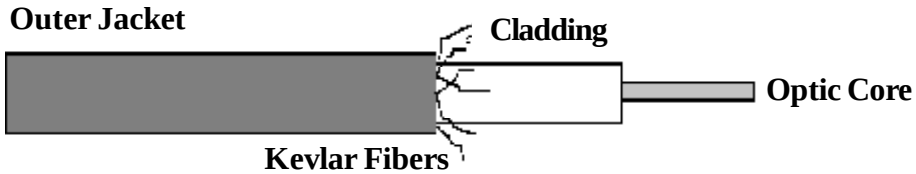


Figure 4.4 : Fiber Optic Cable

Fiber Optic is lightweight and is utilized often with LEDs (Light-Emitting Diodes) and ILDs (Injection Laser Diodes). Since it contains no metal, it is not susceptible to problems that copper wiring encounters like RFI and EMI. Plus, fiber optic is extremely difficult to tap, so security is not a real issue.

Light Source of Optical Fiber

The light source of fiber cable may be either a Light-Emitting Diode (LED) or an Injection Laser Diode (ILD). Single-mode fiber generally uses LEDs as the light-generating device, whereas multimode uses ILDs.

(a) LED

An LED is a solid-state device that emits light when a current is applied to it. The data rates achieved by this type of signaling are in the range of 12.5Mbps to 25Mbps on distances from 0.5km to 1km, respectively. This light source is considered very weak when compared to a true laser.

(b) ILD

An ILD is a solid-state device that produces a very intense beam of light over a very narrow bandwidth. This results in higher data rates over longer distances. The data rates offered are between *25Mps* and *100Mbps* over distances up to *2km*.

The biggest hindrance to fiber is the cost. Special tools and skills are needed to work with fiber. These tools are expensive and hired skills are expensive too. The cable itself is pricey, but demand will ease that burden as more people invest in this medium. Attempts have been made to ease the cost of fiber. One solution was to create synthetic cables from plastic as opposed to glass. While this cable worked, it didn't possess near the capabilities of glass fiber optic, so its acceptance has been somewhat limited. The plastic fiber cables are constructed like glass fiber only with a plastic core and cladding.

The bandwidth or capacity of fiber is enormous in comparison with copper cabling. Multimode fiber can carry data in excess of *5 gigabits per second (that's million megabits)*. Single mode fiber used in telecommunications has a theoretical top speed in excess of *25,000 Gbps*. That much data is the equivalent of all the catalogued knowledge of man transmitted through a single small glass tube in less than 20 seconds. That's impressive.

The standard governing implementation of fiber optic in the marketplace is called the Fiber Distributed Data Interface standard or FDDI. FDDI specifies the speed of the LAN, the construction of the cable, and distance of transmission guidelines. FDDI behaves very much like token ring, only much faster. An added feature for FDDI is a backup ring in case the main ring fails. This fault tolerance along with the fault tolerance already incorporated in token ring technology makes FDDI LANs pretty resilient. One minor drawback for fiber optic LANs is that they can be difficult to layout.

Data transfer rates over fiber reach from 100 Mbps to over 2 gbps from distances of 2 to 25 Km. Since electricity is not the signal source, it is the ideal media for hazardous, high voltage, or high security environments. Most LANs use fiber of 62.5 micron in size.

Fiber Optic Characteristics

- Fiber is expensive to purchase and install
- It requires special training to terminate fiber cable
- It is fragile to handle, and the components that fiber connects to are expensive also
- Provides tremendous bandwidth for data transmissions. The cable can transfer large amounts of data with its high bandwidth
- It is immune to tapping and EMI
- Highly reliable, and very secure
- Attenuation is very low
- Good for high speed, long distance data transmission
- Its construction makes it a very durable medium
- Expensive and difficult to work with and install
- Highly reliable and highly secure
- Supports data, voice and video
- Transmission distances up to 10km are possible
- Up to 4Gbps has been demonstrated in a laboratory
- Either LED or ILD light sources can be used

Working of an OFC

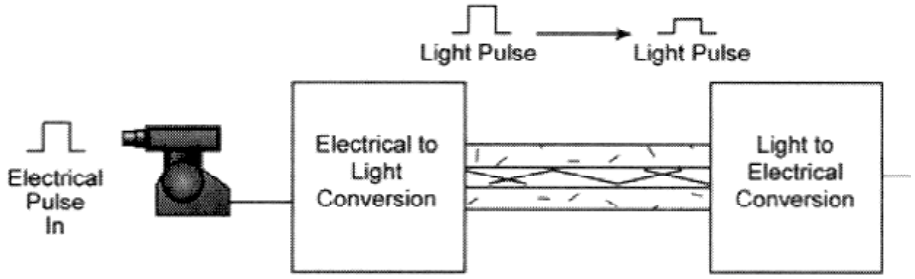


Figure 4.5 : Working of on OFC

Optical fiber are increasingly replacing other wire transmission lines in communications system Such optical fiber lines have several important advantages over other wire lines.

Various glasses and plastic can be used to make optical fiber. The lowest losses have been obtained using fiber of fused silica. Optical fiber is difficult to manufacture. Plastic fiber is evenless costly and can be used for short links, for which moderately high losses are acceptable.

The interface between the core and cladding acts as a reflector to confine light that would otherwise escape the core. The outermost layer surrounding one or a bundle of cladded fibers is the "jacket ". The jacket is composed of plastic and other material layered to protect against moisture, abrasion, crushing and other environmental dangerous.

Principle of light transmission in fiber

Propagation of light in a fiber can be understood from an analysis process called geometric ray tracing in which the paths of individual rays are geometrically traced along the guide path.

Light entering the end of the fiber at a slight angle to the axis follows a zigzag path through a series of reflection down the length of the fiber. Total internal reflection at the fiber wall can occur only if the following two conditions are met.

The first is that the glass inside the fiber core must have a slightly higher index of refraction than the index of refraction of the cladding material surrounding the fiber core.

The second condition is that the light must approach the wall with an angle of incidence $ (between the ray path and the normal to the fiber wall) that is greater than the critical angle $c which is defined as

$$\text{Sin } (\$c) = N2/N1;$$

Where:

N2, refractive index of core

N1, refractive index of cladding

Cabling Summary

Now that we've examined the major bounded media, let's take a quick look at how they compare.

Twisted Pair Cable		
S.No.	**Advantages**	**Disadvantages**
1.	Low cost, easy to install	Susceptible to RFI and EMI
2.	Often available in existing phone system	Not as durable as coax. Unsecured, worst noise immunity
3.	Well tested and easy to get	Doesn't support as high a speed as other media
Coaxial Cable		
S.No.	**Advantages**	**Disadvantages**
1	Fairly resistant to RFI and EMI	Can be effected by strong interference
2	Supports faster data rates than twisted pair on short runs	More costly than TP. Unsecured, poor noise immunity
3	More durable than TP	Bulkier and more rigid than TP
Fiber Optic Cable		
S.No.	**Advantages**	**Disadvantages**
1	Highly secure	Extremely costly in product and service
2	Not affected by RFI and EMI. Voice, data and video, fast, long distance	Difficult to install, limited to point-to-point. Sophisticated tools and methods for installation.
3	Highest bandwidth available	Complex to layout and design
4	Very durable	

4.1.2 Unguided or Wireless Media

Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.

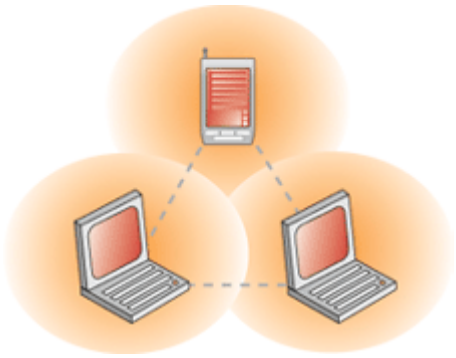


Figure 4.6 : Wireless Technology

WANs obviously make use of wireless technology to transmit data around the globe. The acceptance of wireless networks on the local level has been significantly hindered, however, for a number of reasons.

For *unguided media*, transmission and reception are achieved by means of antennae. For transmission, the antenna radiates electromagnetic energy in the medium and for reception. The antenna picks up electromagnetic waves from the surrounding medium. The wireless transmission consists of several wireless devices.

Additionally, the size of the installed base of physical wiring plays a part in unbounded local media acceptance. The United States, for instance, has a very large installed base of physical cabling. It's readily available and fast. Other countries like Japan, surprisingly enough, do not have such a large installed base. Consequently, their marketplaces are more open to the idea of wireless LANs and emerging higher speed technologies may find better acceptance there.

Another major hurdle for wireless LANs will be the standardization process. This is necessary if there is ever any hope for interoperability in the marketplace between products from different vendors. The IEEE has created a committee that will oversee this standardization. The standard will be called the 802.11 standard.

Types of wireless transmission media

Different types of wireless transmission media are following:

1. Microwave Transmission

This form of RF is a popular form for those organizations, who can afford the cost and it comes in two options:

- Terrestrial Microwave
- Satellite Microwave

(a) Terrestrial Microwave (ground-based line of sight)

The terrestrial microwave system must be in directional line of site antennas beaming signals to

each other for it to work and must be carefully planned out as to where antennas must be placed and controlling obstructions within the line of site, i.e. building being built that block the signal's path. It is regulated by the FCC, very costly, has a bandwidth of less than 1 and up to 10 Mbps, attenuates (signal fades) during rain or fog, and is highly susceptible to EMI and atmospheric conditions.

(b) Satellite Microwave

A *communication satellite* is in effect microwave relay station. It is used to link two or more ground based microwave transmitter/receivers known as *earth stations* or *ground stations*. The satellite receives transmission on one frequency band *(uplink)*, amplifies or repeats the signals and transmit it on another frequency *(down link)*. A single orbiting satellite will operate on a number of frequency bands called transponder channels or simply transponders.

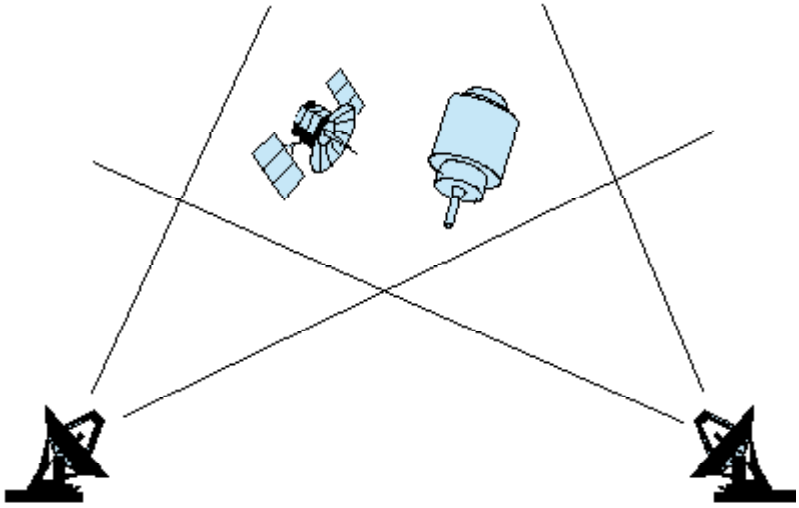


Figure 4.7 : Satellite Communication.

Satellite microwave also requires a line of site transmission, except the line is from the parabolic antennas on the ground to a geosynchronous orbiting satellite. This form of transmission is also regulated by the FCC. Owners must be aware of several factors that inhibit transmission speeds. One is propagation delay, or the time it takes to beam a signal to the satellite *23,000 miles* above earth and then back down again. Usually, this is anywhere from 1 to 5 seconds or more depending on certain factors of the setup. It too is very costly to initialize and maintain, difficult to install, has bandwidth of 1 to 10 Mbps, attenuates during atmospheric conditions, and is susceptible to EMI. Among the most important applications for satellite are the following:

(i) *Television Distribution*

(ii) *Long Distance Transmission*

(iii) *Private Business Network*

VSAT (Very Small Aperture Terminal)

Remote locations are normally inaccessible via traditional telecommunication services. A dynamic corporation constantly needs to keep in touch with its business interests wherever it may be.

VSAT facilitates reliable digital data, video and voice transmissions directly via satellite. It offers a cost-effective means of implementing a high quality, reliable communications link to widely distributed sites or isolated areas. In addition, it allows rapid, wide range of protocols and features, providing

extraordinary flexibility and virtually unlimited expansion capabilities, low-cost network re-configuration and expansion to meet new or unexpected business requirements.The VSAT dish is small, easily transportable and installation lead-time is much shorter compared to terrestrial links.

2. Infrared Transmission

An infrared wireless network operates by using an infrared light beam to carry the data between devices. These systems need to generate very strong signals because weak transmission signals are susceptible to interference from light sources such as windows. Transceivers must be within the line of sight of each other either directly or via reflection from a light-colored surface such as the ceiling of a room. Many of the high-end printers sold today are preconfigured to accept infrared signals. This method can transmit signals at high rates because of infrared light's high bandwidth.

Applications Infrared Transmission

This technology is becoming more and more prevalent in today's society in a variety of applications, mainly in wireless peripherals such *as mice, keyboards, speakers*, etc. We've seen it in television or VCR remote controls for years. It also has been developed to transmit data at high speeds. Using Light Emitting Diodes (LEDs) or Injection Laser Diodes (ILDs), light signals are sent to receivers in point to point or broadcast paths. In a point to point topology, the signal is highly focused on the receiver and therefore little attenuation is realized *(signals cannot be sent through opaque surfaces)*. Precise installation is paramount. Bandwidth ranges from *115 Kbps to 16 Mbps* and it is pretty resistant to EMI. It has a tendency to get more expensive the more specialized the system gets. Other than that, it is an affordable alternative. The broadcast systems work by relaxing the focus of the signal to beam to multiple receivers. It is not a high speed system as bandwidth is usually less than 1 Mbps. It is expensive, but easy to install.

Infrared technology uses the invisible portion of the light spectrum with wavelengths just a little less than those of red light. These frequencies are very high offering nice data transfer rates. Infrared transmissions offer potential for high speed data transfer but are limited by inability to penetrate walls and floors.

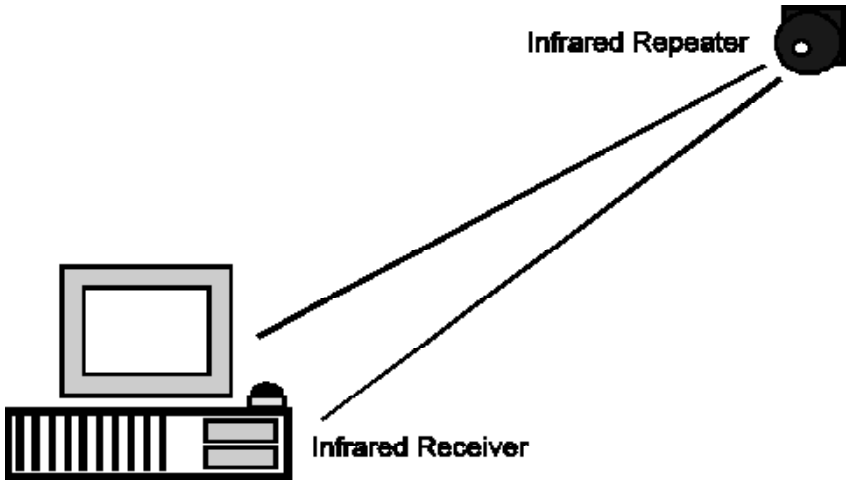


Figure 4.8 : Infrared Transmissions

Infrared technology involves the use of an infrared transmitter like an LED or ILD along with a receiver, typically a photodiode. These components operate in a line-of-sight fashion. That is, nothing can obstruct the pathway between them. Fortunately these signals can be bounced off walls and ceilings providing transmission around obstacles. Line-of-Sight means, however, that these signals cannot be broadcast through walls, severely limiting infrared LANs.

Modern infrared systems use a repeater device simply to retransmit a signal from one room into another. This device is generally mounted on the ceiling or high in a corner to alleviate as many obstacles as possible. These systems also use a process called *"diffusion"* to send the signal in a wide path across a room thus reducing the chance of signals not getting past a single obstacle.

The good news about infrared technology is that it may not be very costly to implement. Since infrared items have been around a while, significant resources exist to mass produce infrared products. Infrared transmissions now are limited to a relatively short distance, and used outdoors, are extremely susceptible to atmospheric conditions.

Types of Infrared Transmission

There are four types of infrared networks:

(i) Line of sight networks

(ii) Scatter infrared networks

(iii) Reflective network

(iv) Broadband optical telepoint

Line of sight networks

As the name implies, this version of infrared networking transmit only if the transmitter and receiver have a clear line of sight between then.

Scatter infrared networks

In this technology, broadcast transmissions are bounced off walls and ceilings and eventually hit the receiver. They are effective within an area limited to about 30.5 meters (100 feet).

Reflective network

Optical transceivers situated near the computers transmit to a common location that redirects the transmission to the appropriate computer.

Broadband optical telepoint

This infrared wireless LAN provides broadband services and is capable of handling high quality multimedia requirements that can match those provided by a cabled network.

Disadvantage of infrared transmission

While its speed and convenience are generating interest, infrared has difficulty in transmitting for distance greater than 30.5 meters. It is also subject to interference from the strong ambient light found in most business environments.

3. Radio Transmission

Radio offers superior characteristics as a wireless media but suffers from a major hindering force known as the government. The government doesn't mean to hinder radio LANs, but the Federal Communications Commission (FCC) must bridle radio for LAN use in order to responsibly manage our public airwaves, and that is, after all, what we pay them to do. Fortunately, radio LAN product manufacturers have isolated frequencies that are not licensed by the government and made use of these allowing them to scoot under the regulatory fence.

Radio transmitters are omni-directional and can easily penetrate walls, floors, ceiling and the like. Electrically speaking, the waves that are classified as radio waves have certain frequencies that are grouped together for certain uses. Some are available for data transmission, but the bandwidth necessary to per-

form high speed data transfers is not found at any given slot on the radio spectrum. Many vendors are now employing spread-spectrum technology where the available slots in the radio spectrum are all used together. Using this technology, speeds upto 2 Mbps have been achieved.

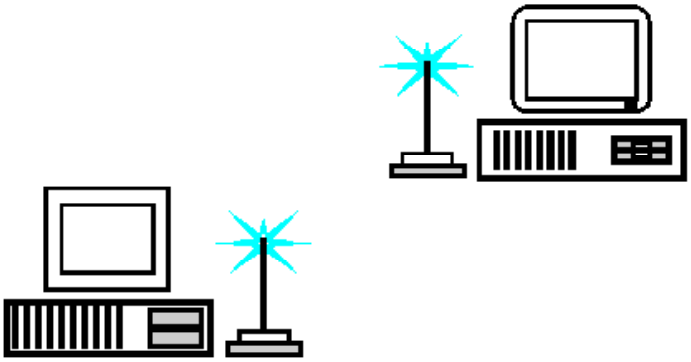


Figure 4.9 : Radio-based LANs use Portable Transmitters and Receivers at Each LAN Device

Radio based LANs have to contend with the interference that occurs daily in the workplace. That interference can come from a number of different electrical sources and can be quite impacting on LAN performance. For radio systems using only a small portion of the radio spectrum *(narrowband systems)*, this could mean that problem might be insurmountable.

The vendors of spread-spectrum products claim that their products can isolate interference problems and avoid using those frequencies.

Though radio offers portability to any node within range, its unbounded nature makes it somewhat less secure. The eavesdropper would have to, of course, know what frequency or frequencies you were using. Once that hurdle was overcome, your LAN would be laid bare.

Applications of Radio Transmissions

Radio, though limited by its speed, may be the wireless transmission method of choice for many desktops because of its low cost and capabilities.

Types of Radio Transmissions

Radio Transmissions are of following two types:

(i) Narrow-Band Radio Transmission

(ii) Spread-Spectrum Radio Transmission

(i) Narrow-Band (Single Frequency) Radio Transmission

This approach is similar to broadcasting from radio station; the user tunes both the transmitter and the receiver to a certain frequency. This does not require lines of sight focusing because the broadcast range is 3 kilo-meters. However, because the signal is high frequency, it is subject to attenuation from steel and load bearing walls.

Narrowband radio is a subscription service. The service provider handles all the Federal Communication Commissions licensing requirements. This method is relatively slow; transmission is in the 4.8 Mbps range.

(ii) Spread-spectrum (Single Frequency) Radio Transmission

Spread-Spectrum radio broadcast signals over a range of frequencies. This helps it avoid

narrowband communication problems.

The available frequencies are divided into channels, known as *hops*, which are comparable to one leg of a journey that includes intervening stops between the starting point and the destination. The spread-spectrum adapters tune into a specific hop for a predetermined length of time, after which they switch to a different hop. A hopping sequence determines the timing. The computers in the network are all synchronized to the hop timing. This type of signaling provides some built in security in that the frequency hopping algorithm of the network would have to be known in order to tap into the data stream.

To further enhance security and to keep unauthorized users from listening in to the broadcast, the sender and the receiver can encrypt the transmission.

Spread spectrum radio technology provides for a truly wireless network. For example, two or more computers equipped with spread spectrum network adapters and an operating system with built in networking capability can act as a peer to peer network with no connecting cables. In addition, such a wireless network can be tied into an existing network by adding an appropriate interface to one of the computers on that network.

Although some implementations of spread-spectrum can offer transmission speeds of 4 Mbps over distances of about 3.22 kilometers outdoors and 244 meters indoors, the typical speed of 250 Kbps makes this method much slower than the other wireless networking options discussed.

Wireless LAN Media Summary

Radio		
S.No.	**Advantages**	**Disadvantages**
1.	Transmission not line of sight	Limited bandwidth means less data throughput
2.	Inexpensive products	Some frequencies subject to FCC regulation
3.	Direct point-to-point linking to receiving station	Highly susceptible to interference
	Ideal for portable devices	

Infrared		
S.No.	**Advantages**	**Disadvantages**
1.	Higher bandwidth means superior throughput to radio	Limited in distance
2.	Inexpensive to produce	Cannot penetrate physical barriers like walls, ceilings, floors, etc.
3.	No longer limited to tight interroom line-of-sight restrictions	

The major drawback to the two major local wireless technologies - radio and infrared - has been their speed. Neither could come close to matching the 10 or 16 Mbps provided by conventional bounded media LANs. In fact, until recently, these technologies were struggling within their confines to reach out of the kbps range. Today wireless LANs are climbing out of the doldrums with comparable speeds to token ring systems. The perception that they are slow and limited is still fairly widespread, however, which will limit wireless' acceptance on the desktop.

4.2 Summary

Transmission media can be *guided* or *unguided*. The principle guided media are twished pair, coaxial cable and fiber optics. Unguided media unclude radio, microwave, intraved, and basis through the air.

4.3 Self-Assessment Questions

1. What is transmission media?
2. How do guided media differ from unguided media?
3. What is the purpose of cladding in an optical fiber?
4. What is the Significance of the twisting in twisted-pair cazle?
5. Name the two major categories of transmit ion media.
6. Name the advantages of optical fiber over twisted-pair and coaxial cazle.
7. What is the difference between STP & UTP?

4.4 References

1. Behrouz A forouzan, "Data communications and Networking", The Mc-Grow-Hill, Fourth Edition, 2006.

Unit - 5

Types of Networks-I

Structure of the Unit

5.0 Objective

This unit primarily focuses on various types of after key networks: Introduction about networks like:

- LAN, MAN and WAN.
- Different types of LANs : Ethernet, Token ring etc.
- The design and organization of the networks. However, now technology
- New network technologies.

5.1 Introduction

Since the emergence of the telephone, researchers have been looking for ways to realize and improve transmission over long distances. Ultimately, as a result of this research, computer-networking mechanisms emerged in the late 1960's. In the 1960's, smaller and more affordable computers appeared. Corporations could afford to own more than one computer. The need to interconnect them grew. This kind of network emerged in the 1960s and the 1970s.

Computer networks are changing the way we do business and the way we live. Today LANs and other networks are powerful, flexible and easy to use. In the past few years, commercial and personal use of Internet *(WWW-World Wide Web)* has increased globally along with network hosts and traffic. Today the life would become very difficult without the use of Internet or computer networking.

For a network to really benefit an organization it must be designed to meet the organizations changing communication requirements. In the last few years, Networks have gone from being an experimental technology to becoming a key business tool used by companies worldwide.

5.2 Need of Networking

By creating a network, devices like printers and scanners, software, and files and data that are stored in the system can be shared. It makes the communication among multiple computers easy.

- A network is a group of computers that are interconnected.
- Networking is the process by which two or more computers are linked together for a flawless communication.
- A network consists of two or more computers that are linked in order to share resources (e.g., printers), exchange files, or allow electronic communications.
- The computers on a network may be linked through cables, telephone lines, radio waves, satel lites, or infrared light beams.
- By computer networking the user access may be restricted when required.

5.3 Types of Networks

The types of network are categorized on the basis of the number of systems or devices that are under the networked area. Computer Networking is one of the most important wings of computing.

There are various parameters which determine whether a computer network is LAN, MAN or WAN. Fig. 5.1 shows all categories of global networks.

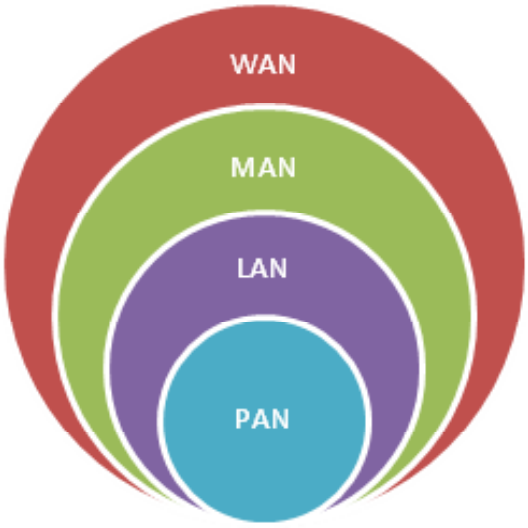


Figure 5.1 : All Global Networks

Depending upon the geographical area covered by a network, it is classified as:

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Personal Area Network (PAN)

5.3.1 Local Area Network (LAN)

As the name implies, a LAN serves a local area. LANs are privately owned networks within a building or campus covering few kilometers of area. There are various parameters which determine whether a computer network is LAN, MAN or WAN. In short, a LAN is a network which:-

- Covers small geographical area (a building or campus).
- Controlled by single organization/administration.
- Share resources within an organization and provides high speed etc.

LANs are distinguished from other kinds of networks by three characteristics, by their:

a) Size (small or large scale LANs)

b) Transmission Technology (Ethernet, Token passing)

c) Topology (Bus, Star, Ring etc.)

LANs are restricted in size. LANs may use a transmission technology consisting of a cable to which all nodes are attached. Various topologies are possible for LANs. A wide variety of LANs have been built and installed, but a few types have more recently become dominant. A leading LAN technology is called Ethernet, which was introduced by Xerox. A LAN may be connected to another LAN or to WANs and MANs using a router etc.

Characteristics of LANs

- A LAN is a network that is used for communicating among computer devices, usually within an office building or home. Fig. 5.2 shows a local area network of five computers.
- LANs enable the sharing of resources such as files or hardware devices that may be needed by multiple users within an organization.
- LANs are restricted in size, typically spanning a distance of few kilometers.
- Traditional LANs run at speeds of 10 Mbps to 100 Mbps. Newer LANs are fast operating at up to 10Gbps.
- Requires little wiring, typically a single cable connecting to each device.
- Has lower cost compared to MANs or WANs.
- LANs can be either wired or wireless. Twisted pair, coaxial or fiber optic cable can be used in wired LANs.
- Every LAN uses a protocol - a set of rules that governs how packets are configured and transmitted.
- Nodes in a LAN are linked together with a certain topology *(will be discussed in detail in chapter 6)*. These topologies mainly include: *Bus, Ring and Star.*
- LANs are capable of very high transmission rates *(10 Mbps to Gbps)*.

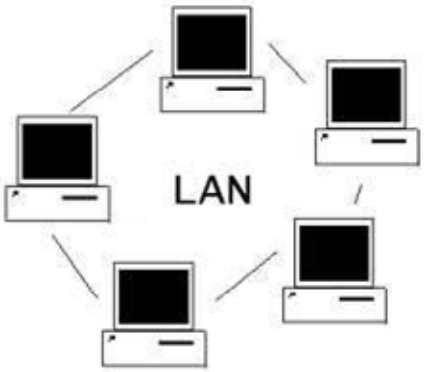


Figure 5.2 : Local Area Network

Advantages of LAN

- High Speed and their speed do not depend of the speeds of the computers that are attached to it.
- Inexpensive, reliable and easy to install and expand in size later.
- Security
- Sharing resource *(such as: printers)*

Disadvantages of LAN

- Requires Administrative Time
- File Server May Fail
- Cables May Break

5.3.2 Personal Area Network (PAN)

Characteristics of PANs

- A PAN is a network that is used for communicating among computers and computer devices (including telephones) in close proximity of around a few meters within a room.
- A PAN is a network that is meant for one person.
- It can be used for communicating between the devices themselves, or for connecting to a larger network such as the internet.
- PANs can be wired or wireless.

Example: A Bluetooth link between a laptop and a mobile/printer/computer etc. as shown in Figure 5.3.

Figure 5.3 : Personal Area Network

It can also be defined as:

"A Personal Area Network (PAN) is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body".

The devices may or may not belong to the person in question. The reach of a PAN is typically a few meters.

5.4 Types of LANs

An another classification of LANs is as following, according to which the three most common types of LAN are;

- Cable based LAN *(Ethernet, Bus, Token Ring etc.)*
- Private Branch Exchange *(PBX)*
- Hierarchical networks

5.4.1 Cable based LAN (Ethernet, Bus, Token Ring etc.)

In the cable based LAN the entire nodes are connected by cable media and signals transmitted through the cables. Any types of cable are used in LAN such as *coaxial, twisted-pair and fiber optical cable.*

LANs may use a transmission technology consisting of a cable to which all nodes are attached. Various topologies are possible for LANs. A wide variety of LANs have been built and installed, but a few types have more recently become dominant. Figure 5.6 shows few attachments.

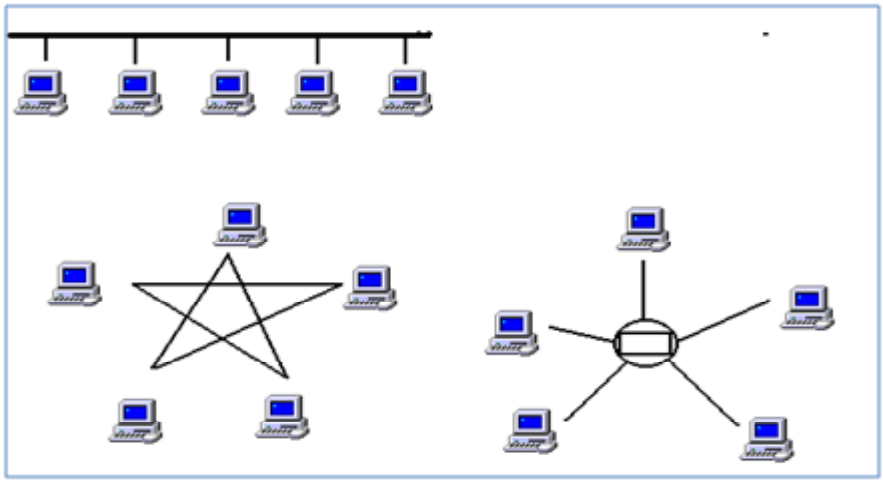


Figure 5.4 : Different Physical Arrangements of Computers in a LAN: Bus, Star and Ring

In a bus *(linear cable)* network, at any instant of time at most one machine is allowed to transmit. All others are required to wait. A mechanism is required to resolve collision when two or more machines want to transmit simultaneously. Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a random time and tries again later.

Ethernet: *Ethernet* is a protocol that controls the way data is transmitted over a local area network (LAN). It uses wires/cables. IEEE 802.3 popularly called Ethernet.

- It is a leading LAN technology, which was introduced by Xerox. Computers on an Ethernet can

transmit whenever they want to; if two or more packets collide, each computer just waits a random amount of time and tries again later.

• Ethernet is the most widely-installed local area network (LAN) technology. Specified in IEEE 802.3 standard.

• Ethernet is by far the most popular LAN protocol used today. It is so popular that if you buy a network card to install on your machine, you will get an Ethernet card, unless you ask for something different, if of course that different protocol is available

• Ethernet was originally developed by Xerox from an earlier specification called Alohanet (for the Palo Alto Research Center Aloha network) and then developed further by Xerox, DEC, and Intel.

• An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Ethernet is also used in wireless LANs. The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps.

•Devices are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.

• Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems.

• Gigabit Ethernet provides an even higher level of backbone support at 1000 megabits per second (1 gigabit or 1 billion bits per second).

• 10-Gigabit Ethernet provides up to 10 billion bits per second.

• Alternate technologies to Ethernet include the "Token Ring" protocol designed by IBM, and the far newer asynchronous transfer mode (ATM) technology. ATM allows devices to be connected over very wide distances to create WANs that behave like LANs.

Token Ring

A Token Ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages simultaneously.

• The Token Ring protocol is the second most widely-used protocol on local area networks after Ethernet.

• The IBM Token Ring protocol led to a standard version, specified as IEEE 802.5. Both protocols are used and are very similar. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second.

Very briefly, here is how it works:

(i) Empty information frames are continuously circulated on the ring.

(ii) When a computer has a message to send, it inserts a token in an empty frame *(this may consist of simply changing a 0 to a 1 in the token bit part of the frame)* and inserts a message and a destination identifier in the frame.

(iii) The frame is then examined by each successive workstation. If the workstation sees that it is the destination for the message, it copies the message from the frame and changes the token back to 0.

(iv) When the frame gets back to the originator, it sees that the token has been changed to 0 and that the message has been copied and received. It removes the message from the frame.

(v) The frame continues to circulate as an *"empty"* frame, ready to be taken by a workstation when it has a message to send.

The token scheme can also be used with bus topology LANs. The standard for the Token Ring protocol is Institute of Electrical and Electronics Engineers (IEEE) 802.5. The Fiber Distributed-Data Interface (FDDI) also uses a Token Ring protocol in its dual ring architecture.

5.4.2 Private Branch Exchange

In the private branch exchange many branches of the companies/organizations connected by telephone lines in order to form a network. It can be defined as:

"A Private Branch Exchange (PBX) is like a telephone exchange that serves a particular business or office, as opposed to one that a common carrier or telephone company operates for many businesses or for the general public". A PBX connection is shown in fig.5.5.

Figure 5.5 : PBX Connections

PBXs are also referred to as:

- PABX - private automatic branch exchange
- EPABX - electronic private automatic branch exchange

PBXs make connections among the internal telephones of a private organization-usually a business-and also connect them to the public switched telephone network (PSTN) via trunk lines. Because they incorporate telephones, fax machines, modems, and more, the general term "extension" is used to refer to any end point on the branch. PBXs are differentiated from *"key systems"* in that users of key systems manually select their own outgoing lines, while PBXs select the outgoing line automatically. Hybrid systems combine features of both.

Advantages of PBX

- The primary advantage of PBXs was cost savings on internal phone calls: handling the circuit switching locally reduced charges for local phone service.
- PBXs offer services that were not available in the operator network, such as hunt groups, call forwarding, and extension dialing etc.

In the 1960s a simulated PBX known as Centrex provided similar features from the central telephone exchange.

5.4.3 Hierarchical Network

In the hierarchical network model, data is stored in a defined hierarchy. For instance, a company is made of departments and each department has employees. So a tree like structure is created with the company at the root of the tree.

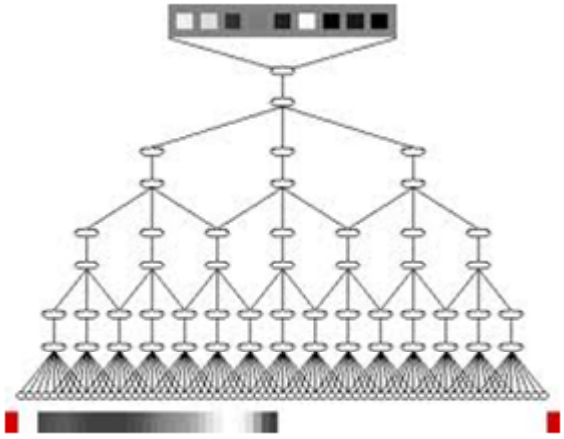


Figure 5.6 : A Hierarchical Network.

To get to all employees in the company, one would have to traverse the entire tree. In this network we may use connecting media both cable and telephone line.

5.5 Summary

• A network is a group of computers that are interconnected in order to share resources *(such as printers)*, exchange files, or allow electronic communications.

• Depending upon the geographical area covered network is classified as: LAN, MAN, WAN and PAN.

• As the name implies, a LAN serves a local area. LANs are privately owned networks within a building or campus covering few kilometers of area. LANs are restricted in size. LANs may use a transmission technology consisting of a cable to which all nodes are attached. Various topologies are possible for LANs.

• A Metropolitan Area Network (MAN) is a large computer network that usually spans a city or a large campus. Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.

• A WAN is two or more LANs connected together. It can also be defined as combination of LANs and MANs. WAN covers a large geographic area such as country, continent or even whole of the world. The world's most popular WAN is the Internet.

• A Personal Area Network (PAN) is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body.

•Cable based LAN the entire nodes are connected by cable media and signals transmitted through the cables. LANs may use a transmission technology consisting of a cable to which all nodes are attached. Various topologies are possible for LANs.

• Ethernet is a protocol that controls the way data is transmitted over a local area network (LAN).

• A Token Ring network is a Local Area Network (LAN) in which all computers are connected in a ring or star topology and a bit or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages simultaneously.

• In the private branch exchange many branches of the companies/organizations connected by telephone lines in order to form a network.

5.6 Self-Assessment Questions

1. Define Network? Explain the need of networking. What are its objectives?
2. What are the parameters that determine whether a computer network is LAN, MAN or WAN?
3. What are the characteristics of a LAN? Explain advantages and disadvantages of LANS.
4. Write short notes on
   a) MAN.
   b) WAN.
   c) PAN.
   d) PBX
   e) Unicasting, Multicasting and Broadcasting.
5. Differentiate between Client-Server model and Peer to Peer model for networking. What are the advantages of each?
6. What is Ethernet?
7. What is Token Ring?
8. Draw possible physical arrangements of a Cable based LAN.

5.7 References

1. Andrew S. Tanenbaum : "Computer Networks" Pearson Education, Third Edition, 1999.
2. Behrouz A Forouzan, "Data Communications and Networking", Mc-Grow-Hill Publication, Fourth Edition, 2006.

Unit - 6

Types of Networks-II

Structure of the Unit

6.0 Objective

- This unit will provide the infromation about followings understanding of MAN and WAN.
- What are the main traditional devices used to build networks.
- Understand the logic behind networks designing.
- Topologies used in network designing.

6.1 Introduction

When one or more than two LANS are connected with each other, a new concept of network arise known as MAN *(Metropolitan Area Network)*. These networks provide very long distances. Two or more MANs to cover very large distances can be connected and forms a Wide Area Network (WANs).

In this unit we discuss to fundamental elements of the networking. The first is network biology, the basic geometric layout of the network. The second in the hardware used in installing networks. Networks can be classified by thier topology, which is the basic geometric arrangement of the networks. The basic topologies used to layout networks are ring, bus, star and mesh, Ring, bus ans star topologies are commanly used in LANs. Star and mesh topologies are commanly used in MANs and WANs. In many cases, the networks are built using a combination of these topologies by framing a new topology called hybrid topology. To form these network topologies the diffrent networks hardware devices helps like networks cables, hub, switches, router, repearters, bridges and gateways are used. These hardware devices helps in connecting one computer mode to another network.

6.2 Metropolitan Area Network (MAN)

A MAN is a network that lies between a LAN and WAN. A MAN can also be defined as:

"A Metropolitan Area Network (MAN) is a large computer network that spans a metropolitan area or campus. Its geographic scope falls between a WAN and LAN. MANs provide Internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the Internet".

A MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks (or WAN) and the Internet. A MAN network is shown in Figure 6.1.

The IEEE 802 standard describes a MAN as:

A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings/campus to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking of local networks.

Characteristics

- A Metropolitan Area Network (MAN) is a large computer network that usually spans a city or a large campus.
- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.

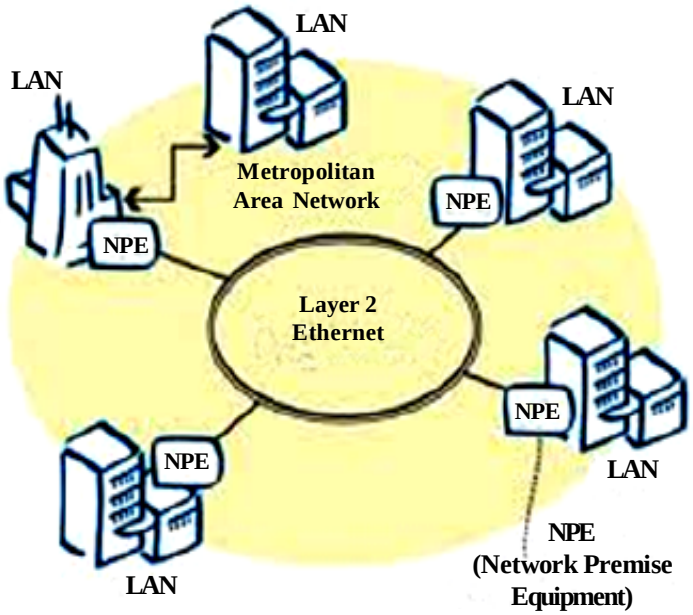


Figure 6.1 : Metropolitan Area Network.

- A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- A MAN often acts as a high speed network to allow sharing of regional resources.
- A MAN typically covers an area of between 5 and 50 km diameter.
- *Examples of MAN*: Telephone company network that provides a high speed DSL to customers and cable TV network. A MAN network is shown in figure 6.1.
- A MAN can be defined as a network of networks.

6.3 Wide Area Network (WAN)

A Wide Area Network (WAN) is a telecommunication network that covers a broad area *(i.e., any network that links across metropolitan, regional, or national boundaries)*. Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations. In essence this mode of telecommunication allows a business to effectively carry out its daily function regardless of location. This is in contrast with Personal Area Networks (PANs), Local Area Networks (LANs), or Metropolitan Area Networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area *(e.g a city)* respectively. In figure 6.2 a WAN connection is shown.

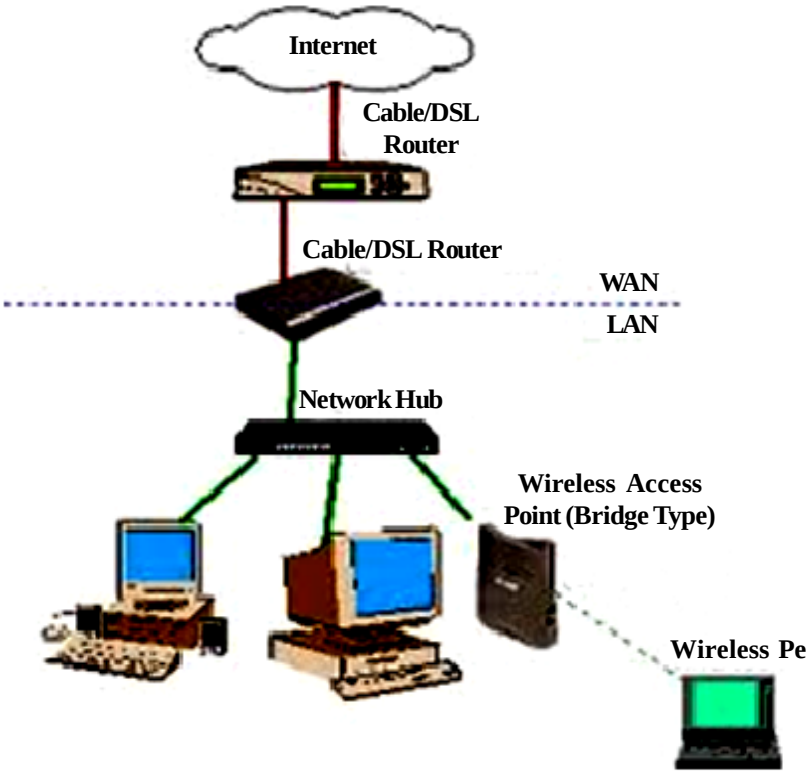


Figure 6.2 : How LAN or MAN Connected to WAN.

Characteristics

A WAN can be seen as a network of networks.

- WAN covers a large geographic area such as country, continent or even whole of the world.
- A WAN is two or more LANs connected together. It can also be defined as combination of LANs and MANs as shown in figure 6.3.

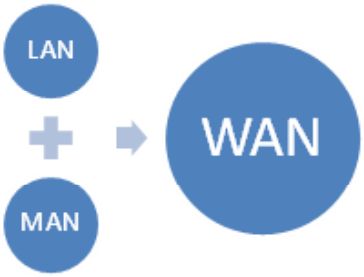


Figure 6.3 : WAN: Combination of LANs and WANs.

• To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.

• Multiple LANs can be connected together using devices such as *bridges, routers, or gateways,* which enable them to share data.

• The world's most popular WAN as shown in figure 6.4 is the Internet.

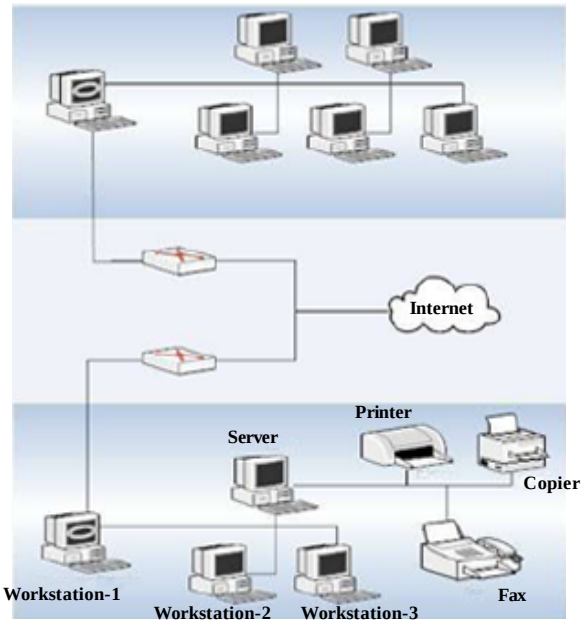


Figure 6.4 : A Wide Area Network

6.4 Network Topology

Topology refers to the Physical and logical arrangements of network nodes.

• The physical topology of a network refers to the configuration of cables, computers, and other peripherals.

• Logical refers to the way in which the network appears to the devices that use it. Logical topologies are often closely associated with Media Access Control methods and protocols.

Different Types of Topologies

There are five basic topologies used to interconnect devices: *bus, ring, star, and mesh and tree*. A hybrid approach may use combination of these topologies.

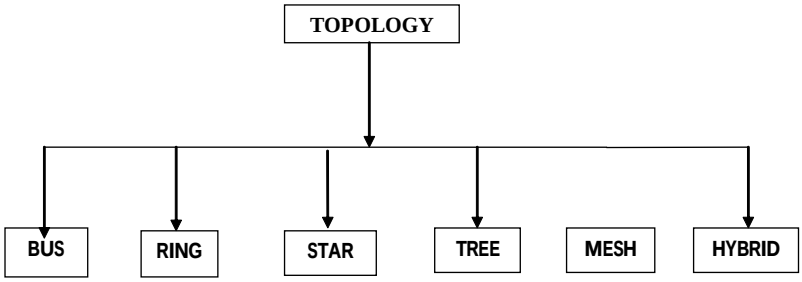


Figure 6.6 : Network Topologies

As shown in the figure 6.6 various network topologies are:-

(i) Bus Topology

(ii) Ring Topology

(iii) Star Topology

(iv) Mesh Topology

(v) Tree Topology

(vi) Hybrid Topology

6.4.1 Bus Topology

• In bus topology all the nodes *(file server, workstations, and peripherals)* are connected by a single cable.

• A bus topology consists of a main run of cable with a terminator at each end. All nodes *(file server, workstations, and peripherals)* are connected to the linear cable.

• Popular on LANs because they are inexpensive and easy to install.

• Uses a trunk or backbone to which all of the computers on the network connect. Systems connect to this backbone using T connectors or taps. Coaxial cables *(10Base-2, 10Base-5 and 100Base-T etc.)* may be used.

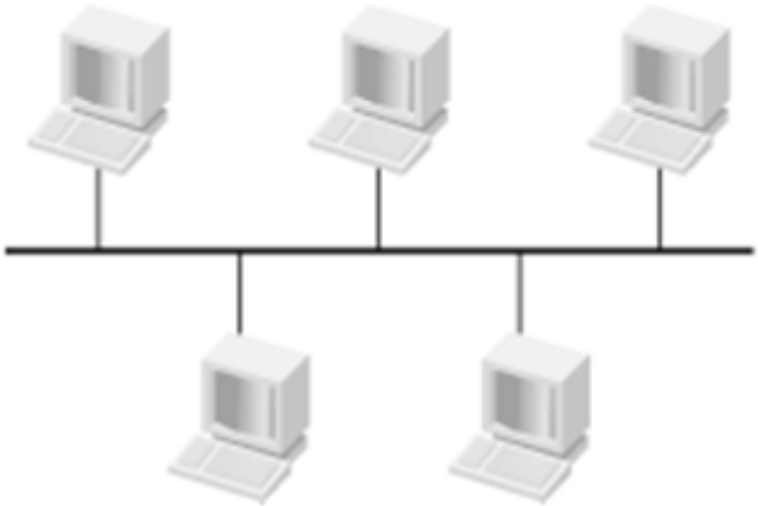


Figure 6.7 : Bus topology

Advantages of Bus Topology

- Cheap, easy to handle and implement.
- Require fewer cables.
- It is best suited for small networks.
- Does not use any specialized network equipment.

Disadvantages of Bus Topology

- Network disruption when computers are added or removed.
- A break in the cable will prevent all systems from accessing the network.
- The cable length is limited. This limits the number of stations that can be connected.
- This network topology can perform well only for a limited number of nodes.

6.4.2 Ring Topology

In a ring network, every device has exactly two neighbors for communication purposes. A network topology that is arranged in a circular fashion in which data travels around the ring in one direction from one computer to another and each device on the right acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring. The network is dependent on the ability of the signal to travel around the ring.

- All messages travel through a ring in the same direction.
- A failure in any cable or device breaks the loop and can take down the entire network.
- To implement a ring network we use the Token Ring technology.
- A token, or small data packet, is continuously passed around the network. When a device needs to transmit, it reserves the token for the next trip around, and then attaches its data packet to it.

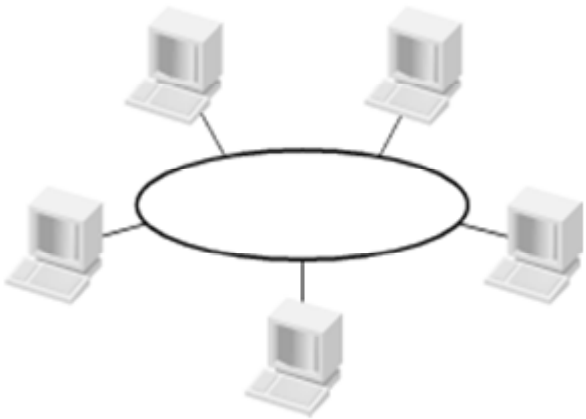


Figure 6.8 : Ring topology

Advantage of Ring Topology

- Very orderly network where every device has access to the token and the opportunity to transmit.
- Easier to install and manage than a Bus Network
- Good Communication over long distances
- Handles high volume of traffic

• Cable faults are easily located, making troubleshooting easier

Disadvantages of Ring Topology

• The failure of a single node of the network can cause the entire network to fail.

• The changes/expansion made to network nodes affects the performance of the entire network.

6.4.3 Star Topology

• In a star network, each node *(file server, workstations, and peripherals)* is connected to a central device called a hub or switch.

• Each device requires a single cable point-to-point connection between the device and hub switch.

• Most widely implemented and used.

• Hub can be the single point of failure.

• The hub takes a signal that comes from any node and passes it along to all the other nodes in the network.

• Data on a star network passes through the hub, switch, or concentrator before continuing to its destination.

• The hub, switch, or concentrator manages and controls all functions of the network.

• The star topology reduces the chance of network failure by connecting all of the systems to a central node.

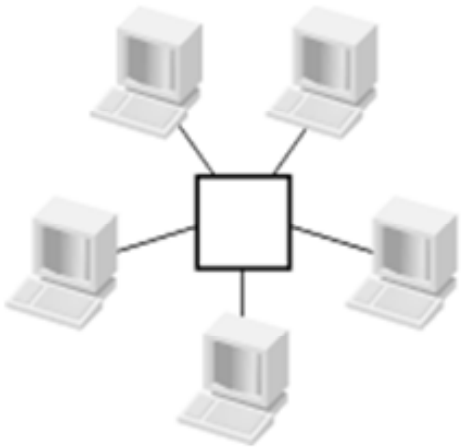


Figure 6.9 : Star topology

Advantages of Star Topology

• Easy to install and manage and wire.

• Easily expanded than a bus/ ring topology without disruption to the network.

• Cable failure affects only a single user.

• Easy to troubleshoot and isolate faults.

Disadvantages of Star Topology

• Requires more cable than a linear topology.

• If the hub or concentrator fails, nodes attached are disabled.

• More expensive because of the cost of the concentrators.

6.4.4 Tree Topology

• A tree topology (hierarchical topology) can be viewed as a collection of star networks arranged in a hierarchy.

• This tree has individual peripheral nodes which are required to transmit to and receive from one other only and are not required to act as repeaters or regenerators.

• The tree topology arranges links and nodes into distinct hierarchies in order to allow greater control and easier troubleshooting.

• This is particularly helpful for colleges, universities and schools so that each connect to the big network in some way.

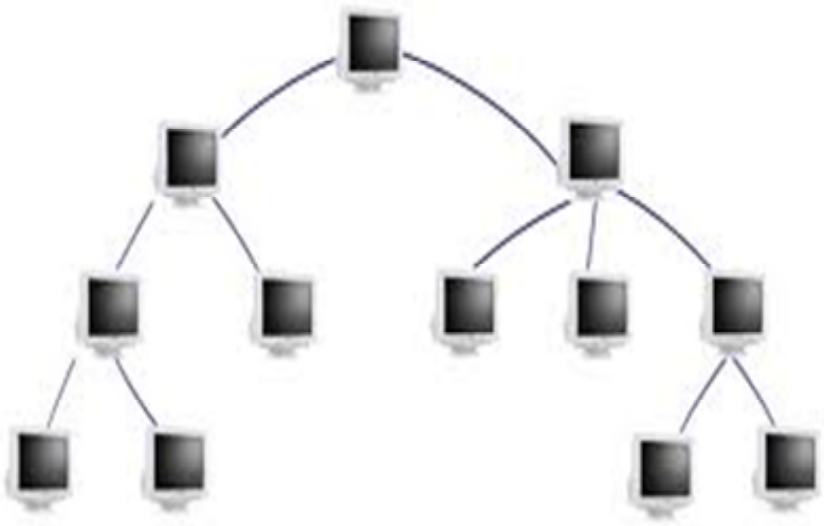


Figure 6.10 : Tree Topology

Advantages of a Tree Topology

• Point-to-point wiring for individual segments.

• Supported by several hardware and software vendors.

• All the computers have access to the larger and their immediate networks.

Disadvantages of a Tree Topology

• Overall length of each segment is limited by the type of cabling used.

• If the backbone line breaks, the entire segment goes down.

• More difficult to configure and wire than other topologies.

6.4.5 Mesh Topology

• In this topology, each node is connected to every other node in the network.

• Implementing the mesh topology is expensive and difficult.

• In this type of network, each node may send message to destination through multiple paths.

• While the data is travelling on the Mesh Network it is automatically configured to reach the destination by taking the shortest route which means the least number of hops.

Mesh Topology

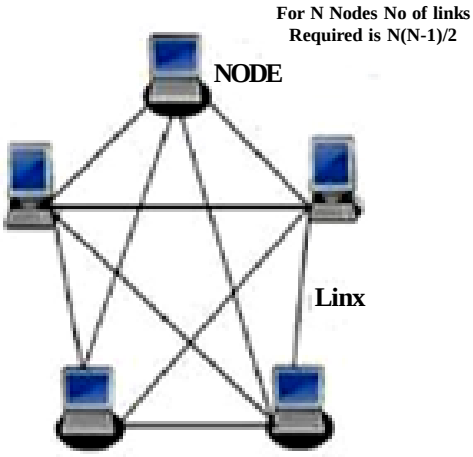


Figure 6.11 : Mesh network having 5 nodes **Figure 6.12 : Mesh network of 6 computers**

NOTE- Making a fully meshed network with N devices requires N*(N-1)/2 links. i.e. to make a fully meshed network with 5 devices requires 5(5-1)/2 = 10 links.

Advantage of Mesh Topology

• No traffic problems as there are redundant paths b/w devices.

• It has multiple links, so if one route is blocked then other routes can be used for data communication.

• Points to point links make fault identification easy.

Disadvantage of Mesh Topology

• There is mesh of wiring which can be difficult to manage.

• Installation is complex as each node is connected to every node.

• Cabling cost is high.

• Troubleshooting a failed cable is tricky.

6.4.6 Hybrid Topology

• A combination of any two or more network topologies.

• A hybrid topology always accrues when two different basic network topologies are connected.

• It is a mixture of above mentioned topologies. Usually, a central computer is attached with sub-controllers which in turn participate in a variety of topologies.

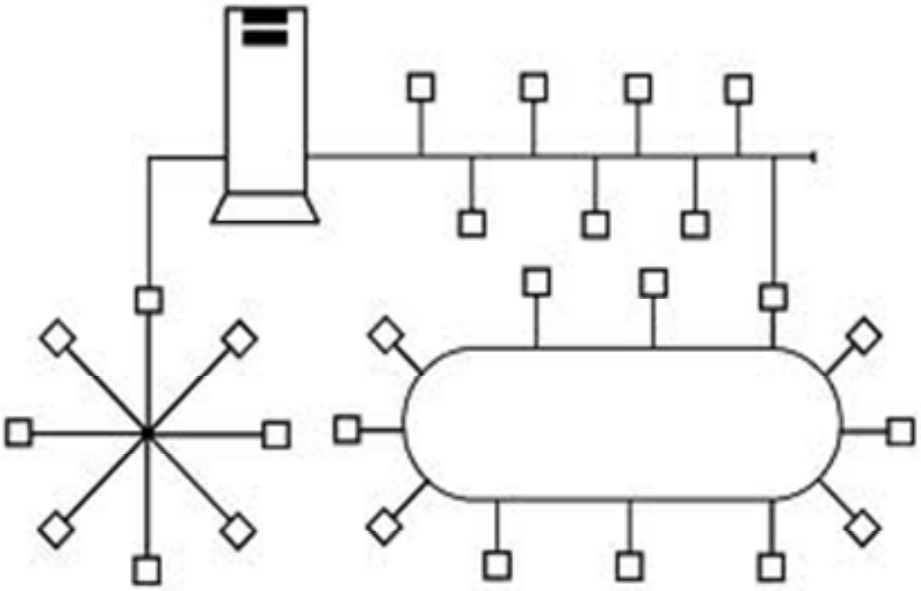


Figure 6.13 : Hybrid Topology

Advantages of a Hybrid Topology

- It is extremely flexible.
- It is very reliable.

Disadvantages of a Hybrid Topology

- Expensive

6.5 Network Hardware

We mentioned that you could connect one computer to another. This can be done using their serial ports:

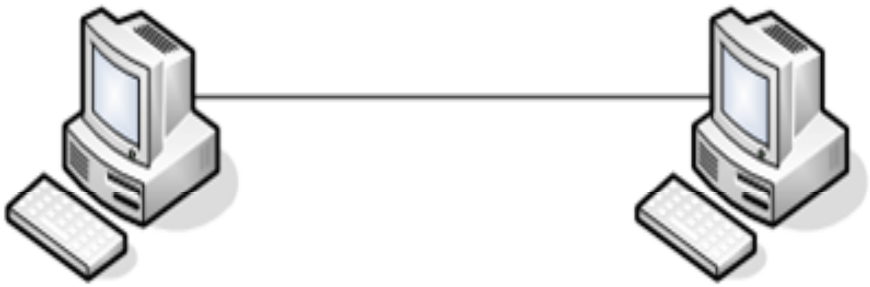


Figure 6.14 : Serial Post Computers

It is possible because almost every computer has a serial port. If you have to connect many computers to produce a network, this serial connection would not be practical. The solution is to use a central object that the computers and other resources can connect to, and then this object becomes responsible to *"distribute"* or manage traffic on network:

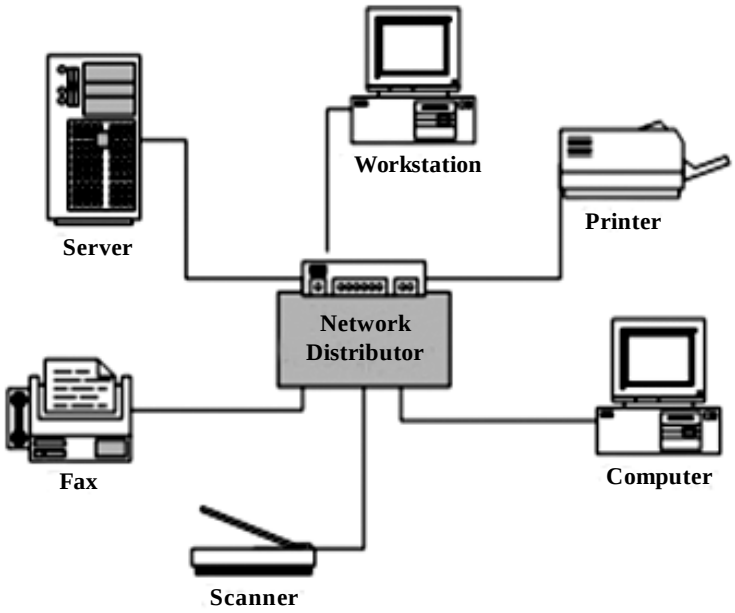


Figure 6.15 : A Network connection using Network Hardware

The most regularly used types of network distributors are the *hub, the switch, and the router.* Networking hardware or networking equipment typically refers to devices facilitating the use of a computer network. Typically, this includes gateways, routers, network bridges, switches, hubs, and repeaters. Also, hybrid network devices such as multilayer switches, protocol converters and bridge routers. And, proxy servers, firewalls and network address translators. Also, multiplexers, network interface controllers, wireless network interface controllers, modems, ISDN terminal adapters and line drivers. And, wireless access points, networking cables and other related hardware.

Computer networking devices are units that mediate data in a computer network. Computer networking devices are also called network equipment, *Intermediate Systems* (IS) or *Inter Working Unit* (IWU). Units which are the last receiver or generate data are called hosts or data terminal equipment.

The most common kind of networking hardware today is copper-based Ethernet adapters, helped largely by its standard inclusion on most modern computer systems. Wireless networking has become increasingly popular, however, especially for portable and hand-held devices.

Other hardware prevalent within computer networking is datacenter equipment *(such as file servers, database servers and storage areas).*

In addition to computers, the hardware components needed to create LAN include the following:-

- PCs, printers, scanners etc.
- Network cables.
- Cable Interface Unit.
- Network Interface Cards (NIC/Ethernet card) for each node.

Other diverse devices which may be considered networking hardware include mobile phones, PDAs and even modern coffee machines. As technology grows and IP-based networks are integrated into building infrastructure and household utilities, network hardware becomes an ambiguous statement owing to the increasing number of *"network capable"* endpoints.

Hubs, Bridges, Switches and Routers are used to build networks. If you are trying to design your own LAN *(Local Area Network)* at home, then you probably need to know what they do and the main differences between them.

6.5.1 Hub

Hubs are used to build a LAN by connecting different computers in a star/hierarchal network topology, the most common type on LANs now a day. A hub is a very simple *(or dumb)* device, once it gets bits of data sent from computer i.e. A to B, it does not check the destination, instead, it forwards that signal to all other computers also within the network. B will then pick it up while other nodes discard it. This amplifies that the traffic is shared.

There are mainly two types of hubs:

• *Passive:* The signal is forwarded as it is *(so it doesn't need power supply)*.

• *Active:* The signal is amplified, so they work as repeaters. In fact they have been called multiport repeaters. *(Use power supply)*

Hubs can be connected to other hubs using an uplink port to extend the network.

OSI Model: Hubs work on the physical layer *(lowest layer)*. That's the reason they can't deal with addressing or data filtering.

A *hub* is rectangular box that is used as the central object on which computers and other devices are connected. To make this possible, a hub is equipped with small holes called *ports*. Here is an *example* of a hub:

Figure 6.16 : Hub

Although this appears with 4 ports, depending on its type, a hub can be equipped with 4, 5, 12, or more ports. Here is an example of a hub with 8 ports:

Figure 6.17 : 8-Ports Hub.

When configuring it, you connect an RJ-45 cable from the network card of a computer to one port of the hub.In most cases for a home-based or a small business network, you may not need (or shouldn't use) a hub.

6.5.2 Switch

A *switch* is an intelligent hub. Switches on the other hand are more advanced. Instead of broad-

casting the frames everywhere, a switch actually checks for the destination MAC address and forward it to the relevant port to reach that computer only. This way, switches reduce traffic and divide the collision domain into segments, this is very sufficient for busy LANs and it also protects frames from being sniffed by other computers sharing the same segment.

They build a table of which MAC address belongs to which segment. If a destination MAC address is not in the table it forwards to all segments except the source segment. If the destination is same as the source, frame is discarded.

Switches have built-in hardware chips solely designed to perform switching capabilities, therefore they are fast and come with many ports. Sometimes they are referred to as intelligent bridges or multiport bridges. Different speed levels are supported. They can be 10 Mbps, 100 Mbps, 1 Gbps or more.

Most common switching methods are:

• *Cut-through:* Directly forward what the switch gets.

• *Store and forward:* receive the full frame before retransmitting it.

OSI: Switches are on the data link layer *(just above physical layer)* that's why they deal with frames instead of bits and filter them based on MAC addresses. Switches are known to be used for their filtering capabilities.

6.5.3 Router

Routers are used to connect different LANs or a LAN with a WAN *(e.g. the internet)*. Routers control both collision domains and broadcast domains. If the packet's destination is on a different network, a router is used to pass it the right way, so without routers the internet could not functions.

Routers use NAT *(Network Address Translation)* in conjunction with IP Masquerading to provide the internet to multiple nodes in the LAN under a single IP address. Now a day, routers come with hub or switch technology to connect computers directly.

In OSI model, routers work on the network layer so they can filter data based on IP addresses. They have route tables to store network addresses and forward packets to the right port.

Like a hub, a router is another type of device that acts as the central point among computers and other devices that are part of a network. Here is an example of a wired router:

Figure 6.18 : Router (front-view).

A router functions a little differently than a hub. In fact, a router can be considered a little *"intelligent"* than the hub.

Like a hub, the computers and other devices are connected to a router using network cables. To make this possible, a router is equipped with holes, called ports, in the back. Here is an example:

Figure 6.19 : Router (Back-view).

Based on advances in the previous years from IEEE and other organizations or research companies, there are wireless routers. With this type, the computers and devices connect to the router using microwaves (no physical cable).

6.5.4 Bridge and Gateway

Bridges are used to extend networks by maintaining signals and traffic. In OSI model, bridges are on the data link layer so in principle they are capable to do what switches do like data filtering and separating the collision domain, but they are less advanced. They are known to be used to extend distance capabilities of networks.

In a comparison with switches, they are slower because they use software to perform switching. They do not control broadcast domains and usually come with less number of ports.

Gateways are very intelligent devices or else can be a computer running the appropriate software to connect and translate data between networks with different protocols or architecture, so their work is much more complex than a normal router. For instance, allowing communication between TCP/IP clients.

In OSI model gateways operate at the network layer and above, but most of them at the application layer.

In this case, the router has gateway software. And Default Gateway is used to refer to the node (e.g. router) connecting the LAN to the outside (e.g. internet).

6.5.5 Repeater

Definition: Network repeaters regenerate incoming electrical, wireless or optical signals. With physical media like Ethernet or Wi-Fi, data transmissions can only span a limited distance before the quality of the signal degrades. Repeaters attempt to preserve signal integrity and extend the distance over which data can safely travel.

Actual network devices that serve as repeaters usually have some other name. Active hubs, for example, are repeaters. Active hubs are sometimes also called "multiport repeaters.Repeaters are simple devices that work at the physical layer of the OSI. They regenerate signals (an active hub does that too).

There is an important rule to obey while using repeaters/hubs to extend a local network and is called the 5-4-3 rule. The rule forces that in a single collision domain there shouldn't be more than 5 segments, 4 repeaters between any two hosts in the network and only 3 of the segments can be populated (contain user connections).This rule ensures that a signal sent over the network will reach every part of it within an acceptable length of time. If the network is bigger, the collision domain can be divided into two parts or more using a switch or a bridge.

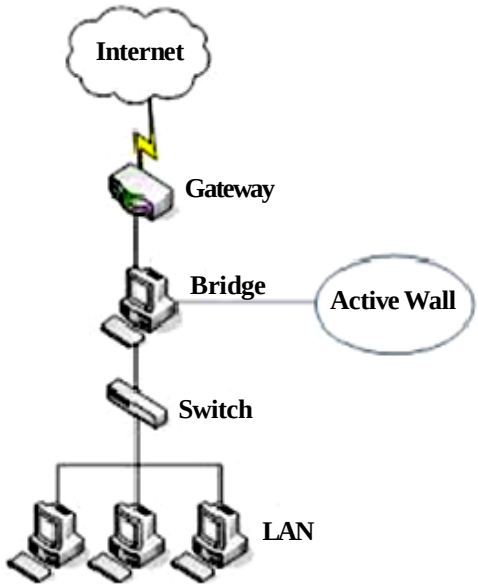


Figure 6.20 : A Network connection.

6.5.6 Network Cables

Cable is used to connect computers. Although we may use wireless networking. The most commonly used cable is referred to as Category 5 cable RJ-45. They can be in different colors: You can purchase this cable from a general store, a computer store. The ends of the cable appear as follows:

Figure 6.21 : Cables.

6.6 Summary

• A Metropolitan Area Network (MAN) is a large computer network that usually spans a city or a large campus. A MAN typically covers an area of between 5 and 50 km diameter. Examples of MAN: Telephone company network that provides a high speed DSL to customers and city cable TV network.

• A Wide Area Network is a network of networks. In a WAN two or more LANs are connected together. It can also be defined as combination of LANs and MANs. WAN covers a large geographic area such as country, continent or even whole of the world. The world's most popular WAN is the Internet.

• Network Topology -Refers to the Physical and logical arrangements of network nodes. The

physical topology of a network refers to the configuration of cables, computers, and other peripherals. Logical refers to the way in which the network appears to the devices that use it.

• In bus topology all the nodes (file server, workstations, and peripherals) are connected by a single cable.

• In a ring network, every device has exactly two neighbors for communication purposes.

• In a star network, each node (file server, workstations, and peripherals) is connected to a central device called a hub or switch.

• A tree topology (hierarchical topology) can be viewed as a collection of star networks arranged in a hierarchy.

• In Mesh topology, each node is connected to every other node in the network.

• Making a fully meshed network with N devices requires N*(N-1)/2 links. i.e. to make a fully meshed network with 5 devices requires 5(5-1)/2 = 10 links.

• Hubs are used to build a LAN by connecting different computers in a star/hierarchal network topology,

• A Switch is an intelligent hub.

• Routers are used to connect different LANs or a LAN with a WAN (e.g. the internet). Like a hub, a router is another type of device that acts as the central point among computers and other devices that are part of a network. Routers operate at network layer.

• Bridges are used to extend networks by maintaining signals and traffic.

• Gateways are very intelligent devices or else can be a computer running the appropriate software to connect and translate data between networks with different protocols or architecture, so their work is much more complex than a normal router. Gateways operate at application layer.

• Network repeaters regenerate incoming electrical, wireless or optical signals.

6.7 Self-Assessment Questions

1. Differentiate between MAN and WAN.
2. What is defined by the physical and logical topology?
3. What are the different types of network topologies? Explain each using suitable diagrams. Write advantages and disadvantages of each.
4. Which network topology is the best? And Why?
5. What do you mean by hybrid topology? Explain using suitable diagram.
6. What do you mean by network hardware? Explain different network hardwares that are used in networking.
7. Differentiate between hubs and switches.
8. What a router does?
9. What is the need of repeaters?
10. Write short note on Bridges and Gateways.
11. Differentiate between router and switch.

6.8 References

1. Behroz A Forouzen, "Data Communication and Networking", Mc-Grow-Hill, Publication, Fourth Edition, 2006.
2. Andrew, S. Tanenbaum, "Computer Networks", Person Education, Third Edition, 1999.

Unit-7
ISO-OSI Model of Networking-I
Concepts of Standards and Protocols, Protocol Architecture

Structure of the Unit

7.0 Objective

After study of this unit you will be able to learn the fundamental concepts in data communications and networking. It also covers the idea of standards, protocols and different standard organizations.

7.1 Introduction

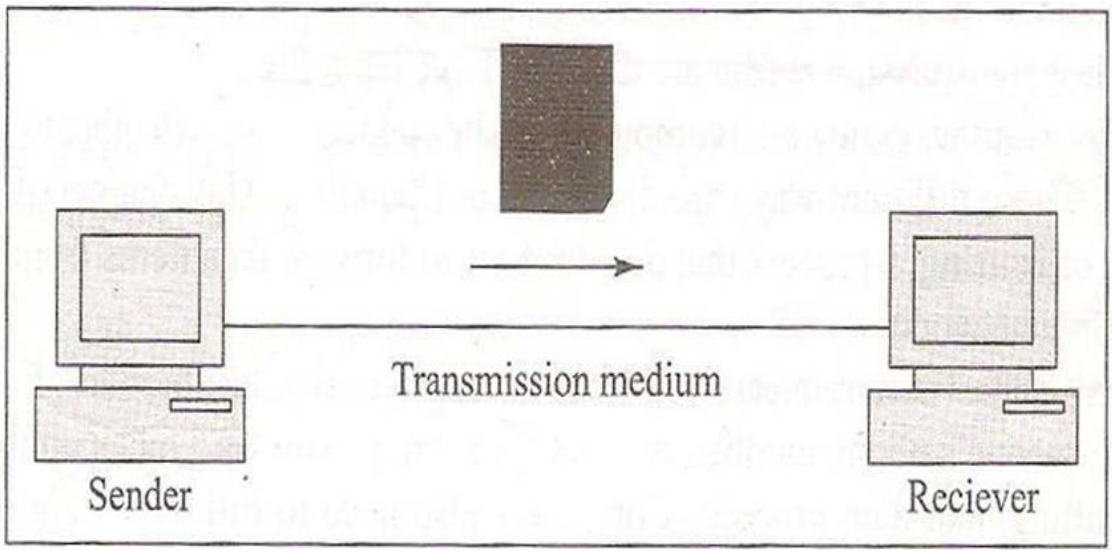
This chapter introduces the basic concepts of data communications. Before we understand how computer networks and inter-networks work, it is essential to know how data can be transmitted from a source to a destination in the first place. This forms the basis for all data communications. The principle of signal propagation is used for this purpose.

We shall first have an overview of data communications, some important concepts and the standards related to data communications along with the organizations who govern these standards.We shall start our technical discussion with an understanding of how we can transmit data in the form of signals from one point to another. Using this as the base, we shall then consider how a signal can be analyzed for understanding data communications. We shall introduce several important terms as we go along, that are very commonly used in the discussions of data communications.

7.2 Fundamental Concepts

7.2.1 Basic Idea

Communication can be defined as exchange of information between two humans. Data communications can be defined the exchange of information between two computers. In its simplest form, the data communication process can be shown in fig. 7.1. The figure shows one computer (sender) sending a message to another computer (receiver) over a wire (called **transmission medium**).



Figur 7.1 : Data Communication

Of course, this is an oversimplified view. Real-life data communication process involves many hardware devices and software techniques. This makes data communication an extremely complex process. Real-life data communication process (still for more simplified) is sown in Fig.

7.2.2 Real-life Data Communications

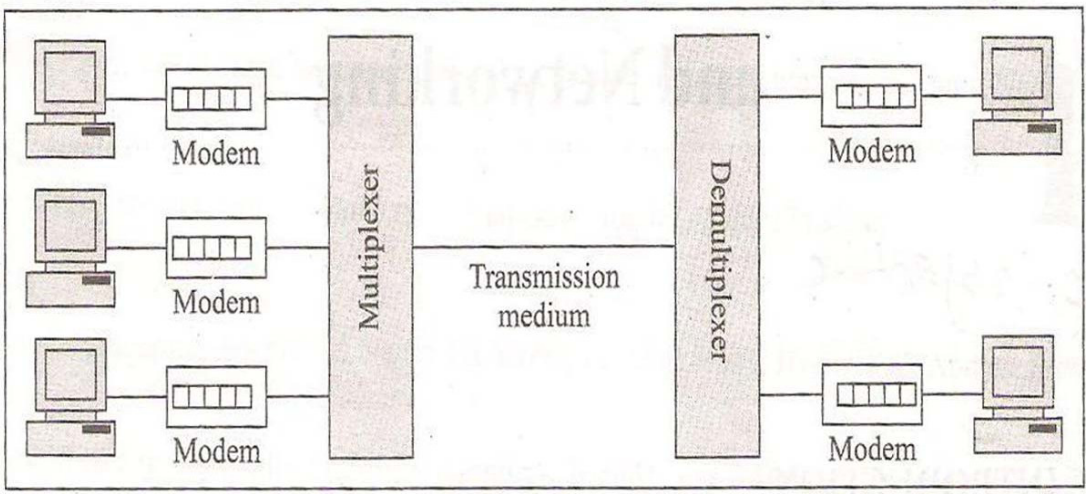


Figure 7.2 : Real-life Data Communication Systems

Figure 7.2 shows a real-life data communication systems. It contains various components *(shown)* as well as other aspects *(hidden)* as discussed below:

Modem-A modem is connected to every computer that is involved in data communications *(either for sending or receiving data)*.

Multiplexer *and* ***Demultiplexer***-The figure shows the multiplexer at one end and the demultiplexer at the other end.

The subject of data communications is closely related to the understanding of errors that can occur during transmission. Data can be compressed, so that its size is reduced, and it can be sent faster. Modern data communications demand a lot of security mechanisms to be in palace.

Transmission medium-Transmission medium, or wire, is the means of transferring data from the sender to the receiver. Modern data communications can also be wireless.

Computers cannot communicate with each other arbitrarily, like humans. For instance, when we dial someone's phone number, we first greet the person who picks up the phone, inform who is calling, and then proceed. Computers also need to follow certain **protocols** during data communications.

Type of Network-Local Area Networks (LAN), Metropolitan Area Networks (MAN) and **Wide Area Networks (WAN)**

7.3 Data Communications

Data communications has become an extremely important aspect of the modern world. It has been a subject of grate interest for many decades. However, the possibilities of exchanging business-critical documents and information, conducting mission-critical transactions across geographical boundaries, sharing personal information with friends, etc., have made it very important to understand how to exchange data and how it works internally.

It the simplest form, when we talk of data communications, it involves exchange of data between two computers. Computers work with the binary language of zeros and ones. Therefore, one computer generates a stream of zeroes and ones, and sends it to another computer, to which it is connected in some fashion. The connection can be either a simple wire, or it can be through wireless media as well. Moreover, these two computers need not, necessarily, be close to each other-they can be in different rooms, streets, cities, states, countries or even continents, the magic of data communications technology enables this exchange of zeroes and ones from one computer to another.

For enabling data communications, a combination of hardware and software is essential. In any data communications systems, the following three characteristics are desired :

1. Correct delivery – When a sender transmits data for an intended recipient, the data must reach only the intended recipient and not someone else.

2. Accurate delivery – Data send by the sender must be received by the receiver in the receiver in the same form as the one in which it was sent. There must not be any sort of alterations in it while in transit.

3. Timely delivery – Data must travel from the sender to the receiver in a finite amount of time. The term finite is quite vague, and would depend on the reseons why data communication is taking place.

Two key aspects of data communication systems need a good amount of understanding. These are, namely, **transmission medium** and data communication **protocols**.

Transmission medium is the physical path over which data travels from the sender to the receiver. The transmission medium can be a twisted pair of copper wires, coaxial cable optical fiber or wireless media such as radio waves. We shall discuss all of these in detail later.

7.4 Protocols

A protocol is a set of rules and conventions that govern data communications. The sender and the receiver, the two key parties in data communication, must agree on a common set of rules, i.e., protocols before they can communicate with each other. Just as a person speaking only French cannot communicate with another person who understands only English, two devices that are connected to each other need not necessarily be able to communicate with each other unless they agree on a set of data communication protocols. There are many protocols for data communication, some of which are more popular than others. We shall have a quick overview of protocols now and study these in detail later.

Two devices wishing to communicate with each other cannot just begin data transmission arbitrarily. That is, one device cannot simply start sending bit streams to the other. The two devices must agree on a set of rules before this transmission can begin. Otherwise, how would the receiver know what the sender has sent? Conversely, how would the sender know it the receiver has correctly received the data that it had sent?

A protocol defines the following (in addition to a few other things) :

(i) Syntax (What is to be communicated) –Syntax defines the structure or format of data. This means that the order in which it is to be sent is decided. For instance, a protocol could define that the first 16 bits of any data transmission must always contain the receiver's address.

(ii) Semantics (How it is to be communicated?)-Semantics define the interpretation of the data that is being sent. For example, the semantics could define that if the last two bits of the receiver's address field contain a 00, it means that the sender and the receiver are on the same network.

(iii) Timing (When it should be communicated?)-This refers to an agreement between the sender and the receiver about data transmission rates and duration. For instance, a protocol could demand that the sender must send 1000 bytes and then wait for an acknowledgement from the receiver before sending any more data.

7.4.1 Protocol Hierarchies (Layered Architecture)

As a matter of fact, most networks are organized as a series of layers or levels. To reduce the design complexity, networks are organized as a series of layer or levels, one above the other as shown in figure 7.3. The number of layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network. The number or layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers. Layer n on one machine *(source)* carries on a conversation with layer n on another machine *(designation)*.

The rules and conventions used in this conversation are collectively known as the layer n protocol

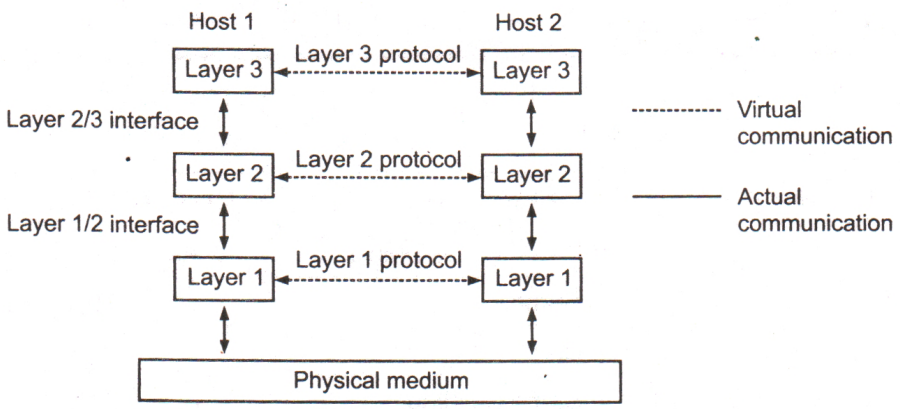


Figure 7.3 : Layers, protocols and interfaces

Basically, a protocol is an agreement between the two machines as how communication link should be established, maintained and released. Violation of the protocol will make the communication difficult.

Peer

A three layers network is shown in figure 7.3. The entities comprising the corresponding layers on different machines are called **peers**. The communication actually takes place between the peers using the protocol. The dotted lines in figure 7.3 show the virtual communication, and physical communication is shown by solid lines.

7.5 Standards

Standards are necessary in every walk of life. For instance, when you want to replace a light bulb in your home because it has been damaged, you expect the new bulb to fit in the holder straightaway and work like the old bulb. What is the use if the bulb does not fit in the holder or if it fits in the holder but does not illuminate because it requires a different voltage level. Consequently, everything that we use in our daily life has some common features, some standards that every manufacturer must abide by. In the absence of standards, every manufacturer can theoretically manufacture a set of goods or services that are incompatible with other manufactures.

To avoid such anomalies, a set of standards is established, which governs the rules that manufactures must obey. In exactly the same fashion, standards for data communications have been set. These standards ensure elimination of incompatibility issues, which is highly desirable in all data communications.

Data communication standards can be classified into the following two categories: **de facto** (which means by convention) and **de jure** (which means by regulation).

De facto standards can be further divided into proprietary and non-proprietary standards. Proprietary standards are invented and owned by an organization. These standards gain popularity post the owner's successful usage. This is because once the products of the organization using these standards are popular, the standards automatically gain popularity. Another name of proprietary standards is closed, because they close off communication with devices/systems of other vendors. Non-proprietary or open standards are those that are developed by an organization/committee/group, which become popular and vendors start supporting them. They are open because anybody adhering to those automatically gain access to all others following those standards.

De jure standards are the standards that have been legislated by an official body. These are usually led by governments or government-appointed agencies.

7.6 Standards Organizations

Various standards organizations for data communications exist. Broadly, they can be classified into the following three categories? **Standards creation committees, Forums** and **Regulatory agencies.**

7.6.1 Standards Creation Committee

There are a number of organizations serving as standards creation committees. Let us name a few key players in this area.

• **The International Standards Organization (ISO)** is a well known multinational standards body. Most members of ISO are representatives of their respective governments. Created in 1947, the ISO is a non-profitable standards creation organization. Members from over 80 developed nations actively represent the ISO. The **Open Systems Interconnection (OSI)** model as a networking protocol is a big contribution of ISO to the data communications world.

• **The International Telecommunications Union-Telecommunications Standards Sector (ITU-T)** was earlier known as the Consultative Committee for International Telegraphy and Telephony (CCITT). The name was changed on 1 March 1993 to ITU-T. This committee was formed by the United Nations in response to the demands from some nations, who were developing their own national standards for data communications in the early 1970s, leading to issues of incompatibility with each other. The V-series standards for use in modems (e.g., V.32), the X-series standards for public digital networks (e.g., X.25), email (e.g.,X.400), directory services (e.g., X.500) and the Integrated Digital Services Network (ISDN) are some of the major contributions of ITU-T to data communications.

• The **American National Standards Institute (ANSI)** is a private non-profit organization that dose not have any direct ties with the US federal government. However, generally, all ANSI projects are undertaken for the social benefit of US citizens. Professional groups, industry representatives, government, regulatory bodies, and consumer groups represent ANS, ANSI is an affiliate of the ITU-T.

• The Institute of Electrical and Electronics Engineers (IEEE) is the biggest professional engineering body in the world. As the name suggests IEEE focus areas are developments in the areas of electric and electronic engineering, and radio SCIENCES. IEEE also oversees the development and adoption of international computer and communications standards.

• The Electronic Industries Association (EIA) Iis a non-profit organization that is aligned with ANSI. Its focus is public awareness and lobbying for standards. Its main contributions to data communications technology are the development of interfaces for physical connections and electronic signal specifications for data communications.

7.6.2 Forums

Standards committees are notorious for the slow pace of developments and decision making. Consequently, user groups, university students, industry representatives and experts come together and set-up with standards forums to address the various issues and concerns of data communications technology, and come up with standards from time to time. These forums generally concentrate on a particular technology , and this specialization helps them achieve a grate amount of throughput with contributions from a variety of forum members.

The Internet Society (ISOC), Internet Engineering Task Force (IEFT), Frame Relay Forum, ATM Forum, ATM Consortium are some of the most well-known forums. The Frame Relay Forum and ATM Forum have interests in specialized technologies such as frame relay and ATM, while the ISOC and IEFT are concerned with the development of Internet-related standards and protocols

7.6.3 Regulatory Agencies

Government-appointed agencies such as the Federal Communications Commission (FCC) of the US are always involved in regulation the standards. These agencies help protect interests of the general public in areas such as radio, television and wired communications. For instance, every portion of communications technology must be approved by FCC before it can be sold in the market. FCC periodically reviews the rate charged by service providers, technology specifications of communication hardware and divides, and allocates radio frequencies, etc.

7.7 Summary

• Communication can be defined as exchange of information between two humans. Data communications can be defined the exchange of information between two computers.

• Transmission medium, or wire, is the means of transferring data from the sender to the receiver. Modern data communications can also be wireless.

• A protocol is a set of rules and conventions that govern data communications. The sender and the receiver, the two key parties in data communication, must agree on a common set of rules, i.e., protocols before they can communicate with each other.

7.8 Self-Assessment Questions

1. Define data communication. Explain characteristics of data communication.
2. Explain multiplexer and demultiplexer with their functionality.
3. Define protocol and standard. What a protocol define?
4. Explain different standards exist for data communication.

7.9 References

1. Behroz A Forouzen, "Data Communication and Networking", Mc-Grow-Hill, Publication, Fourth Edition, 2006.
2. Andrew, S. Tanenbaum, "Computer Networks", Person Education, Third Edition, 1999.

Unit-8

ISO-OSI Model of Networking II

Different Layers and Their Functions of OSI Model

Structure of the Unit

8.0 Objective

After study of this unit we will be able

1. To learn about the Open Systems Interconnection Reference Model (OSI Reference Model or OSI Model).
2. Seven layers Architecture of OSI.
3. To understand the various functions of each layer.
4. Diffrent products used of each layer.

8.1 Introduction

After discussing about the protocols, now let us discuss two network architectures of reference models. The two most important reference models are :

(i) The OSI reference model and

(ii) The TCP/IP reference model

The International Standards Organization (ISO) covers all aspects of network communication in the Open Systems Interconnection (OSI) model. An OSI model is a layered framework for the design of network systems that allows for communication across all types of computer systems. The purpose of each layer is to offer certain services to the higher layers. Layer n on one machine *(source)* carries on a conversation with layer n on another machine *(destination).* The rules and conventions used in this conversation are collectively known as the layer n protocol. Basically, a protocol is an agreement between the two machines as how communication link should be established, maintained and released.

The users of a computer network are located over a wide physical range i.e. all over the world. Therefore, to ensure that nationwide and worldwide data communication systems can be developed and are compatible to each other, an international group of standards has been developed. These standards will fit into a framework which has been developed by the International organization of standardization (ISO). This framework is called as Model for Open System Interconnection (OSI) and it is normally referred to as OSI reference model. Figure 8.1 shows the seven layer architecture of ISO-OSI reference model. It defines seven levels or layers in a complete communication systems. The lowest layer is physical layer and highest one is called the application layer.

A more detailed OSI reference model is shown in figure 8.2. It is called as ISO-OSI (Open System Interconnection) reference model because it is designed to deal with open systems i.e., the systems which are open for communication with other systems.

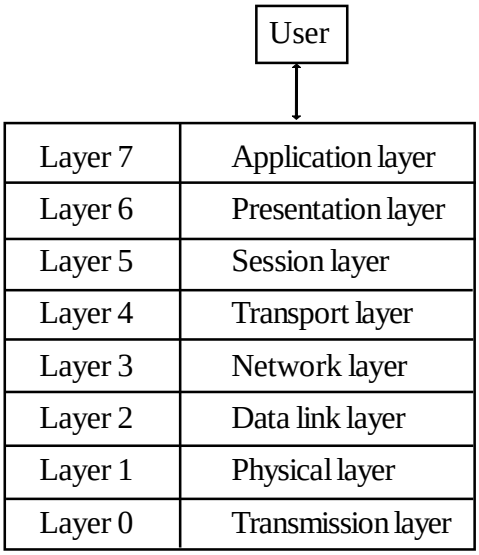


Figure 8.1 : A seven layer ISO-OSI reference model

Level	Name of the layer	Functions
1	Physical Layer	Make and break connections, define voltages and data rates, convert data bits into electrical signal. Decide whether transmission is simplex, half duplex or full duplex.
2	Data Link Layer	Synchronization, error detection and correction. To assemble outgoing messages into frames.
3	Network Layer	Routing of the signals; to outgoing message into packets; to act as net work controller for routing data.
4	Transport Layer	Decides whether transmission should be parallel or signal path, multiplexing, splitting or segmenting the data, to break data into smaller units for efficient handling.
5	Session Layer	To manage and synchronize conversation between two systems. It controls logging on and off, user identification, billing and session man agement.
6	Presentation Layer	It works as a translating layer.
7	Application Layer	Retransferring files of information. LOGIN, password checking etc.

Table 8.1 : Functions of the layer of ISO-OSI model

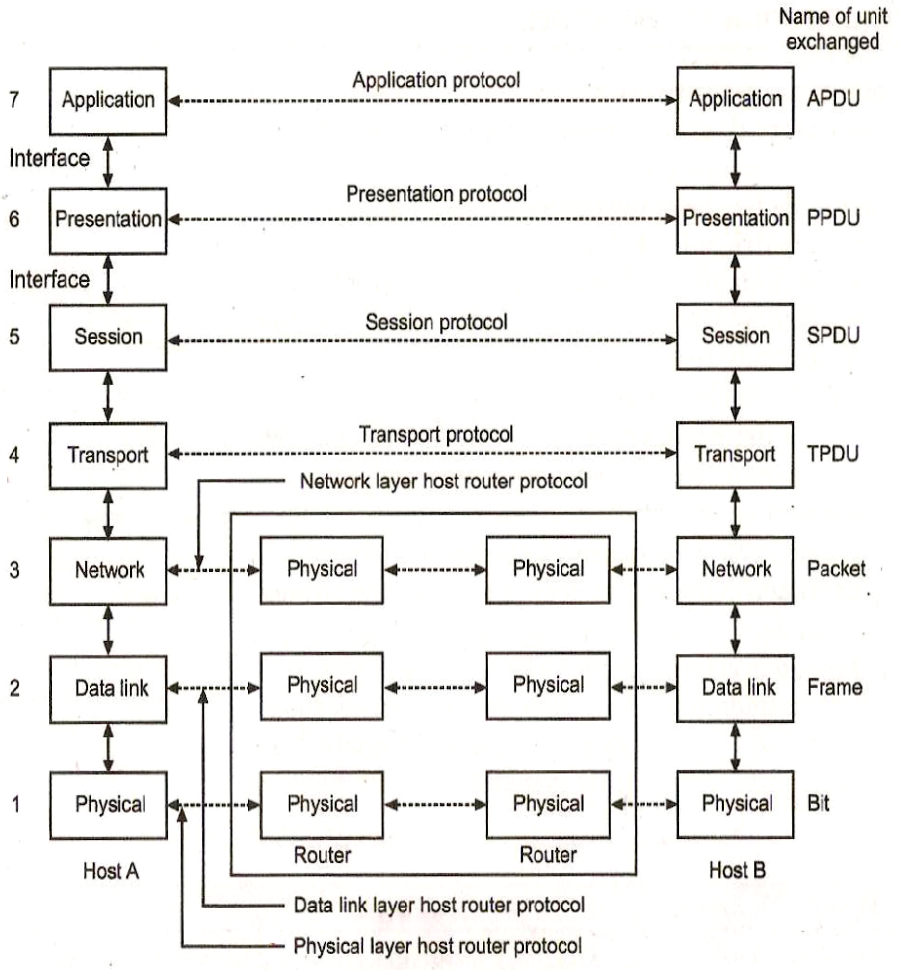


Figure 8.2 : The OSI reference model

All the applications need not use all the seven layers shown in figure 8.1. The lower three layers are enough for most of the applications. Each layer is built from electronic circuits and /or software and has a separate existence from the remaining layers. Each layer is supposed to handle message or data from the layers which are immediately above or below it. This is done by following the protocol rules. Thus, each layer takes data from the adjacent layer, handles it according to these rules and then passes the processed data to the next layer on the other side.

8.2 Functions of Different Layers

At the physical layer, communication is direct i.e. machine X sends a stream of bits to message it receives from the layer just above it and passes the whole package to the layer just below it as shown in figure 8.3. the information added by each layer is in the form of headers or trailers. Headers are added to the massages at the layers 6,5,4,3, and 2. A trailer is added at layer 2. A layer 1, the entire package is converted to a form that can be transferred to the receiving machine. At the receiving machine, the massage is unwrapped layer by layer with each processing receiving and removing the data meant for it.

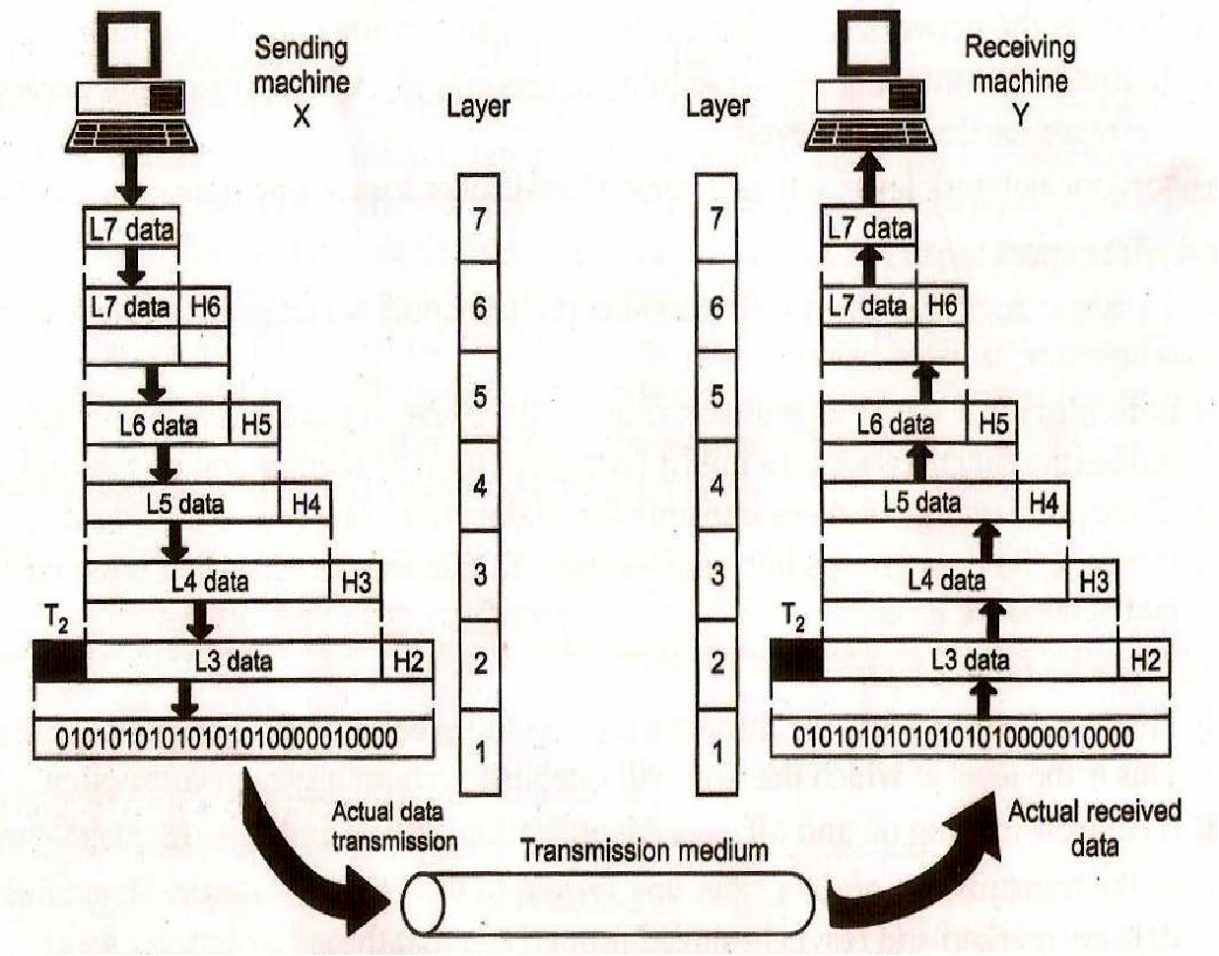


Figure 8.3 : An exchange using the OSI model

The upper OSI layers are always implemented in software (4,5,6 and 7) and lower layers are a combination of hardware and software (2,3) except for the physical layer which is mostly hardware. Layers 1, 2 and 3 (i.e. physical, data link and network) are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical connections, physical addressing and transport timing and reliability. Layer 4, the transport layer ensures end to end reliable data transmission. Layers 5, 6 and 7 (i.e. session, presentation and application) they allow interoperatibility among unrelated software systems.

8.2.1 Layer 1 : Physical Layer

The physical layer is responsible for sending bits from one computer to another. The physical layer is not concerned with the meaning of the bits, but it deals with physical connection to the network and with transmission and reception of signals. The physical level is used to define physical and electrical details such as what will represent a 1 or a 0, how many pins a network will have, how data will be synchronized and when the network adapter may or may not transmit the data. The position of the physical layer with respect to the transmission medium and the data link layer is shown in figure 8.4.

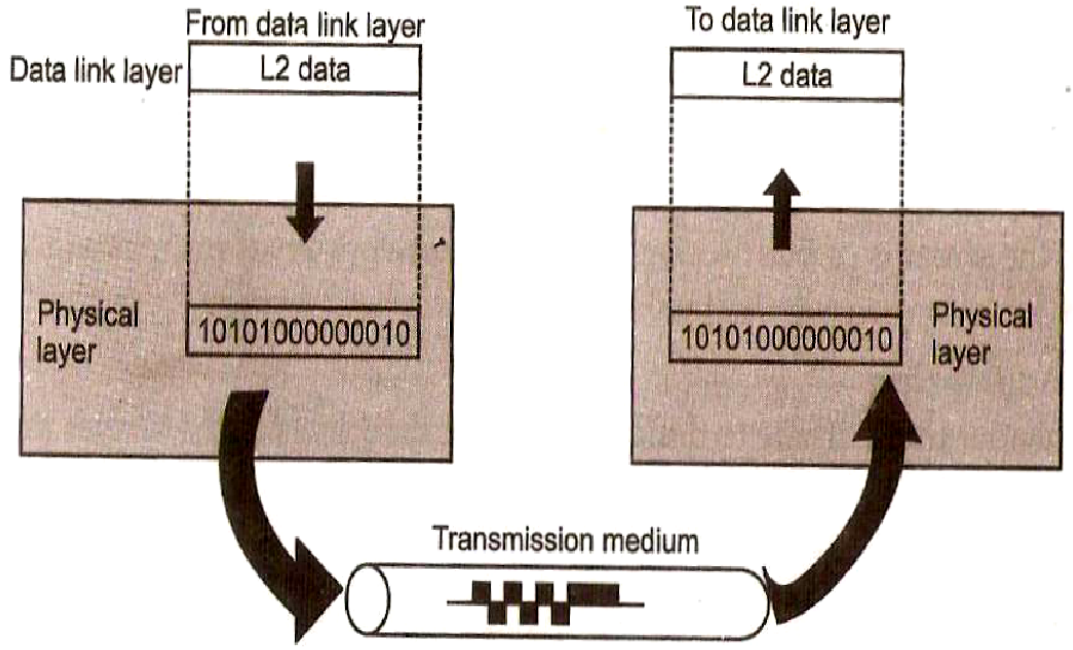


Figure 8.4 : Physical layer

Following are the functions of the physical layer :

(i) To define the type of encoding *i.e. how 0's and 1's are changed to signals.*

(ii) To define the transmission rate *i.e. the number of bits transmitted per second.*

(iii) To deal with the synchronization of the transmitter and receiver.

(iv) To deal with network connection types, including multipoint and point to point connections.

(v) To deal with physical topologies *i.e. bus, star, ring, or mesh.*

(vi) To deal with the media bandwidth *i.e. baseband and broadband transmission.*

(vii) Multiplexing which deals with combining several data channels into one.

(viii) To define the characteristics between the device and the transmission medium.

(ix) To define the transmission mode between two devices i.e. *whether it should be simplex, half duplex or full duplex.*

Connecting devices associated with physical layer

Passive hubs, simple active hubs, terminators, couplers, cable and cabling, connectors, repeaters, multiplexers, transmitters, receivers, transceivers and associated with the physical layers.

8.2.2 Layer 2 : Data Link Layer

It is responsible for reliable node to node delivery of the data. It accepts packets from the network layer and forms frames and gives it to the physical layer as shown in figure 8.5.

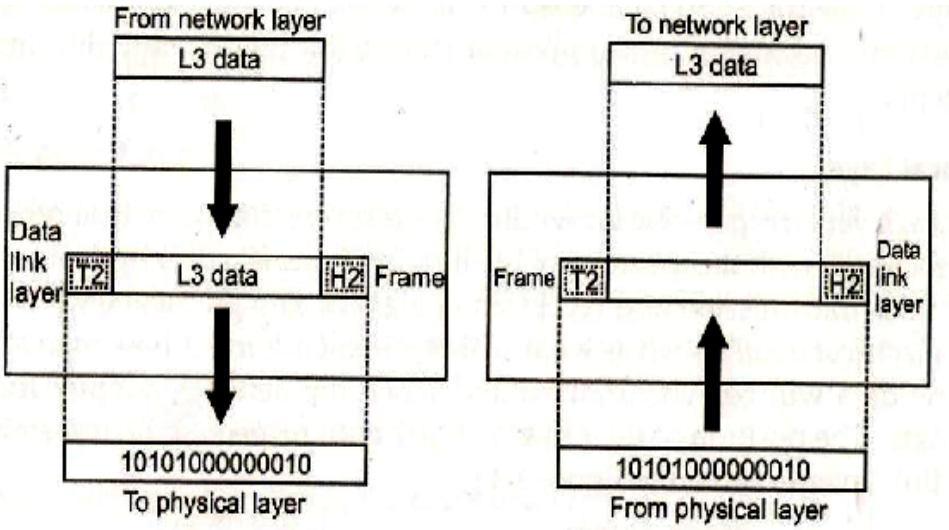


Figure 8.5 : Data link layer

Following are the functions of data link layer :

- Farming

It divides the streams of bits received from the network layer into manageable data units called frames.

- Physical Addressing

It adds a header to the frame to define the physical address of the sender and/or receiver of the frame.

- Flow control

It provides a flow control mechanism to avoid a fast transmitter from over-running a slow receiver by buffering the extra bits.

- Error Control

Error control is achieved by adding a trailer at the end of the frame. It also uses a mechanism to prevent duplication of frames.

- Access Control

The data link layer protocol determines which of the devices has control over the link at any given time, when two or more devices are connected to the same link. The Institution of Electrical and Electronics Engineers (IEEE) felt the need to define the data link layer in more details, so they split in into two sub-layers.

(i) *Logical Link Control (LLC)*

It establishes and maintains links between the communicating device.

(ii) *Media Access Control (MAC)*

It controls the way multiple devices share the same media channel. The logical link control sub-layer provides Service Access Points (SAPs) that the other computers can refer to and use to transfer information from LLC to the network layer. The MAC sub-layer provides for shared access to the network adapter

and communicates directly with the network interface cards. Network interface cards (NIC) have unique 12-digit hexadecimal MAC address assigned before they leave the factory where they are manufactured.

The MAC addresses are used to establish logical link between two computers on the same LAN. Bridges, intelligent hubs and network interface cards are devices associated with the data link layer.

8.2.3 Layer 3 : The Network Layer

The main function of this layer is to deliver packets from source to destination across multiple networks *(links)*. If two systems are connected on the same link, there is no need for a network layer. The relationship of the network layer to the data link and transport is shown in figure 8.6.

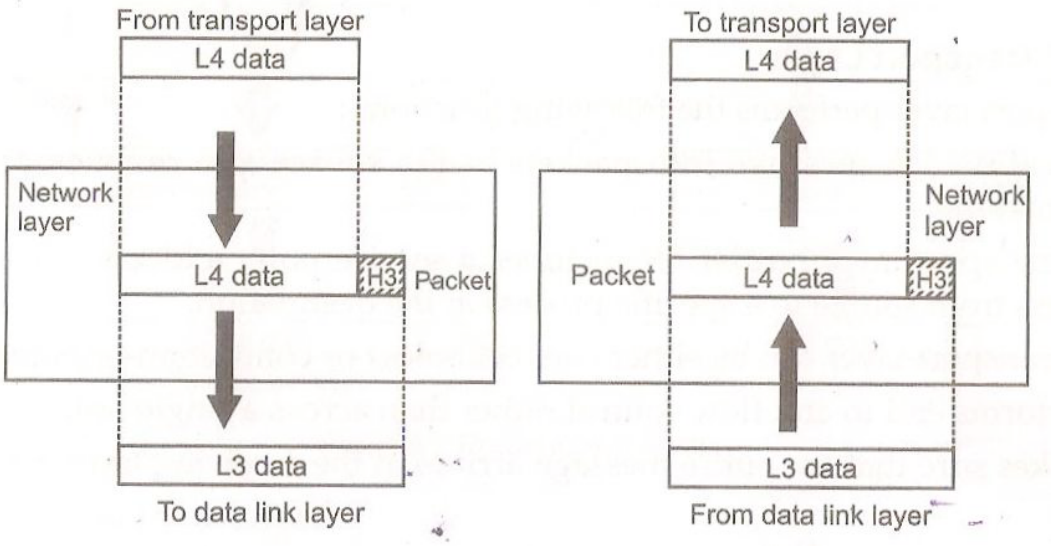


Figure 8.6 : Network layer

Function of the Network Layer

(i) It translates logical network address into physical machine addresses i.e. the numbers used a destination IDs in the physical network cards.

(ii) It determines the quality of service by deciding the priority of message and the route a message will take if there are several ways a message can get to its destination.

(iii) It breaks the larger packets into smaller packets it the packet is lager than the largest data frame the data link will accept.

(iv) It is concerned with the circuit, message or packet switching.

(v) It provides connection services, including network layer flow control, network layer error control and packet sequence control.

(vi) Routers and gateways operate in the network layer.

8.2.4 Layer 4 : Transport Layer

It is responsible for source to destination delivery of the entire message. It ensures that the whole message arrives intact and in order, ensuring both error control and flow control at the source to destination level. Figure 8.7 shows the relationship of the transport layer to the network layer and session layer.

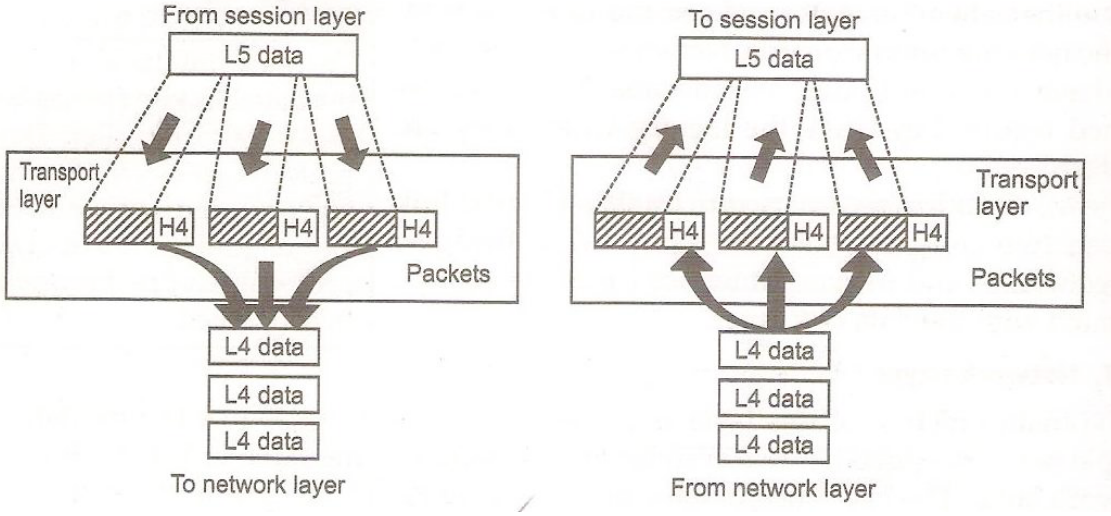


Figure 8.7 : Transport layer

Functions of Transport Layer

The transport layer performs the following functions :

(i) It divides each message into packets at the source and re-assembles then at the destination.

(ii) The transport layer header H4 includes a service point address to deliver a specific process from source to a specific process at the destination.

(iii) The transport layer can be either connectionless or connection-oriented.

(iv) It performs end to end flow control rather than across a single link.

(v) It makes sure that the entire message arrivers at the receiving transport layer without error.

8.2.5 Layer 5 : The Session Layer

The job of session layer is to establish, maintain and synchronize the interaction between the communicating systems. Figure 8.8 show the relationship of the session layer to the transport layer and the presentation layer.

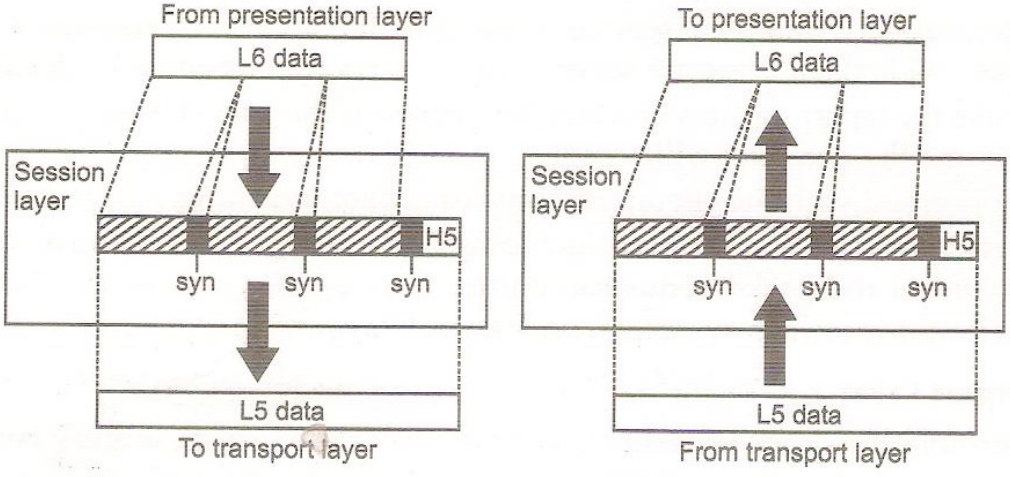


Fig. 8.8 Session layer

Functions of Session Layer

The session layer performs the following functions :

(i) It allows two systems to start a dialogue with each other. The communication initiated between two processes can be either in half duplex or full duplex.

(ii) The session layer allows addition of check points i.e. synchronization points into a stream of data. In case of crash doing the transmission of the data can be retransmitted from the check point inspite of retransmitting it from the start.

8.2.6 Layer 6 : The Presentation Layer

This layer takes care of the syntax and semantics of the information exchanged between two communicating systems. The relationship between the presentation layer and the application and session layer is shown in figure 8.9.

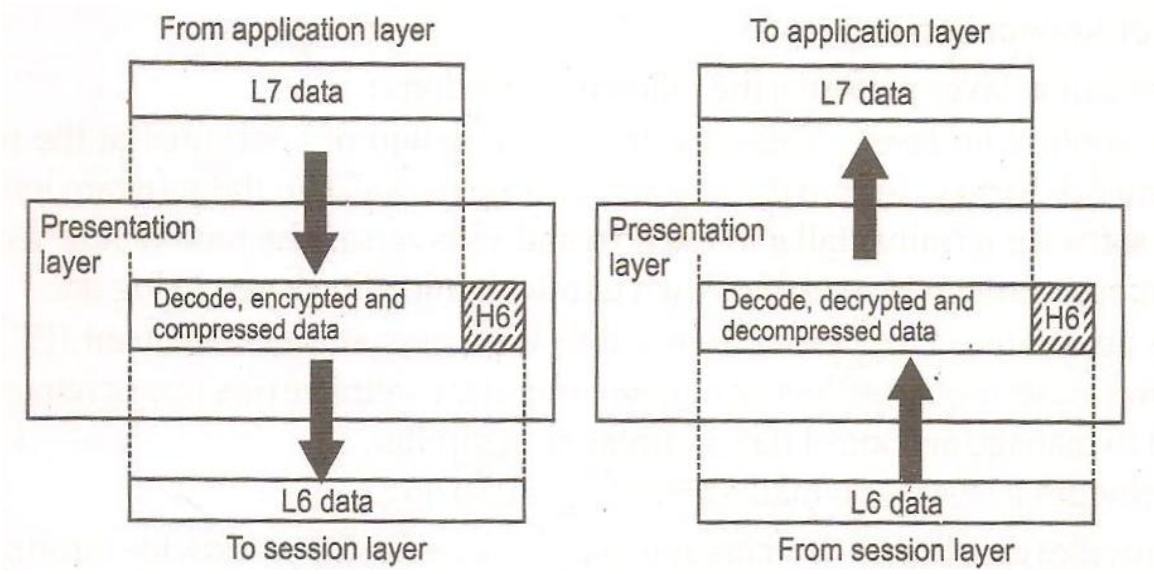


Figure 8.9 : Presentation layer

Functions of Presentation Layer

The Presentation layer performs the following function :

(i) It translates data between the formats the network requires and the format the computer expects (e.g. ASCII or EBCDIS).

(ii) It does the protocol conversion.

(iii) For security and privacy purpose, it carries out encryption at the transmitter and decryption at the receiver.

(iv) It carries out data compression to reduce the bandwidth of the data to be transmitted.

8.2.7 Application Layer

It is the topmost layer of OSI model. It provides services that directly support user application such as database access, e-mail and file transfer. It allows application to communicate with applications on other computers as though they were on the same computer. The relationship of the application layer to the user and the presentation layer is shown in figure 8.10.

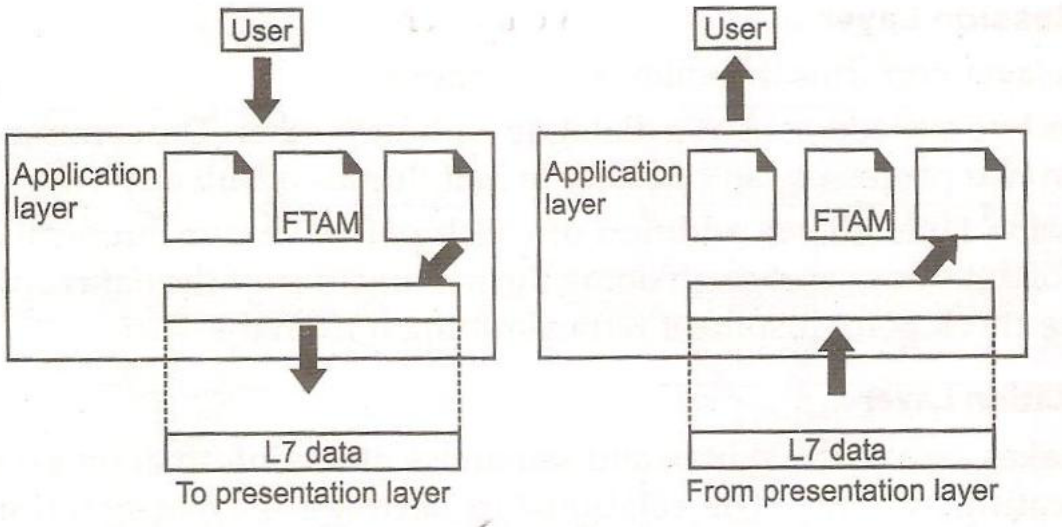


Figure 8.10 : Application layer

Functions of Application Layer

The application layer performs the following functions :

(i) The application layer creates a software emulation of a terminal at the remote host *(Network Virtual Terminal)*. The user's computer talks to the software terminal, then the software terminal talks to the host and vice-versa. The remote host fells that it is communicating with one of its own terminals and allows you to log on.

(ii) The application layer provides file transfer access and management (FTAM) which allows a user to access files in a remote computer to retrieve files from a remote computer and to manage or control files in a remote computer.

(iii) It provides a basis for e-mail forwarding and string.

(iv) It provides distributed database sources and access to the worldwide information about various objects and services.

8.3 Summary

An ISO standard that cover all aspects of networks communications is the Open System Interconnection (OSI) model. An open system is a model that allows any two different systems to communicate regardless of their underlying architecture.

The Open System Interconnection (OSI) model is a layered framework for network systems designing. This model allows for communication across all types of computer systems.

The physical layer co-ordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions to be performed by physical devices and interfaces for transmission to occur.

The data link layer transforms the physical layer to a reliable link and is responsible for node-to-node delivery. It make the physical layer appear error free to the upper layer (i.e., network layer).

The transport layer is responsible for source-to-destination (end-to-end) delivery of the entire

message. Whereas the network layer oversees end-to-end delivery of individual packet: it does not recognize any relationship between those packets. The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialogue controller. The presentation layer is concerned with the syntax and semantics of the information exchanged between systems. The application layer enables the user, whether human or software to access the network. It provides users interfaces and support for services such as electronic mail remote file access and transfer shared database management, and types of distributed information services. The TCP/IP protocol architecture is a result of protocol research and development conducted on the experimental packet switched network, ARPANET, funded by the Defense Advanced Research Projects Agency (DARPA), and is generally referred to as the TCP/P protocol suite. The TCP/IP model organizes the communication task into five relatively independent layers as under (i) Physical layer, (ii) Network access layer, (iii) Internet layer, (iv) Host-to-host, or transport layer, (v) Application layer.

8.4 Self-Assessment Questions

1. What do you mean by reference model?
2. Draw the OSI reference model and explain the functions of different layers.
3. Distinguish between TCP/IP and OSI reference models. Which model is more popular and why?
4. Write short technical note on : Connection oriented and connection less.
5. Explain the working of Transport, Session, Presentation and Physical layer of OSI model given by IEEE.

8.5 References

1. Behroz A Forouzen, "Data Communication and Networking", Mc-Grow-Hill, Publication, Fourth Edition, 2006.
2. Andrew, S. Tanenbaum, "Computer Networks", Person Education, Third Edition, 1999.

Unit-9

TCP/IP Protocol Suite

Structure of the Unit

9.0 Objective

After study of this unit student will be able to learn :

- The TCP/IP protocol suite
- Different layer KP/IP

9.1 Introduction

This model was developed before the OSI Reference Model, and the Internet Engineering Task Force (IETF) is responsible for the model and protocols developed under it. While the basic OSI model is widely used in teaching, OSI does not reflect real-world protocol architecture.

TCP/IP Model was developed by Department of Defense (DoD) research project to connect a number of different networks designed by different vendors into a network of networks (the Internet). The funding came through the DoD's Advanced Research Projects Agency (DARPA). At that time, DARPA had set up a network called ARPANET that connected government agencies, educational institutions and research sites together.

This task to create a protocol that worked on top of any physical structure was daunting because so many different types of machines were in use. That's why TCP/IP functions on layers above the Data Link and Physical OSI layers. Several computers in a small department can use TCP/IP (along with other protocols) on a single LAN. It was initially successful because, across a very large number of clients and server systems, it delivered a few basic services that everyone needs as: File transfer, E-mail and Remote login.

In the early 80s, TCP/IP was fully implemented across the ARPANET. The Internet is now the largest internetworking collection in the world offering packet switched services to millions of individuals. The Internet grew out of ARPANET that still exists as a subset of the larger entity. TCP/IP later was included with Berkeley Software Distribution (BSD) UNIX and has since become the foundation on which the Internet and the World Wide Web (WWW) are based.

A major development for TCP/IP was occurred in 1982 when developers at Berkeley University in California added TCP/IP support to their UNIX operating system (known as Berkeley UNIX). Today TCP/IP is a commercial success almost becoming the de-facto standard for inter-networks. The TCP/IP protocol suite provides services that function on all layers above the Data Link layer on the OSI model. Perhaps no other protocols designed to work above the Data Link and Physical OSI layers are as popular

as TCP/IP. That's primarily because this global protocol suite has been used by and continually promulgated by thousands of government and educational institutions world-wide.

TCP/IP was developed in the 1970s by the Defense Advanced Research Projects Agency (DARPA) for use in developing the Internet's protocols. DARPA started an inter-network called ARPANET which utilized TCP/IP. This model was named after two of its main protocols TCP and IP.TCP/IP protocol suite is also known as the Internet protocol suite. It is a set of rules for connections between networks of dissimilar computers over an internet i.e. to allow any type of computer to communicate with any other computer over the network. It is a Network model used in the current Internet architecture. Structure of the Internet is closely reflected by the TCP/IP model.

TCP/IP model is a layered abstract description for communications and computer network protocol design. It has fewer, less rigidly defined layers than OSI model and thus provides an easier fit for real world protocols.TCP/IP model is a universal standard for packet switched network. It is not only simply one application of rules, but many small applications that provide a host of functions for Internetworking.TCP/IP is not owned by any one organization, but accepted and used by almost all computer systems. Being flexible, it is becoming the protocol of choice and fills the networking needs of most organizations when it comes to interconnectivity. It is popular because it is the protocol used on the Internet.

To insure that all types of systems from all vendors can communicate, TCP/IP is absolutely standardized on the LAN. The original design of TCP/IP as a network of networks fits nicely within the current technological uncertainty. TCP/IP data can:

be sent across a LAN

be carried within an internal corporate SNA network

piggyback on the cable TV service

9.1 TCP/IP Layering Model

TCP/IP uses a networking model with two versions namely four layer and five layer model.The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers as given in the table below. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers where the last layer-network access layer is divided into two parts namely data link layer and physical layer.

Level	Name of the Layer	Description
Layer 4	Application or Process	User program
Layer 3	Transport or Host-to-Host	Higher level data encapsulation
Layer 2	Network or Internet	Lower level datagram transport
Layer 1	Network access or Host-to-Network	Network

Table 9.1: The original four layer versions

9.1.1 Layer 4: Application or Process Layer

This layer is broadly equivalent to the top three layers of the OSI model, namely: Application, presentation and session layers. This layer specifies how:

- Application requests from one computer to another are handled e.g. application access to the communication environment.
- Data representation conversions between two computers are dealt with
- Communications are initiated and terminated on the network

Protocols

The following are the protocols at this layer:

DNS , DHCP , FTP , HTTP , SMTP , SNMP , Gopher , IMAP4 , IRC , NNTP , XMPP , POP3 , SIP, SSH , TELNET , RPC , RTP , RTCP , RTSP , TLS/SSL , SDP , SOAP , BGP , PPTP , L2TP , GTP , STUN , NTP etc.

The SSL/TLS library operates above the transport layer (utilizes TCP) but below application protocols. There was no intention, on the part of the designers of these protocols, to comply with OSI architecture.

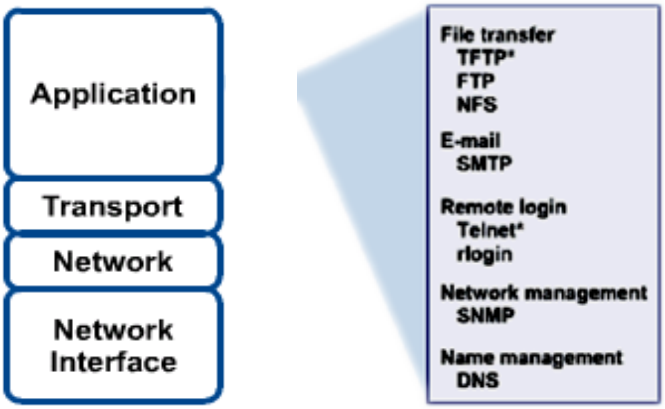


Figure 9.1: Main protocols at Application layer

Some important Application layer Protocols are discussed in Details as under:

(i) FTP (File Transfer Protocol)

FTP was originally designed to promote the sharing of files among the networked computers. Using this utility to copy data is typically referred to as *"FTPing"* a file. FTP is hardware independent, so its services can function just about anywhere.

Functions

Shields the users from the variations of file storage on different architectures Allows reliable and efficient file or data transfer between dissimilar computer systems such as between UNIX and Windows computers

(ii) TELNET (Remote Terminal Emulation)

It is a general two way protocol that provides the following functions:

- Remote Terminal emulation - provides terminal-type access to PCs
- Used to connect to another host and run applications on that host i.e. run a session
- Allows users to communicate with diverse or remote hosts

(iii) SMTP (Simple Mail Transfer Protocol)

It is the middle-man that uses UDP to move data around from one host to another. Applications run on both hosts that make use of SMTP. It happens to be the most widely used mail protocol on the Internet today.

Functions

- Handles the exchange of email information between computers through a series of other computers along the route.
- Not concerned with the format of messages but rather the way it gets to where it is going.

(iv) DNS (Domain Name System)

This protocol resolves the numerical address of a network node into its textual name or vice-versa. It would translate for e.g. "www.abc.com" to its equivalents IP address to allow the routing protocols to find the host that the packet is destined for.

DNS is a naming convention by which Internet Protocol (IP) addresses are stored in a database along with their corresponding domain names. Computers on the Inter-network have addresses that require 4 sets of numbers called the IP address. For instance, the IP address 165.76.124.82 would be hard to remember. So, with DNS enabled, the user could type in the domain name www.abc.com. The address is queried from the DNS server and the IP address is returned, thus the web site is connected to and loaded.

(v) SNMP (Simple Network Management Protocol)

This protocol uses UDP and is used to monitor network performance.

9.1.2 Layer 3: Host-to-Host or Transport Layer

This layer is similar to the OSI transport layer but with OSI session layer functionality. It ensures reliable data transfer from one computer to another i.e. application layer delivery service.

Functions

- Provides Levels or acknowledgement
- Handles Flow control
- Deals with opening and maintaining the connections
- Ensure the delivery of packets
- Allows the peer entities on source and destination hosts to carry on conversations
- Works as an interface between the Application layer and the complex hardware of the network
- Data may be user data or the control data
- Two modes of communication are available:
- *Full Duplex:* Both sides can transmit and receive the data simultaneously
- *Half Duplex:* One side at a time can send and receive

The session layer roughly corresponds to the Telnet virtual terminal functionality, which is part of text based protocols such as HTTP and SMTP, the TCP/IP model application layer protocols. It also corresponds to TCP and UDP port numbering, which is considered as part of the transport layer in the TCP/IP model. The presentation layer has similarities to the MIME standard, which also is used in HTTP and SMTP.

Protocols

The protocols at this layer are: TCP, UDP, DCCP, SCTP, RSVP etc.Computers running on the Internet communicate to each other using either TCP or the User Datagram Protocol (UDP).

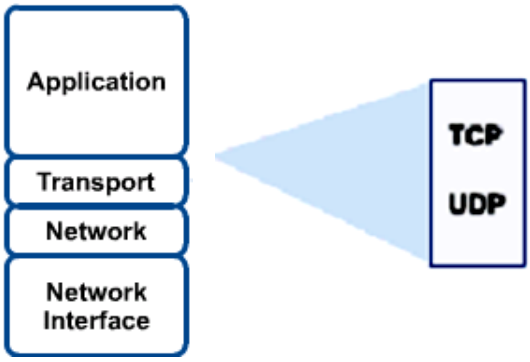


Figure 9.2: Main protocols at transport layer

Some important Transport layer Protocols are discussed in Details as under:

(i) TCP (Transmission Control Protocol)

It is the major transport layer protocol in TCP/IP suite. It is reliable connection oriented protocol which provides reliable transmission of data in an IP environment.

Functions

- Guarantees delivery of data packets and puts them in their proper orders
- Uses the datagram service
- Corresponds to the transport layer of the OSI reference model
- Provides error checking and flow control through a virtual link that it establishes and finally terminate
- Checks for errors after sending data, and if errors are detected, TCP resends the bad packet
- Would be utilized by FTP and SMTP - file transfer and email delivery have to be accurate and error free.

(ii) UDP (User Datagram Protocol)

It is bare-bones rapid transmission protocol that uses IP packets to deliver data with no reliability features like connections and acknowledgement.

Features

- *Unreliable (forte of UDP is speed not reliability)* - does not guarantee delivery
- *Connectionless* - designed for connectionless and unacknowledged communication links
- Used in NFS

Functions

- Provides data transmission with lower network traffic overhead than TCP
- Does not perform error checking and any flow control that is left to an Application process
- Provides data integrity (via a checksum) (TCP provides both data integrity and delivery guarantee by retransmitting until the receiver receives the packet)
- Works by adding information about the source and destination socket identifiers

For example when we write Java programs that communicate over the network, we are programming at the application layer. Typically, we don't need to concern ourself with the TCP and UDP layers. Instead, we can use the classes in the java.net package. These classes provide system-independent network communication. However, to decide which Java classes our programs should use, we do need to understand how TCP and UDP differ.

Later we will discuss the TCP and UDP in more detail.

9.1.3 Layer 2: Internet or Network Layer

Functions

- Decides the format of packets sent across the inter-network
- Inject packets over the network and have them travel independently to the destination
- Provides routing - Mechanisms used to forward packets from a computer through one or more
- routers to a final destination
- Defines IP addresses, with many routing schemes for navigating the packets from one IP address to another

Protocols

The protocols at this layer are as under:

IP (IPv4, IPv6), ICMP, IGMP, OSPF, ISIS, IPsec, ARP, RARP, RIP

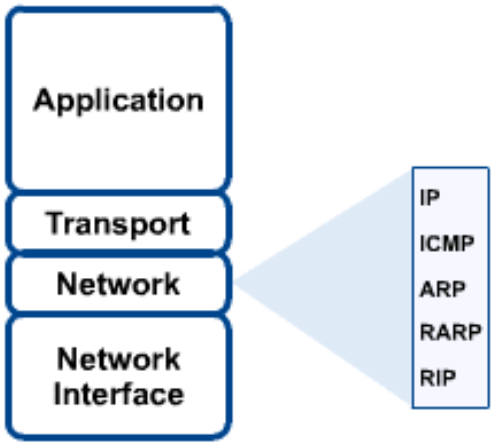


Figure 9.3: Main protocols at transport layer

(i) IP (Internet Protocol)

The Internet Protocol was developed to create a Network of Networks (Internet). Individual machines are first connected to a LAN *(Ethernet or Token Ring)*. TCP/IP shares the LAN with other uses *(a Novell file server, Windows for Workgroups peer systems)*. One device provides the TCP/IP connection between the LAN and the rest of the world.

Functions

- Provides connectionless communication with other computer systems

- Being connectionless, it neither does guarantee the delivery of data packets, nor the proper order of arrival of data
- Used for governing the official format of the packet
- Move packet from node to node
- Does no error checking, only the higher level protocols handle these features
- Forwards each packet based on a four byte destination address (the IP number)

The Internet authorities assign ranges of numbers to different organizations. The organizations assign groups of their numbers to departments. IP operates on gateway machines that move data from department to organization to region and then around the world.

Socket

It is a name given to the package of subroutines that provide access to TCP/IP on most of the systems.

Datagram

IP includes a specification of addresses and basic units of data transmission. The official name for the lowest level data `packages' in the internet protocol is datagram. Each datagram consists of a number of 32 bit words. The first six of these words consists of the IP header.

The size of datagram may be altered by the transport agents during the process of being sent. If a router transmits datagram from one physical network to another, and the second network uses a smaller packet size, it will divide datagram up into smaller datagram called fragments. The above header is then reproduced in each fragment together with a `fragment offset' which determines the order in which the fragments should be reconstructed at their final destination. The packet size on different physical networks is part of the low-level protocol definition. This is chosen when the physical layer is designed, based on the efficiency and speed of the network. On a slow network, a small packet size would be used so that the multi-user sharing of network time is more equitable, i.e. a greater number of packets per unit time can be sent if the packets are smaller. On the other hand, if the packet size is too small, the overhead becomes a significant portion of the total packet size and the transfer is inefficient.

(ii) ICMP (Internet Control Message Protocol)

ICMP and IGMP operate on top of IP but do not transport data like UDP or TCP. This functionality exists as layer management extensions to the OSI model Management Framework (OSIRM MF).

Functions

- Offers flow control and error-detection to the unreliable delivery method of IP
- Enables IP to include error detection and reporting mechanisms for transmission problems
- Provides a facility for routers and gateways on the net to communicate with a source if there is a problem. Routers send ICMP error messages to the original source of the datagram which caused the problem.
- Provides a mechanism for determining if a destination can not be reached

ICMP manages information transmitted through TCP/IP by allowing nodes to share error and status information. The information is then passed on to higher level protocols to notify the nodes of unreachable hosts and also to help resolve the transmission problems. If a route is congested or the data cannot reach its destination on a given route, the data is rerouted by the ICMP.

(iii) RIP (Routing Information Protocol)

It provides information for routing devices about pathways and number of hops to achieve them. It was popularized by its use in a Berkeley UNIX application called "Routed". RIP is ideal for smaller

networks, but considered impractical for larger inter-networks.

(iv) ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol)

These are special protocols to allow TCP/IP to interact in environments such as Ethernet. ARP maps TCP/IP addresses to Ethernet Data Link layer addresses. RARP maps the Ethernet Data Link layer address to the TCP/IP address.

ARP is a maintenance protocol that requests a computer's Media Access Control address *(network adapter address)* when only the Internet Protocol (IP) address is known. After the information is found, it is cached for later use. ARP can be used to update other systems' MAC address cache since it can be broadcast.

RARP is the same as ARP except it works in reverse. It will get an IP address of a computer node if only the MAC address is known. Certain domains such as the mil domain used for military access only can restrict public access by using the RARP protocol. It does this in the following manner:

Let's say a person is on a public dial-up Internet connection and tries to enter the web site indefense.mil. The mil site is restricted to only those computers using a military LAN under the mil domain. Before the user gets access, the mil server uses RARP to check the user's domain and compares it to see if it is the same domain. If it is, the web site loads. If it isn't, then a message occurs in the browser saying the site cannot be located or the server redirects the user to a web page telling him or her that only mil domains are authorized.

9.1.3 Layer 1: Network Access or Host-to-network Layer

This layer is supposed to be the combination of Data link layer and Physical layers corresponding to the OSI Model.

Functions

- Interfaces the TCP/IP protocol stack to the physical network
- Can access methods such as CSMA/CD
- Ensure that how to receive and transmit datagram

It deals with various forms of networking hardware (NIC, Modem etc.) and physical transmission media and related things as:

- How data is transmitted in its physical form as some sort of wave or pulsing electrical signal
- Signaling used on that networking equipment or hardware
- Low level protocols using that signaling

The TCP/IP model does not specify in any great detail, the operation of this layer, except that the host has to connect to the network using some protocol. So it can send IP packets over it. As it is not defined officially, it varies implementation to implementation, with vendors supplying their own version.

Host to network Layer Protocols

Host to network Layer is supposed to be a combination of the following two layers.

Data link layer

Physical layer

Hence the protocols at this layer are divided into two parts as given under.

Protocols at Data link layer

802.11, Wi Fi, WiMAX, ATM, DTM, Token Ring, Ethernet, FDDI, Frame Relay, GPRS, EVDO, HSPA, HDLC, PPP

Protocols at Physical layer

Ethernet physical layer, ISDN, Modems, PLC, SONET/SDH, G.709, OFDM, Optical Fiber, Coaxial Cable, Twisted Pair

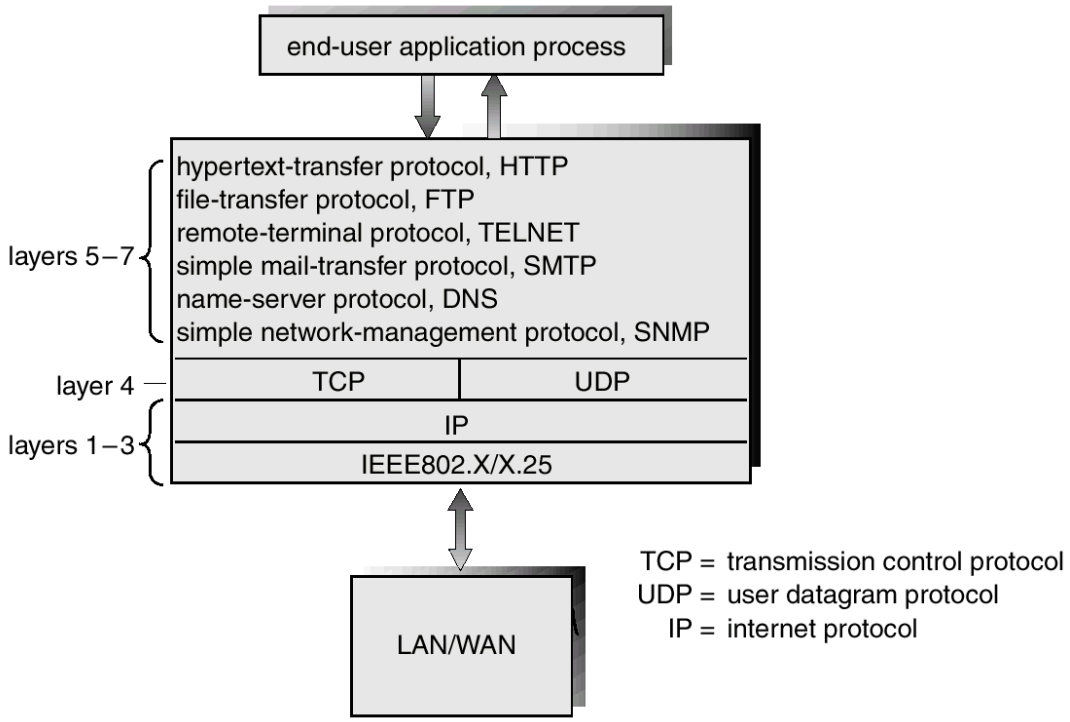


Figure 9.4: TCP/IP protocol stack

9.2 Comparison between OSI and TCP/IP Model

Concepts central to the OSI Model are:

(i) Services - tells what the layer does

(ii) Interfaces

- *Tells the processes above it, how to access it*
- *Specifies what parameters are*
- *Specifies what result to expect*

(iii) Protocols

It provides the offered service. It is used in a layer and are layers own business.

TCP/IP model did not originally distinguish between the service, interface and protocols. The only

real services offered by the Internet layer are:

- SEND IP packets
- RECEIVE IP packets

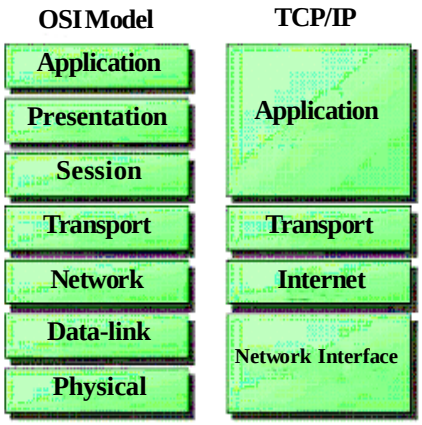


Figure 9.5: OSI and TCP/IP model

The OSI model was devised before the protocols were invented. Data link layer originally dealt with point to point networks. When broadcast Networks came around, a new sub-layer had to be hacked into the model. With TCP/IP, the reverse was true. The protocols came first and the TCP/IP model was really just a description of the existing protocols. the TCP/IP model did fit any other protocol stack.

The very important difference between the two occurs in the area of connectionless services and connection oriented services. The OSI model supports both these services in the Network layer but supports only connection oriented communication in the Transport layer. Whereas the TCP/IP model supports the connectionless communication in the Network layer and supports both these services in the Transport layer.

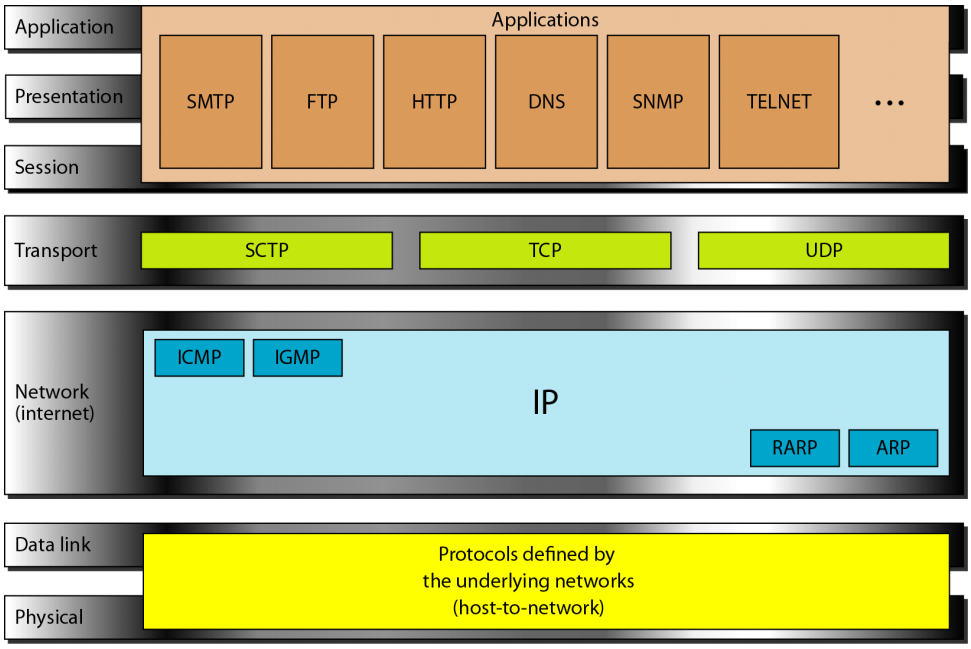


Figure 9.6: TCP/IP and OSI model with protocols

9.3 A Critique of the OSI Model

The OSI model did not take over the world due to the following reasons:

- Bad timing
- Bad technology
- Bad implementations
- Bad politics

Problems are as under:

- Service, interface and protocols are not distinguished
- Not a general model
- Host to network layer is really not a layer
- No mention of physical layer and data link layer
- Minor protocols deeply entrenched, hard to replace

The layers near the top are logically closer to the user application (as opposed to the human user) while those near the bottom are logically closer to the physical transmission of the data. Viewing layers as providing or consuming a service is a method of abstraction to isolate upper layer protocols from the nitty-gritty details of transmitting bits over, say, Ethernet and collision detection while the lower layers avoid having to know the details of each and every application and its protocol. This abstraction also allows upper layers to provide services that the lower layers cannot, or choose not, to provide. Again, the original OSI Reference Model was extended to included connectionless services (OSIRM CL). For example, IP is not designed to be reliable and is a best effort delivery protocol. This means that all transport layers must choose whether or not to provide reliability and to what degree. For multi-access links with their own addressing systems (e.g. Ethernet), an address mapping protocol is needed. Such protocols can be considered to be below IP but above the existing link system.

Ethernet is one form of cabling which is in common use. Other kinds of cables include:

- Fiber optics (FDDI)
- 10BaseT
- ISDN

9.4 TCP (Transmission Control protocol)

TCP provides the following Services:

(i) Connection Orientation

TCP is a connection-based protocol that provides a reliable flow of data between two computers. This feature requires an application to first request a connection to a destination, and then use the connection to transfer data. To use reliable transport services, TCP hosts must establish a connection-oriented session with one another.

When two applications want to communicate to each other reliably, they establish a connection and send data back and forth over that connection. This is analogous to making a telephone call. We send data back and forth over the connection by speaking to one another over the phone lines. Like the phone company, TCP guarantees that data sent from one end of the connection actually gets to the other end and

in the same order it was sent. Otherwise, an error is reported. Connection establishment is performed by using a "three-way handshake" mechanism. A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well. This is necessary so that packets are not to transmitted or retransmitted during session establishment or after session termination.

A single message of the TCP is called a segment. The TCP is a reliable or connection-oriented protocol as sufficient handshaking is provided to guarantee the arrival and the ordering of the segments at their destination. The ordering of each message implies a concept of two machines being continual contact with one another. This is like a telephone conversation: both parties are in contact all the time.

TCP is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP connections are useful for sending data to servers, where no particular reply is required. For example, it would be used to send print jobs to a printer queue across a network. The sender receives no reply from the print spooler, and wants every single line of data to arrive in the correct order without having to worry.

(ii) Point-to-Point Communication

This feature defines a TCP connection as having exactly two endpoints.

TCP provides a point-to-point channel for applications that require reliable communications. Examples of applications that require a reliable communication channel are:

- *The Hypertext Transfer Protocol (HTTP)*
- *File Transfer Protocol (FTP)*
- *TELNET*

The order in which the data is sent and received over the network is critical to the success of these applications. When HTTP is used to read from a URL, the data must be received in the order in which it was sent. Otherwise, we end up with:

- *A jumbled HTML file*
- *A corrupt zip file or*
- *Some other invalid information*

(iii) Reliability

This feature guarantees that data sent across a connection will be delivered exactly as sent, with no data missing or out of order. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. The major benefit of TCP is the reliability and this is achieved through a form of retransmission. A time-out mechanism allows devices to detect lost packets and request retransmission. TCP adds support to:

- *Detect errors or lost data*
- *Trigger retransmission until the data is correctly and completely received*

TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an inter-network.When data is received at the destination, TCP requires that acknowledgement be sent back to the sender. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. A timer is used when data is sent and if it

times out for an item of data without receiving an acknowledgement, it resends this item of data.

Bytes not acknowledged within a specified time period are retransmitted.

(iv) Full Duplex Communication

Full-duplex operation means that TCP processes can both send and receive at the same time. This feature allows:

o Data to flow in either direction

o Either application programs to send data at any time

(v) Stream Interface or stream data transfer

Stream interface is the process in which an application sends a continuous stream of data across a connection. With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers. This service benefits applications because they do not have to chop data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery.

(vi) Reliable Connection Startup

This feature requires two applications creating a connection to both agree on establishing the new connection.

(vii) Graceful Connection Shutdown

This feature guarantees the following in that order:

• an application program can open a connection

• *send arbitrary amounts of data*

• *and then request that the connection be shut down*

• *with all data reliably delivered before the connection is closed*

From the user's point of view, when we download a file from the Internet using File Transfer Protocol (FTP), it is using a form of TCP to break down a large file into packets and verifying that we receive each packet sent. On the other hand, when we e-mail a message to a friend, this connection is not established for the same reliability. The message is simply forwarded as a type of datagram directed to our friend's IP address. We can just think of TCP/IP as the way of doing things on the Internet. We send an e-mail message and it breaks down into smaller pieces, these eventually become plain pieces of data that can be transmitted across different kinds of networks. When the message fragments reach the destination, it is rebuilt to duplicate what we sent.

(viii) Flow Control

TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence number it can receive without overflowing its internal buffers.

(ix) Multiplexing

Multiplexing means numerous simultaneous upper-layer conversations can be multiplexed (mixed) over a single connection.

Additional TCP/IP-Related Protocols

There are several additional protocols designed to assist TCP/IP. Since routing is so important on a packet-switched network like the Internet, specialized protocols have been designed to assist in this function. Special protocols for determining addressing on the Internet have also been devised. Additionally, some additional protocols may be involved in error-checking and flow control, just to name a few. Let's explore some of these additional protocols that are included in the TCP/IP suite of protocols.

NFS (Network Filing System)

It was developed by Sun Microsystems Inc. It provides shared access to files in a very transparent and integrated way. NFS is only one contribution to a protocol suite that has found usage in nearly every sector of networking. It's continued acceptance and evolution will ensure that it stays around as am internetworking standard for a while.NFS is the network standard for UNIX environment distributed file systems. NFS provides a means for sharing files regardless of the individual file systems on each computer platform. To understand the import of NFS, we have to go back to the original goal of DARPA. The idea behind the ARPANET and the Internet was to provide communication between machines of incredible diversity. NFS has moved the TCP/IP much closer to achieving that goal.By providing a standard interface, NFS allows machines to use each other's filing systems transparently as if the machines were local and of the same species. This feat is accomplished using Remote Procedure Calls (RPC) and External Data Representation (XDR).

RPC provides a mechanism by which programmers can distribute an application over multiple resources. Effectively what happens is that a programmer divides an application up into a client and server section. These two will communicate normally except that RPC provides the communication link. He or she then integrates RPC code into both sections and the job is done. RPC handles the gathering of data and transmission of it from one section to the other. As RPC handles the transparent application execution, XDR provides transparent data flow from one hardware platform to another. Since different hardware platforms may require different representation of data, XDR acts as the common denominator. One machine encodes data and hands it off to XDR which in turn formats it correctly for the recipient machine. XDR is highly automated and greatly enhances and speeds the work of programmers who must move data between diverse platforms.

UDP (User Datagram Protocol)

UDP is a protocol that sends independent packets of data, called datagram, from one computer to another with no guarantees about arrival. The UDP protocol provides for communication that is not guaranteed between two applications on the network. When we use UDP transport, there is no guarantee that data will arrive at the destination and no confirmation of receipt is sent by the receiver.

UDP is not connection-based like TCP. It is called connectionless because the messages are sent one by one, without any concept of there being an on-going connection between the sender and receiver. Rather, it sends independent packets of data, called datagram, from one application to another. Sending datagram is much like sending a letter through the postal service: The order of delivery is not important and is not guaranteed, and each message is independent of any other. For many applications, the guarantee of reliability is critical to the success of the transfer of information from one end of the connection to the other. However, other forms of communication don't require such strict standards. In fact, they may be slowed down by the extra overhead or the reliable connection may invalidate the service altogether.

Consider, for example, a clock server that sends the current time to its client when requested to do so. If the client misses a packet, it doesn't really make sense to resend it because the time will be incorrect when the client receives it on the second try. If the client makes two requests and receives packets from the server out of order, it doesn't really matter because the client can figure out that the packets are out of order and make another request. The reliability of TCP is unnecessary in this instance because it causes

performance degradation and may hinder the usefulness of the service.

Another example of a service that doesn't need the guarantee of a reliable channel is the ping command. The purpose of the ping command is to test the communication between two programs over the network. In fact, ping needs to know about dropped or out-of-order packets to determine how good or bad the connection is. A reliable channel would invalidate this service altogether.

Many firewalls and routers have been configured not to allow UDP packets. If you're having trouble connecting to a service outside your firewall, or if clients are having trouble connecting to your service, ask your system administrator if UDP is permitted.

UDP is the simpler of the two transport layer protocols, since it requires no handshaking by the system. It is useful for applications which either need or want to provide their own form of handshaking. For example, it would be natural to use the UDP for a question-answer type of client-server system. The client knows that its question arrived if it gets an answer from the server, so asking the network protocols to guarantee it would be a waste of time. A single message of UDP encapsulated datagram is officially called a packet and is given a small header. This header contains no ordering information - so the order in which the packets arrive at their destination is not guaranteed by the protocol itself. Only the integrity of the data is checked, using a checksum.

9.4 Summary

- TCP/IP uses a networking model with two versions namely four layer and five layer and five layer model.
- Transport layer is similar to the OSI transport layer but with OSI session layer functionality.
- Host to network layer is supported to be a combination of data link and physical layer.
- The IP Address uniquely defines a host on the Internet.
- The port address identifies a process on a host.
- A specific address is a user-friendly address.

9.5 Self-Assessment Questions

1. What are the differences between OSI & TCP/IP reference model?
2. What are the resposibilities of the transport layer in the TCP/IP model?
3. Name some services provided by the application layer in the TCP/IP model.
4. List the layers of the TCP/IP model.
5. What is a peer-to-peer process?

9.6 References

1. Behroz A Forouzen, "Data Communication and Networking", Mc-Grow-Hill, Publication, Fourth Edition, 2006.
2. Andrew, S. Tanenbaum, "Computer Networks", Person Education, Third Edition, 1999.

Unit-10

Routing

Structure of the Unit

10.0 Objective

After study of this unit you will be able to learn

- The fundamental concept of routing
- Routing Algorithms.
- Concept of congestion
- How to control the congestion on network. This chapter covers algorithms for routing.

10.1 Introduction

The network layer is concerned with getting packets from the source all the way to the destination. The packets may require to make many hops at the intermediate routers while reaching the destination. This is the lowest layer that deals with end to end transmission. In order to achieve its goals, the network layer must know about the topology of the communication network. It must also take care to choose routes to avoid overloading of some of the communication lines while leaving others idle. The main

functions performed by the network layer are as follows:

- *Routing*
- *Congestion Control*
- *Internetworking*

10.1.1 Routing

Routing is the act of moving information across an internetwork from a source to a destination. Along the way, at least one intermediate node typically is encountered or it may be the process of finding a path from a source to every destination in the network. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. The primary difference between the two is that bridging occurs at Layer 2 (the data link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways.

Routing is performed for many kinds of networks, including the telephone network *(circuit switching)*, electronic data networks *(such as the Internet)*, and transportation networks.

Routing is the process of forwarding of a packet in a network so that it reaches its intended destination. The main goals of routing are:

1. Correctness: The routing should be done properly and correctly so that the packets may reach their proper destination.

2. Simplicity: The routing should be done in a simple manner so that the overhead is as low as possible. With increasing complexity of the routing algorithms the overhead also increases.

3. Robustness: Once a major network becomes operative, it may be expected to run continuously for years without any failures. The algorithms designed for routing should be robust enough to handle hardware and software failures and should be able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted and the network rebooted every time some router goes down.

4. Stability: The routing algorithms should be stable under all possible circumstances.

5. Fairness: Every node connected to the network should get a fair chance of transmitting their packets. This is generally done on a first come first serve basis.

6. Optimality: The routing algorithms should be optimal in terms of throughput and minimizing mean packet delays. Here there is a trade-off and one has to choose depending on his suitability.

10.1.2 Routing Components

Routing involves two basic activities:

(a) Determining optimal routing paths

(b) Transporting information groups *(typically called packets)* through an internetwork.

10.1.3 Path Determination

To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Route information varies depending on the routing algorithm used.Routing algorithms fill routing tables with a variety of information. Destination/next hop associations tell a router that a particular destination can be gained optimally by sending the packet to a particular router representing the *"next hop"* on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop

10.2 Routing Algorithms

Routing Algorithm can be differentiated based on several key characteristics. First, the particular goals of the algorithm designer affect the operation of the resulting routing protocol. Second, various types of routing algorithms exist, and each algorithm has a different impact on network and router resources. Finally, routing algorithms use a variety of metrics that affect calculation of optimal routes. The following sections analyze these routing algorithm attributes.

Usually Routing algorithms have one of these goals

- Rapid convergence
- Flexibility
- Robustness & Stability
- Optimality
- Simplicity and low overhead

Routing algorithms are usually flexible, which means that they should quickly and accurately adapt to a variety of network circumstances. Assume, for example, that a network segment has gone down. Routing algorithms will become aware of the problem , they will quickly select the next-best path for all the routes. It can also be programmed to adapt to changes in network bandwidth, router queue size, and network delay also.

The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on. If the subnet uses datagrams internally, this decision must be made a new for every arriving data packet since the best route may have changed since last time. If the subnet uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set up. Thereafter, data packets just follow the previously established route. The latter case is sometimes called session routing , because a route remains in force for an entire user session.

Routing algorithms can be grouped into two major classes:

Adaptive and non-adaptive

10.2.1 Adaptive algorithms

Adaptive algorithms, in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well. Adaptive algorithms differ in where they get their information *(e.g., locally, from adjacent routers, or from all routers),* when they change the routes *(e.g., every ?T sec, when the load changes, or when the topology changes),* and what metric is used for optimization *(e.g., distance, number of hops, or estimated transmit time).*

Adaptive algorithms are of the following:

(i). Distance vector routing

(ii). Link state routing

(iii). Broadcast routing

10.2.2 Non-adaptive algorithms

They do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from I to J (for all I and J) is computed in advance, off-line and downloaded to the route when the network is booted. This procedure is sometimes called static routing. Non-adaptive algorithms are of the following:

(a). Shortest path routing

(b). Flooding

(c) Flow-based routing

10.2.1.1 Distance Vector Routing

Distance vector routing is a dynamic algorithm. Distance vector routing algorithms operate by having each router maintain a table i.e., vector giving the best known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbors. The distance vector routing algorithm is sometimes called by other names, including the distributed *Bellman-Ford routing algorithm* and the *Ford Fulkerson algorithm*, in distance vector routing, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet.

This entry contains two parts: the preferred outgoing line to use for that destination and an estimate of the time of distance to that destination. The metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path, or something similar. The router is assumed to know the "distance" to each of its neighbors. If the metric is hope the distance is just one hop. If the metric is queue length, the router simply examines each queue. If the metric is delay, the router can measure it directly with special ECHO packets that the receiver just timestamps and sends back as fast as it can. An example, assume that delay is used as a metric and that the router knows the delay to each of its neighbors. Once every T msec each router sends to each neighbor a list of its estimated delays to each destination. It also receives a similar list from each neighbor. Imagine that one of these tables has just come in from neighbor X, with Xi?m msec via X. By performing this calculation for each neighbor, a router can find out which estimate seems the best and use estimate and corresponding line in this new routing table. Note that the old routing table is not used in the calculation.

Limitations

This algorithm does not prevent routing loops from happening and suffers from the count-to-infinity problem. The core of the count-to-infinity problem is that if A tells B that it has a path somewhere, there is no way for B to know if it is on the path. To see the problem clearly, imagine a subnet connected like A-B-C-D-E-F, and let the metric between the routers be "number of jumps". Now suppose that A goes down. In the vector-update-process B notices that its once very short route of 1 to A is down - B does not receive the vector update from A. The problem is, B also gets an update from C, and C is still not aware of the fact that A is down - so it tells B that A is only two jumps from it, which is false. This slowly propagates through the network until it reaches infinity.

10.2.1.2 Link State Routing

A Link-state routing is a concept used in routing of packet-switched networks in computer communications. Link-state routing works by having the routers tell every router on the network about its closest neighbors. The entire routing table is not distributed from any router, only the part of the table containing its neighbors. Some of the link-state routing protocols are the OSPF, IS-IS and EIGRP. Novell's NLSP (NetWare Link State Protocol) is also a link-state routing protocol, which only supports IPX. This type of routing protocol requires each router to maintain at least a partial map of the network. When a network link changes state (up to down, or vice versa), a notification, called a link state advertisement (LSA) is flooded throughout the network. All the routers note the change, and re-compute their routes accordingly

The idea behind link state routing is simple and can be stated as five parts. Each router must:

(i). Discover its neighbors and learn their network addresses.

(ii). Measure the delay or cost to each of its neighbor.

(iii). Construct a packet telling all it has just learned.

(iv). Send this packet to all other routers.

(v). Compute the shortest path to every other router.

In effect the complete topology and all delay are experimentally measured and distributed to every

router. Then to find the shortest path to every other router Dijkstra's algorithm is used considering five steps.

1. Learning about the Neighbors

When a router is booted, its first task is to learn who its neighbors are. It accomplishes this properly by sending a special HELLO packet on each point-to-point line. The route on the other end is expected to send back a reply telling who it is. These names must be globally unique.

2. Measuring Line Cost

The link state routing algorithm requires each router to know, or at least have a reasonable estimate, of the delay to each of its neighbors. The most direct way to determine this delay is to send a special ECHO packet over the line that the other side is required to send back immediate. By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay. For even better results the test can be conducted several times, and the average used.

3. Building Link State Packets

Once the information needed for the exchange has been collected, the next step is for each router to build packet containing all the data. The packet starts with the identity of the sender, followed by a sequence number and age, and a list of neighbors. For each neighbors, the delay to that neighbor is given.

4. Distributing the Link State Packets

The trickiest part of the algorithm is distributing the link state packets reliably. As the packets are distributed and installed, the routers getting the first ones will change their routes. Consequently, the different routers may be using different versions of the topology, which can lead to inconsistencies, loops, unreachable machine, and other problems.

5. Computing the New Routes

Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph because every link is represented. Every link is, in fact, represented twice, once for each direction. The two values can be averaged or used separately. Now Dijkstra's algorithm can be run locally to construct the shortest path to all possibled estimations. The results of this algorithm can be installed in the routing tables, and normal operation resumed.

10.2.1.3 Broadcast Routing

For some applications, hosts need to send message to many or all other hosts. For example, a service distributing weather reports, stock market updates, or live radio programs might work best by broadcasting to all machines and letting those that are interested read to data "sending a packet to all destinations simultaneously is called broadcasting".

Various methods of broadcast routing have been proposed for doing it.

1. One broadcast method is source to simply send a distinct packet to each destination.

2. Flooding is another obvious candidate. Although flooding is ill-suited for ordinary point-to-point communication. Here it generates too many packet and consumes too much bandwidth.

3. The third algorithm is multi destination routing. If this method is used, each packet Contains either a list of destinations or a bit map indicating the desired destinations.

Multi destination routing is like separately addressed packets, except that when several packets must follow the same route, one of them pays full fare and the rest ride free.

4. The fourth broadcasting method, based on the use of a spanning tree.i.e., A spanning tree is

connected sub-graph of the network that includes all nodes and has no cycles. It is more communication-efficient than flooding.

5.Last broadcast algorithm is reverse path forwarding. The advantage of this is that both reason ably efficient and easy to implement. It neither require outers to know about spanning tree, nor does it have the overhead of a destination list or bit map in each broadcast packet as does multidestination addressing. It doesn't require any special Mechanism to stop the process, as flooding does.

10.2.2 Non-adaptive algorithms

An important issue in a packet-switched networks is congestion or we can say that is the load on the network or the number of packets sent to the networks. Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity. Congestion happens in any system that in values waiting, like an accident during rush hour.In computer network congestion in a network or internetwork occurs became routers and switches have quees, and butter that hold the pockets before and after processing.

10.2.2.1 Shortest Path Routing

Many Practical routing algorithms are based on the notion of a shortest path between two nodes. Here, each communication link is assigned a positive number called it length. A link can have a different length in each direction. Each path between two nodes has a length equal to the sum of the lengths of its links. A shortest path routing algorithm route search packet along a minimum length *(or shortest)* path between the source and destination nodes of the packet. The simplest possibility is for each link to have unit length, in which case a shortest path is simply a path with minimum number of links. More generally, the length of a link may depend on hits transmission capacity and its projected traffic load. The idea here is that a shortest path should contain relatively few and non-congested links, and therefore be desirable for routing. A more sophisticated alternative is to allow the length of each link to change over time and to depend on the prevailing congestion level of the link. Then a shortest path may adapt to temporary overloads and route packets around points of congestion. This idea is simple but also contains some hidden pitfalls, because by making link lengths dependent on congestion, we introduce a feedback effect between the routing algorithm and the traffic pattern within the network.

An important distributed algorithm for calculating shortest paths to a given destination, known as the Bellman-ford method, has the form

$$Di = Mini[dij + Dj]$$

Where

Di is the estimated shortest distance of node to the destination.

dij is the length of the link (i , j).

Each node executes periodically this interaction with the minimum taken over all its neighbors *j*. Thus *dij + Dj* may be viewed as the estimate of shortest distance from node i to the destination subject to the constant of going through j, and minj *(dij + Dj)* may be viewed as the estimate of shortest distance from i to the destination going through the best neighbor.

Shortest path routing has the following two drawbacks:

- It uses only one path per origin-destination Pair thereby potentially limiting the throughout of the network.

- Its capability to adapt to changing traffic conditions is limited by its susceptibility to oscillations; this is due to the abrupt traffic shifts resulting when some of the shortest paths change due to changes in link lengths.

10.2.2.2 Flooding

During the operation of a data network, it is often necessary to broadcast some information that is, to send this information from an origin node to all other nodes.

For example, when there are changes in the network topology due to link failure and repairs, these changes must be transmitted to the entire network .Broadcasting could also be used as a primitive form of routing packet from a single transmitter to a single receiver. More generally, to a subnet of receivers, this use is generally rather inefficient, but may be sensible because it is simple or because the locations of the receivers within the network are unknown

A widely used broadcasting method is known as flooding. It operates as follows:

The origin node sends its information in the form of a packet to its neighbors (directly connected with a link). In turn the neighbors relay it to their neighbors, and so on, until the packet reaches all nodes in the network.

Two additional rules are also observed, which limit the number of packet transmissions.

- A node will not relay the packet back to the node from which the packet was obtained.
- A node will transmit the packet to its neighbors at most once, including on the packet the ID number of the origin node a sequence number, which is incremented with each new packet issued by the origin node, can ensure this by storing the highest sequence numbers that are less than or equal of its incident links. Note that with these rules, links need not preserve the order of packet transmissions, the sequence numbers can be used to recognize the correct order.

10.2.2.3 Flow Based Routing

The algorithms studied above take only the topology into account. They do not consider the load. Here we will study a static algorithm that uses both topology and load for routing. It is called flow-based routing. In some networks, the mean data flow between each pair of nodes is relatively stable and predictable. For example, in a corporate network for a retail store chain, each store might send orders, sales reports, inventory updates, and other well defined types of messages to known sites in a predefined pattern, so that the total volume of traffic varies little from day to day. Under conditions in which the average traffic from i to j s known in advance and, to a reasonable approximation, constant in time, it is possible to analyze the flows mathematically to optimize the routing.

The basic idea behind the analysis is that for a given line, if the capacity and average flow and known, it is possible to compute the mean packet delay on that line from queuing theory. From the mean delays on all the lines, it is straight forward to calculate a flow-weighted average to get the mean packet delay for the whole subnet.

To use this technique, certain-information must be known in advance.

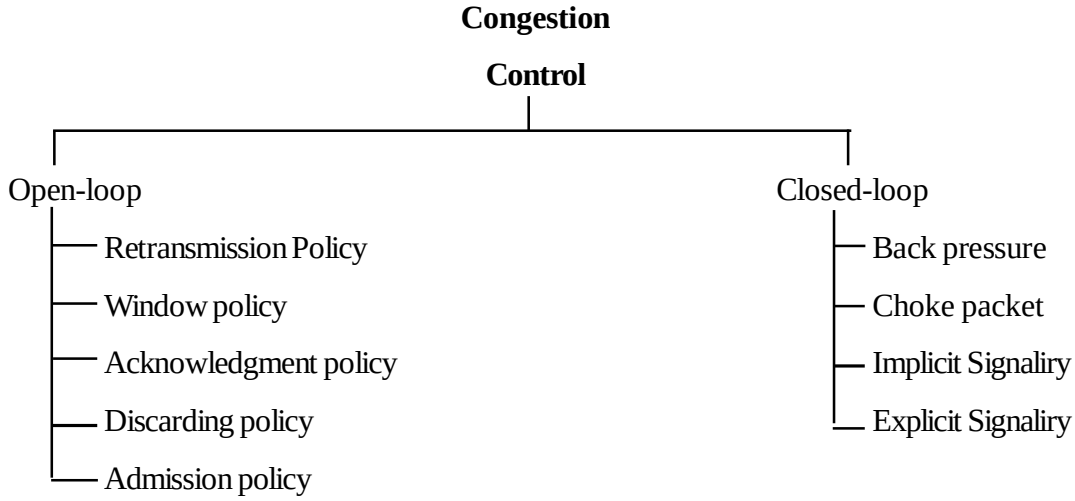
- The subnet topology must be known.
- The traffic matrix must be given.
- The line capacity matrix specifying capacity of each line in bps must be available.
- A routing algorithm must be chosen.

10.3 Congestion

Network congestion occurs when a link or node is carrying so much data that its quality of service deteriorates or when too many packets are present in a subnet, performance degrades t his situation is called congestion.In any network when there is too much the data traffic at a node that the network slows down or starts loosing data, it is known as network congestion. e.g. dropped calls on a telephone network.

10.4.1 Congestion Control

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories : Open-loop congestion control *(prevention)* and closed loop congestion control *(removal)* as shown in below figure :



10.5 Summary

- Routing is the act of moving intonation across an internetwork from a source to a destination.
- Routing algorithms can be grouped in two major charges Adaptive and non-adaptive.
- Adaptive algorithms, change their routing decisions to reflect charges in the topology usually the traffic as well.
- Non-adaptive algorithms, decisions on measurement or estimates of the current traffic and topology.
- A link state routing is a concept used in routing of pocket switched reworks in computer communications.
- Congestion is the load on the network or the number of pockets sent to the network.
- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens or remove congestion after it has happened.

10.6 Self-Assessment Questions

1. What is difference between adaptive and non-adaptive routing?
2. Describe the different types of routing algorithms.
3. What is congestion and why we required congestion control?
4. Write short note on :
   (a) Distance vector routing
   (b) Link state routing
   (c) Broad cast routing

10.7 References

1. Behroz A Forouzen, "Data Communication and Networking",Mc-Grow-Hill, Publication, Fourth Edition, 2006.
2. Andrew, S. Tanenbaum, "Computer Networks", Person Education, Third Edition, 1999.

Unit-11

Network Services

Structure of the Unit

11.0 Objective

After study of this unit student will learn the concept of network services like

- ATM
- ISD
- SONET/SDH.

11.1 Introduction

A network service is a service hosted on a computer network. Network services provide some functionality for members or users of the network. Services are usually based on a defined service protocol. Network services are hosted by servers to provide shared resources to client computers. The service software is often referred to as a port, daemon, or listener. A specific kind of service is often mapped to a specific port number for the underlying transmission protocol *(e.g. Internet Protocol, Transmission Control Protocol, and User Datagram Protocol).*

11.2 ATM

Asynchronous Transfer Mode (ATM) describes several related, standards-based technologies that

provide high-speed communication over a broad range of media. The International Telecommunication Union (ITU-T) defines ATM as "a high-speed, connection-oriented multiplexing and switching method specified in international standards utilizing fixed-length cells to support multiple types of traffic." Before you can decide whether to deploy ATM in your network, you need to understand how it integrates with current networking environments and how it functions in new networking environments.

Asynchronous Transfer Mode (ATM) is a wide array of services and concepts. At this time, ATM technologies are used selectively in local and wide area networks. Some networks have been completely transformed into native ATM networks, with software, end-station hardware, and network fabric all made up of ATM devices and drivers. In other networks, ATM is used only in the network backbone, shuttling data from one local area network (LAN) to another. In some instances, ATM is deployed in small pockets intermixed with standard LAN components and other networking technologies.

ATM is continually evolving. In some cases, its usefulness is judged by how well it emulates legacy networks; that is, how it compares with traditional LAN technologies such as Ethernet and Token Ring. In other cases, ATM provides so many clear advantages in terms of speed, manageability, and accuracy that it has quickly been recognized as the only viable solution.

11.2.1 Connection Types

There are following types of connections available at this time with ATM. Point-to-point connections can be unidirectional or bidirectional Point-to-multipoint can be unidirectional only. Multipoint-to-multipoint is not available yet. There is no method for a receiver to identify the cells from individual sources since the cells would be interleaved from multiple sources. This prohibits proper reassembly of the cells into the proper data frames at the receiver.

11.2.2 Architecture

ATM is a combination of hardware and software that can provide either an end-to-end network or form a high-speed backbone. The structure of ATM and its software components comprise the ATM architecture, as the following illustration shows. The primary layers of ATM are the physical layer, the ATM layer, and the ATM Adaptation layer.

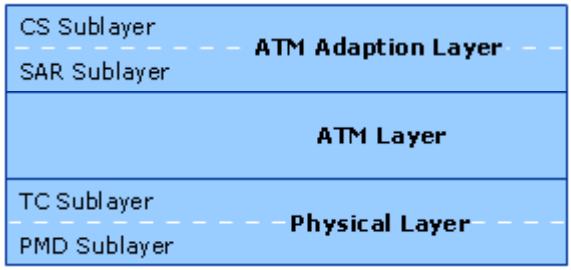


Figure 11.1 : ATM Layers

ATM Adaption Layer :

The ATM Adaptation layer facilitates the use of packets larger than a cell. Packets are segmented by the ATM interface, transmitted individually, and then reassembled on the receiving end. The ATM Adaptation Layer includes the Segmentation and Reassembly and Convergence sub layers.

ATM Layer : The ATM layer regulates cells and cell transport and establishes and releases Virtual Circuits. The ATM layer has no sub layers

Physical Layer : The Physical layer represents the physical medium and regulates Physical layer functions such as voltages and bit timing. The Physical layer consists of the Transmission Convergence and the Physical Medium Dependent sub layers

11.3 Frame Relay

Frame relay is a data link network protocol designed to transfer data on Wide Area Networks (WANs). Frame relay works over fiber optic or ISDN lines. The protocol offers low latency and to reduce overhead, does perform any error correction, which is instead handled by other components of the network.

Frame relay has traditionally provided a cost-effective way for telecommunications companies to transmit data over long distances. Frame relay is a synchronous HDLC protocol based network. Data is sent in HDLC packets, referred to as "frames". Frame relay is a technique used to transport data from locations to location, just like T-1 lines or ISDN connections do. In frame relay, there are a number of locations on the network that can send and receive data. These connections are known as Ports. Each location that needs access to the frame system, needs to have one of these ports.

Every port in a Frame Relay system has an Address. This address is Unique to the port at that specific location. The port is connected to the equipment that handles the Data on one side, to the Frame Relay Cloud on the other side. The equipment that handles the data can send data out the frame relay port. This happens in the form of Packets, or Frames.Each frame is built up of two parts; the actual Data and the Control block. These frames are sent over Virtual Connections.

11.3.1 Frame Relay Structure

The Frame Relay frame structure is based on the LAPD protocol. In the Frame Relay structure, the frame header is altered slightly to contain the Data Link Connection Identifier (DLCI) and congestion bits, in place of the normal address and control fields. This new Frame Relay header is 2 bytes in length and has the following format:

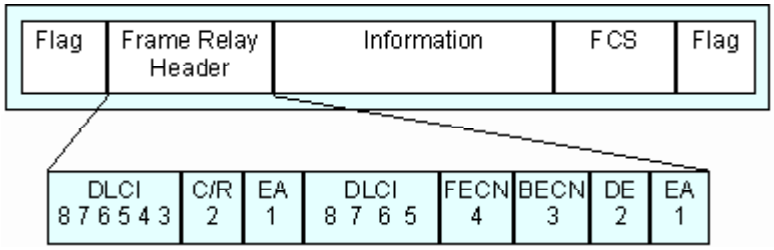


Figure 11.2 : Frame Relay header structure

Flags : Delimits the beginning and end of the frame. The value of this field is always the same and is represented either as the hexadecimal number 7E or the binary number 01111110.

Information : The Information field may include other protocols within it, such as an X.25, IP or SDLC (SNA) packet.

Data : Contains encapsulated upper-layer data. Each frame in this variable-length field includes a user data or payload field that will vary in length up to 16,000 octets. This field serves to transport the higher-layer protocol packet (PDU) through a Frame Relay network.

Frame Check Sequence (FCS) : Ensures the integrity of transmitted data. This value is computed by the source device and verified by the receiver to ensure integrity of transmission.

Frame Relay Header

Address Field (DLCI) - The first 6 bits of the first byte makes up the first part of the DLCI. The second part of the DLCI uses the first 4 bits of the second byte.10-bit DLCI field represents the address of the frame and corresponds to a PVC.

Command/ Response(C/R) - It allow upper layers to identity a frame is either as command or response.

Extended Address (EA) - It indicates whether the current byte is final byte of address. An EA of 0 means that another address byte is follow and 1 means that the current byte is final one.

Forward Explicit Congestion Notification (FECN) - Bit can set by any switch to indicate that the traffic is congested. This bit informs the destination that congestion has occurred. In this way, the destination knows that is should expect delay or loss of packets.

Backward Explicit Congestion Notification (BECN) - Bit is set to indicate that the congestion problem in network. This bit informs the sender that congestion has occurred. In this way, the source knows it needs to slow down to prevent the loss of packets.

Discard Eligibility (DE) - This bit indicates the priority level of the frame.

Explicit Congestion Notification (ECN) Bits

When the network becomes congested to the point that it cannot process new data transmissions, it begins to discard frames. These discarded frames are retransmitted, thus causing more congestion. In an effort to prevent this situation, several mechanisms have been developed to notify user devices at the onset of congestion, so that the offered load may be reduced.

Two bits in the Frame Relay header are used to signal the user device that congestion is occurring on the line: They are the Forward Explicit Congestion Notification (FECN) bit and the Backward Explicit Congestion Notification (BECN) bit. The FECN is changed to 1 as a frame is sent downstream toward the destination location when congestion occurs during data transmission. In this way, all downstream nodes and the attached user device learn about congestion on the line. The BECN is changed to 1 in a frame traveling back toward the source of data transmission on a path where congestion is occurring. Thus the source node is notified to slow down transmission until congestion subsides

11.3.2 Frame Relay Topologies

a. Hub and Spoke

The figure 11.3 is a hub-and-spoke topology diagram. It's a dedicated circuit point-to-point network to each branch office with the headquarter office. It is a very cost effective mechanism you can use.

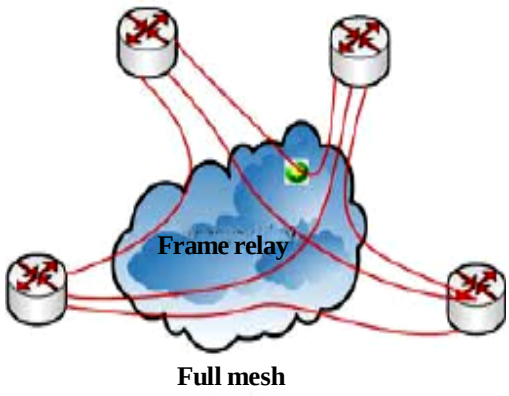


Figure 11.3 : Hub and Spoke topology

b. Full Mesh

The figure 11.4 is a full-mesh topology diagram. Every single unit has a dedicated circuit point-to-point. Every single branch office and central office has a single dedicated circuit. It's a very expensive deployment of the frame relay. Only critical sites where no single point of failure is acceptable. If one link to the site is failure, they still can link together from other links.

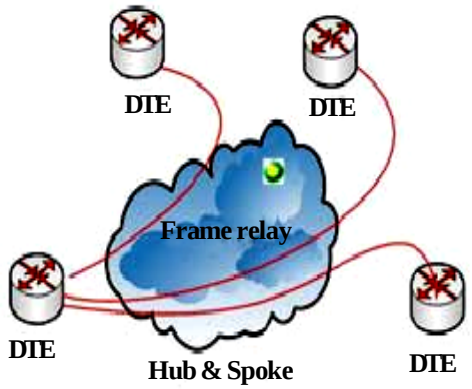


Figure 11.4 : Full mesh frame relay topology

c. Partial Mesh

Figure 11.5 is a partial mesh topology diagram : it's a less expensive than the full mesh topology where only several branch offices have a dedicated circuit to each other. Only critical sites are configured with redundant links.

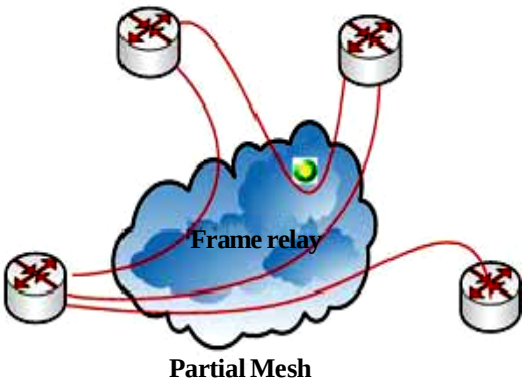


Figure 11.5 : Partial mesh frame relay topology

11.4 ISDN

ISDN is Integrated Services Digital Network. A digital telephone service that provides fast, accurate data transmission over existing copper telephone wiring and a fast way to go online. ISDN is based on a number of fundamental building blocks. First, there are two types of ISDN "channels" or communication paths:

• **B-channel**

The Bearer ("B") channel is a 64 kbps channel which can be used for voice, video, data, or multimedia calls. B-channels can be aggregated together for even higher bandwidth applications.

• **D-channel**

The Delta ("D") channel can be either a 16 kbps or 64 kbps channel used primarily for communications (or *"signaling"*) between switching equipment in the ISDN network and the ISDN equipment at your site.

These ISDN channels are delivered to the user in one of two pre-defined configurations:

• **Basic Rate Interface (BRI)**

ISDNBRI in used by service most people to connect to the Internet. An ISDN BRI connection supports two 64 kbps B-channels and one 16 kbps D-channel over a standard phone line. BRI is often called "2B+D" referring to its two B-channels and one D-channel. The D-channel on a BRI line can even support low-speed (9.6 kbps) X.25 data; however, this is not a very popular application in the United States.

BRI is the most common ISDN service for Internet access. A single BRI line can support up to three calls at the same time because it is comprised of three channels (2B+D). Two voice, fax or data "conversations," and one packet switched data "conversation" can take place at the same time. Multiple channels or even multiple BRI lines can be combined into a single faster connection depending on the ISDN equipment you have. Channels can be combined as needed for a specific application (a large multimedia file transfer, for example), then broken down and reassembled into individual channels for different applications (normal voice or data transmissions).

• **Primary Rate Interface (PRI)**

ISDN PRI service is used primarily by large organizations with intensive communications needs. An ISDN PRI connection supports twenty three (23) B-channels and one D-channel of 64 kbps (or 23B+D) over a high speed DS1 (or T-1) circuit. The European PRI configuration is slightly different, supporting 30B+D. ISDN offers the speed and quality that previously was only available to people who bought expensive, point-to-point digital leased lines. Combined with its flexibility as a dial-up service, ISDN has become the service of choice for many communications applications. Popular ISDN applications include:

• *Internet access*

• *Telecommuting/remote access to corporate computing*

• *Video conferencing*

• *Small and home office data networking*

11.4.1 ISDN Components

ISDN standards use function groups and reference points to describe the various components that can be utilized in making an ISDN connection. Function groups describe a set of functions that are implemented by a device and software.

In the figure below, router 1 is a router without a BRI interface so it uses a TA (ISDN Modem) to connect to the ISDN line. Router 2 has a BRI interface without a built-in NT1. Router 3 has a BRI interface with a built-in NT1. Router 4 is attached to a line that uses a NT2 device for the local PBX.

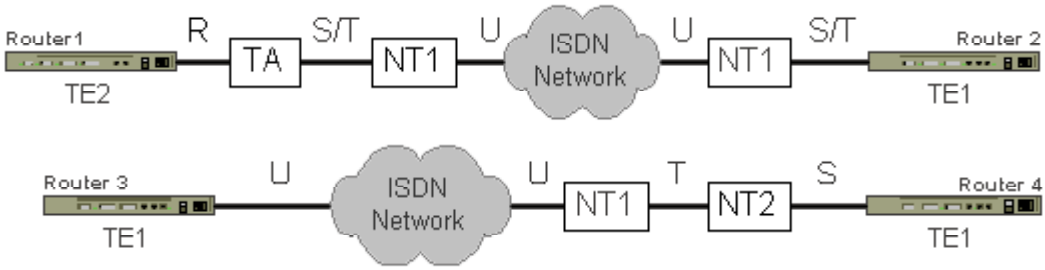


Figure 11.6 : Frame Function Groups and Reference Points

• *Terminal Adapter (TA) :* A converter device that allows non-ISDN devices to operate on an ISDN network.

• *Terminal Equipment 1 (TE1):* A device that supports ISDN standards and that can be connected directly to an ISDN network connection. For example, routers with integrated ISDN interfaces, ISDN telephones, personal computers, or videophones could function as TE1s.

`• *Terminal Equipment 2 (TE2) :* A non-ISDN device, such as a router, analog phone or modem, which requires a TA in order to connect to an ISDN network.

• *Network Termination 1 (NT1) :* A small connection box that is attached to ISDN BRI lines. This device terminates the connection from the Central Office (CO). Converts BRI signals for use by ISDN line.

• *Network Termination 2 (NT2) :* A device that provides switching services for the internal network. This type of interface is typically used with PRI lines, when they need to be divided for several functions. For example, some channels may be used for WAN data communications and others for the telephone system (such as PBX) and/or video tele-conferencing. It is a more complex NT1 that perfoms layer 2 and 3 functions.

The connection between two function groups (including cabling) is called a reference point.

ISDN Reference Points

• U - The U-interface is the actual two-wire cable, also called the local loop, that connects the Customer Premise Equipment to the telecommunications provider.

• R - The R-interface is the wire or circuit that connects the TE2 to the TA.

• S - The S-interface is a four-wire cable from TE1 or TA to the NT1 or NT2, which is a two-wire termination point.

• T - The point between the NT1 and NT2, is the T-interface. This four-wire cable is used to divide the normal telephone company's two-wire cable into four-wires, which then allows the connection of up to eight ISDN devices.

• S/T - When NT2 is not used on a connection that uses NT1, the connection from the router or TA to the NT1 connection is typically called S/T. This is essentially the combination of the S and T reference points.

11.5 SONET

The Synchronous Optical Network (SONET) standard for fiber optic networks was developed in the mid-1980s. It remains in widespread use today. In a nutshell, SONET allows multiple technologies and vendor products to interoperate by defining standard physical network interfaces.

The American National Standards Institute (ANSI) successfully devised SONET as the new standard for these applications. Like Ethernet, SONET provides a "layer 1" or interface layer technology (also termed physical layer in the OSI model). As such, SONET acts a carrier of multiple higher-level application protocols. For example, Internet Protocol (IP) packets can be configured to flow over SONET.

11.5.1 Technology

SONET commonly transmits data at speeds between 155 megabits per second (Mbps) and 2.5 gigabits per second (Gbps). To build these high-bandwidth data streams, SONET multiplexes together channels having bandwidth as low as 64 kilobits per second (Kpbs) into data frames sent at fixed intervals.

Compared to Ethernet cabling that spans distances up to100 meters (328 feet), SONET fiber typically runs much further. Even short reach links span up to 2 kilometers (1.2 miles); intermediate and long reach links cover dozens of kilometers.

11.5.2 SONET Layers

Each SONET network node ultimately derives its timing from an exceedingly precise and stable cesium atomic clock somewhere on the network, leading to the "synchronous" part of the name. The SONET model is totally different from the familiar OSI 7-layer model. The SONET model defines four layers:

• *Photonic*, which corresponds to the OSIs physical layer, defines the optical equipment's attributes (OC-n.) The tolerances in areas such as signal timing, jitter, phase shift, etc. required to maintain a synchronous network over a wide area are exacting, much more so than in asynchronous networks such as Ethernet, and we won't get into them here; those interested can order up the inches-thick Bellcore specifications for their reading enjoyment.

• *Section*, the frame format and certain low-level signal definitions, roughly corresponding to the OSI link layer.

• *Line*, the way in which lower-level frames are synchronized and combined into higher levels; you can sort of look at this as parts of the network and transport layers. The line layer also defines data channels carrying operations, administration, and maintenance and provisioning (OAM&P) information, which would be an application layer (like SNMP) in an OSI modeled network.

• *Path*, the end-to-end transport of a circuit, which also has application information (performance monitoring, status, tracing) for management.

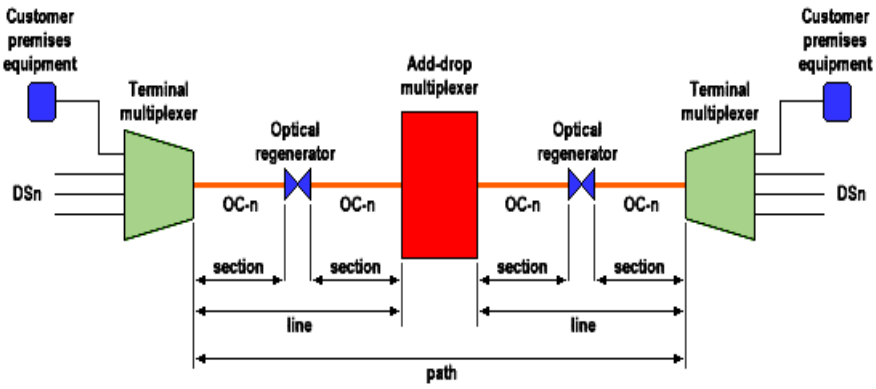


Figure 11.7 : SONET Layers

11.6 SDH

SDH *(Synchronous Digital Hierarchy)* is a standard technology for synchronous data transmission on optical media. It is the international equivalent of Synchronous Optical Network. Both technologies provide faster and less expensive network interconnection than traditional PDH *(Plesiochronous Digital Hierarchy)* equipment.

In digital telephone transmission, *"synchronous"* means the bits from one call are carried within one transmission frame. *"Plesiochronous"* means "almost (but not) synchronous," or a call that must be extracted from more than one transmission frame.

SDH uses the following Synchronous Transport Modules (STM) and rates: STM-1 (155 megabits per second), STM-4 (622 Mbps), STM-16 (2.5 gigabits per second), and STM-64 (10 Gbps).

11.6.1 Layers model of SDH

SDH networks are subdivided into various layers that are directly related to the network topology.

Physical layer - denotes the transmission medium. Example- a glass fiber or possibly a radio-link or satellite link.

Regenerator section - means the path between regenerators. Part of the overhead (RSOH, regenerator section overhead) is accessible for the signaling needed within this layer.

Multiplex section - binds the part of the SDH link between multiplexers. The remainder of the overhead (MSOH, multiplex section overhead) is used for the needs of the multiplex section.

VC layers -shows a part of the mapping process. Mapping is the process whereby the tributary signals, such as PDH and ATM signals are packed into the SDH transport modules. VC-4 mapping is used for 140 Mbps or ATM signals and VC-12 mapping is used for 2.048 Mbps.

Uppermost layer represents applications of the SDH transport network.

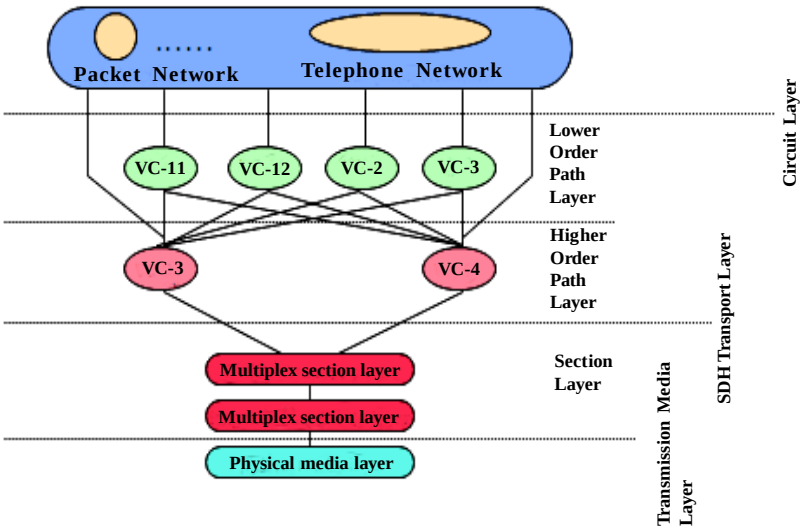


Figure 11.8 : SDH Layer architecture

11.6.2 Difference between SDH vs. SONET

SDH is basically the international version of SONET. It can be thought of as the *North American* version of SDH.The main differences are in the basic SDH and SONET frame formats, but SDH and SONET are essentially identical beyond the STS-3 signal level. The base signal for SONET is STS-1 and the base signal for SDH is STM-1. STS-3c is equivalent to STM-1 and the lower tributaries can be

mapped interchangeably between the two formats from that point on.In SDH, both electrical and optical signals are referred to as STM signals. In SONET, however, electrical signals are called STS and optical signals are referred to as OC.

11.7 Summary

- Frame relay s a relatively high-speed, cost-effective technology that can handle bursly data.
- ATM is a cell relay protocol that, in combination with SONET, allows high speed connections.
- ATM can handle real time transmission.
- ISDN is Integrated Services Digital Network. A digital telephone service that provides fast, accurate data tranmission over existing copper telephone wiring and a tast way to to online.

11.8 Self-Assessment Questions

1. What is a Network Service? Explain its concept.
2. What is the difference between SONET & SDH?
3. Explain the different types of Frame Relay topologies.
4. Write a short note on ISDN.
5. Discuss the frame Relay physical layer.
6. There are no sequence numbers in Frame Relay. Why?
7. What are the functions & ISDN?

11.9 References

1. Behroz A Forouzen, "Data Communication and Networking", Mc-Grow-Hill, Publication, Fourth Edition, 2006.
2. Andrew, S. Tanenbaum, "Computer Networks", Person Education, +Third Edition, 1999.

Unit-12

Network Applications

Structure of the Unit

12.0 Objective

This chapter provides a general overview of

- Applications of network
- Use of Teleconferencing
- Video conferencing applications
- Aim of Electronic banking
- Use of E-business
- Use of E-commerce

12.1 Introduction

When we speak of applications, we simply mean the things a computer or other tool can be used for. You are familiar with many applications, like word processing, email, web browsing, and spreadsheet

processing. We can distinguish between network and stand-alone applications. For example, if you use Microsoft Word to write a letter and save it on your PC, both the program and the data are stored on your computer. Since your computer does not have to be connected to a network, this is an example of a stand-alone application.In this class, our focus is on network applications-applications in which either the program you are using or the data you are working with or both reside on a network (often, but not always, the Internet).

Network applications are everywhere. Any time you browse the Web, send an email message, or pop up an X window, you are using a network application. Interestingly, all network applications are based on the same basic programming model, have similar overall logical structures, and rely on the same programming interface. Network applications rely on many of the concepts that you have already learned in our study of systems. For example, processes, signals, byte ordering, memory mapping and dynamic storage allocation all play important roles. There are new concepts to master as well. We will need to understand the basic client-server programming model and how to write client-server programs that use the services provided by the Internet. At the end, we will tie all of these ideas together by developing a small but functional web server that can serve both static and dynamic content with text and graphics to real Web browsers.

Network applications use a client-server architecture, where the client and server are two computers connected to the network. The server is programmed to provide some service to the client.The client is typically a desktop, laptop or portable device like an Apple iPhone. The server can be any of these, but is typically a computer in a data center.

12.2 Teleconferencing

The word 'Tele' means distance. The word *'conference'* means consultations or discussions. Through teleconferencing two or more locations situated at a distance are connected so that they can hear or both see and hear each other. It allows the distant sites to interact with each other and with the teaching end through phone, fax, and e-mail. The interactions occur in real time. This means that the learners/participants and the resource persons are present at the same time in different locations and are able to communicate with each other. In some situations, questions can be faxed/e-mailed early for response by the resource persons

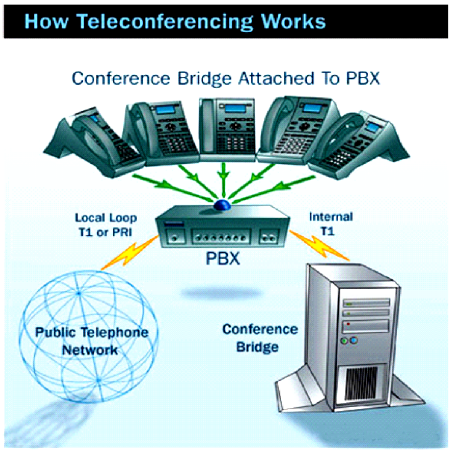


Figure 12.1 Teleconferencing work

12.2.1 Applications of Teleconferencing

Teleconferencing is essentially a means for communication and training. It can be used for information dissemination, guidance in response to policy, consultations with experts, focused group discussions,

interviews, etc. As a technology, it has broad applications in education, training and development, business/corporate communication, governanc, professional and medical courses/services.

a) Educationa

In the academic area, teleconferencing is useful for the following activities :

Delivery of full courses, lessons, tutoring, project work and training can be provided to the students through teleconferencing, Delivery of certificate level courses for professional development. These courses can be modular and multi-media in nature comprising print, contact programmes, and audio-video conferencing. Partial support to courses through counseling, etc. to address problems related to introduction of new curriculum, and lack of teachers and facilities. Tutoring in difficult areas of the curriculum. Remedial learning and off-hours teaching can be provided. Enrichment, updating, guidance to additional learning ad off-hours teaching can be provided. Enrichment, updating, guidance to additonal learning resources, extension of existing courses.Interaction by students with scientists, experts, decision and policy makers, etc. to obtain multiple perspectives on an issue.

Apart from academic activities, teleconferencing is used for administrative matters such as : Problems solving and counseling on admissions, examination, status of courseware materials distribution, Guidance and advice on course content, expectations, assignments, grading, credit, etc.

b) Training and Development

Teleconferencing is used to provide training and staff development for capacity building in agriculture, health, nutrition, family welfare, etc. in remote rural areas. It reaches out to a large number of groups such as community workers, farmers, functionaries, etc. for extension activities, sharing of experiences, raising of issues, introducing government schemes, projects, mobilizing for activities and conducting campaigns. Teleconferencing has been effectively used for empowerment of women and local self-government bodies and training of grass root workers spread over large geographical areas.

c) Business/Corporate Communication

In the business and corporate sector, teleconferencing has been used for a variety of purposes such as organizing conferences, interviews for recruitment, project supervision, problem solving, consultations, information dissemination and training of the personnel. Education, training, instruction, information and counseling are merged resulting in an overall improvement in staff performance.

d) Governance

Using teleconferencing facilities, planners, administrators and executives can directly and simultaneously interact with people at all levels for speedy dissemination of policy, execution and monitoring the implementation of projects, problem solving, and providing expert consultations.

e) Professional and Medicinal Courses and Services

Medicine is an area in which teleconferencing is being increasingly used. Hospitals can provide medical services to remote areas with expert diagnosis and medical advice. Similarly, many professional training institutes are using the teleconferencing mode to provide quality teaching support to widely dispersed student community.

12.2.2 Strengths of Teleconferencing

There is greater appeal, motivation and retention of information as a variety of teaching methodologies are used.By using animation, graphics and other techniques, teleconferencing is good at showing processes for demonstrations and experiments, thereby concretizing learning.

By conveying sights, sounds, and the spirit of the subject, it provides a more rounded view of an

issue.

It provides uniformity of training, which is interactive. On the basis of feedback, instructors can make appropriate shifts in the teaching strategies to meet learner needs.

The element of interactivity in teleconferencing is encouraged through dialogue and by stimulating responses to situations and visuals. The opportunity of dialogue allows the learners to discuss, question, and chellenge issues. Stimulting the lerners to respond to sitution nd visuls leads to higher processes of learning. As the learners become familiar become familiar with the technology and its parctices, their communication and learning skills are enhanced.

Interactivit gives a sense of participation and an active environment for learning. The learners feel themselves to be a part of the 'real-life' learning situation, and though located on different sites theyfeel they are connected. Relationships are established as in a group situation. For the field functionaries in remote rural areas, it reducess the sense of isolation, encourages sharing of concerns and ideas, and helps solve their problems.

12.2.3 Limitations of Teleconferencing

Teleconferencing has its limitations, but these can be overcome to a great extent by corrective measures and using appropriate content, planning, organization and management. For example, for effective interaction, there is a limit to the number of learning centers. If the number of centers is increased, time for interactivity for each center is correspondingly reduced. However, this can be overcome to a great extent by using fax and e-mail technologies along with telephone lines. Another way is to rotate the question-answer sessions among different groups of centers. This strategy would take care of language differences as well.

Since teleconferencing demands real time interaction, the learners are required to be present at particular times and places. It may be difficult for them to do so because of logistics problems and other reasons, resulting in poor attendance at the sessions. However, the proceedings can be recorded and sent to such learners as cannot attend at the learning centers. Experience shows that learners benefit a great deal even from recorded versions. For those who have participated, repeatability provides new insights.

12.3 Video Conferencing

Videoconferencing is the conduct of a videoconference *(also known as a video conference or videoteleconference)* by a set of telecommunication technologies which allow two or more locations to communicate by simultaneous two-way video and audio transmissions. It has also been called 'visual collaboration' and is a type of groupware.

Videoconferencing differs from videophone calls in that it's designed to serve a conference or multiple locations rather than individuals. It is an intermediate form of videotelephony, first deployed commercially in the United States by AT & T during the early 1970s as part of their dcevelopment of Picturephone technology. With the introduction of relatively low cost, high capacity broadband telecommunication services in the late 1990s, coupled with powerful computing processors and video compression techniques, videoconferencing usage has made significant inroads in business, education, medicine and media. Like all long distance communications technologies (such as phone and Internet), by reducing the need to travel to bring people together the technology also contributes to reductions in carbon emissions, thereby helping to reduce global warming.

Earlier, Videoconferencing uses audio and video telecommunications to bring people at different sites together. This can be as simple as a conversation between people in private offices (point-to-point) or involove several (multipoint) sites in large rooms at multiple locations. Besides the audio and visual transmission of meeting activities, allied videoconferencing technologies can be used to share documents and display information on whiteboards.

• The components required for a videoconferencing system include :

Video input : video camera or webcam

Video output : computer monitor, television or projector

Audio input : microphones, CD/DVD player, cassette player, or any other source of PreAmp audio outlet.

Audio output : usually loudspeakers associated witht the display device or telephone.

Data transfer : analog or digital telephone network, LAN or Internet

Compouter : a data processing unit thatties together the other components, does the compressing and decompressing, and initiates and maintains the data linkage via the network.

Videophone calls *(also : videocalls and video chat),* differ from videoconferencing in that they expect to serve individuals, not groups. However that distinction has become increasingly blurred with technology improvements such as increased bandwidth and sophisticated software clients that can allow for multiple parties on a call. In general everyday usage the term videoconferencing is now frequently used instead of videocall for point-to-point calls between two units. Both videophone calls and videoconferencing are also now commonly referred to as a video link.

Figure 12.2 : Video conferencing

12.3.1 Advantages of Video conferencing

There are many advantages to video conferences :

1. Companies are able to have meetings easily between branches that are situated very far away;

2. Companies are able to save on travel and hotel costs, previously incurred through transporting different employees to one place.

3. Meetings can be organized at short notice,

4. Employees are able to work from home, increasing work flexibility,

5. Meeting do not require large room facilities.

12.4 Electronic banking

Internet banking *(or E-banking)* means any user with a personal computer and a brower can get connected to his bank website to perform any of the virtual banking functions. In internet banking system the bank has a centralized database that is web-enabled. All the services that the bank has permitted on the internet are displayed in menu. Any service can be selected and further interaction is dictated by the nature of service. The traditional branch model of bank is now giving place to an laternative delivery channels with ATM network. Once the branch offices of bank are interconnected through terrestrial or satellite links,

there would be no physical identity for any branch. It would a borderless entity permitting anytime, anywhere and anyhow banking.

The network which connects the various locations and gives connectivity to the central office within the organization is called internet. These networks are limited to organizations for which they are setup. SWIFT is a live example of internet application.

12.4.1 Advantage of E-banking

As per the Internet and Mobile Association of India's report on online banking 2006, "There are many advantages of online banking. It is convenient, it isn't bound by operational timings, there are no geographical barriers and the services can be offered at a miniscule cost."

Through Internet banking, you can check your transactions at any time ofthe day, and as many times as you want to. Where in a traditional method, you get quarterly statements from the bank. Ifthe fund transfer has to be made outstation, where the bank does not have a branch, the bank would demand outstation charges. Whereas with the help of online banking, it will be absolutely free for you.

You can avail the following services through E-banking

a) Bill payment service : You can facilitate payment of electricity and telephone bills, mobile phone, credit card and insurance premium bills as each bank has tie-ups with various utility companies, service providers and insurance companies, across the country. To pay your bills, all you need to do is complete a simple one-time registration for each biller. You can also set up standing instructions online to pay your recurring bills, automatically. Generally, the bank does not charge customers for online bill payment.

b) Fund transfer : You can transfer any amount from one account to another ofthe same or any another bank. Customers can send money anywhere in India. Once you login to your account, you need to mention the payee's account number, his bank and the branch. The transfer will take place in a day or so, whereas in a traditional method, it takes about three workign days, ICICI Bank says that online bill payment service and fund transfer have been their most popular online services.

c) Credit card customers : With Internet banking, customers can not only pay their credit card bills online but also get a loan on their cards.If you lose your credit card, you can report lost card online. Railway pass this is something that would interest all the aam janta. Indian Railways has tied up with ICICI bank and you can now make your railway pass for local trains online. The pass will be delivered to you at your doorstep. But the facility is limited to Mumbai, Thane, Nashik, Surat and Pune. Investing through Internet banking. You can now open an FD online through funds transfer. Now investors withinterlinked demat account and bank account can easily trade in the stock market and the amount will be automitically debited from their respective bank accounts and the shares will be credited in their demat account. Moreover, some banks even give you the facility to purchase mutual funds directly from the online banking system.

Now a days, most leading banks offer both online banking and demat account. However if you have your two accounts. Recharging your prepaid phone. Now just top-up your prepaid mobile cards by logging in to Internet banking. By just selecting your operator's name, entering your mobile number and the amount for recharge, your phone is again back in action within few minutes.

Electronic banking in India

The Reserve Bank of India constituted a working group on Internet Banking. The group divided the internet banking products in India. These are :

a) Information Only System :

General purpose information like interest rates, branch location, bank products and their features, loan and deposit calculations are provided in the banks website. There exist facilities for downloading various types of application forms. The communication is normally done through e-mail. There is no interaction between the customer and bank's application system. No identification of the customer is done. In this system, there is no possibility of any unauthorized person getting into production systems of the bank through internet.

b) Electronic Information Transfer System :

The system provides customer-specific information in the form of account balances, transaction details, and statement of accounts. The informationis still largely of the 'read only' format. Identification and authenticationofthe customer is through password. The information is fetched from the bank's application system either in batch mode or off-line. The application systems cannot directly access through the internet.

c) Fully Electronic Transactional System :

This system allow bidirectional capabilities. Transactions can be submitted by the customer for online update. This system requires high degree of security and control. In this environment, web server and application systems are linked over secure infrastructure. It comprises technology convering computerization, networking and security, inter-bank payment gateway and legal infrastructure.

d) Automated Teller Machine (ATM) :

ATM is designed to perform the perform the most important function of bank. It is operated by plastic card with its special features. The plastic card is replacing cheque, personal attendance of the customer, banking hours restrictions and paper based verification. There are debit cards. ATMs used as spring board for Electronic Fund Transfer. ATM itself can provide information about customers account and also receive instructions from customers-ATM cardholders. An ATM is an Electronic Fund Transfer terminal capable of handling cash depsits, transfer between accounts, balance enquires, cash withdrawals and pay bills. It may be on-line or off-line. The on-line ATM enables the customer to avail banking facilities from anywhere. In off-line the facilities are confined to that particular ATM assigned. Any customer possessing ATM card issued by the Shared Payment Network System can go to any ATM linked to Shared Payment Networks and perform his transactions.

e) Pay by Phone Systems:

Let consumers phone their financial institutions with instructions to pay certain bills or to transfer funds between accounts.

12.4.2 Types of Electronic Currency

a) Credit Cards/Debit Cards : The Credit Card holder is empowered to spend wherever and whenever he wants with his Credit Card within thelimits fixed by his bank. Credit Card is a post paid card. Debit Card, on the other hand, is a prepaid card with some stored value. Everytime a person uses this card, the Internet Banking house gets money transfered to its account from the bank of the buyer. The buyers account is debited with the exact amount of purchases. An individual has to open anaccount with the issuing bank which gives debit card with a Personal Identification Number (PIN). When he makes a purchase, he enters his PIN on shops PIN pad. When the card is slurped through the electronic terminal, it dials the acquiring bank system-either Master Card or VISA that validates the PIN and finds out from the issuing bank whether to accept or decline the transactions. The customer can never overspend because the system rejects any transaction which exceeds the balance in his account. The bank never faces a default because the amount spent is debited immediately from the customers account.

b) Smart Card : Bank are adding chips to their current magnetic stripe cards to enhance securityand offer new service, called Smart Cards. Smart Cards allow thousands of times of information storable on magnetic stripe cards. In addition, these cards are highlysecure, more reliable and perform multiple functions. They hold a large amount of personal information, from medical and health history to personal banking and personal preferences. Sometimes called stored-value cards, have a specific amount of credit embedded electronically in the card. For example, a $ 100 smart card that you have purchased in advance can be used to cover expenses such as pay phone charges, bridge or expressway tolls, parking fees or Internet purchases. These cards make the transaction fast, easy and convenient.

Smart card techonlogy is in a period of rapid change. Ultimately consumers should be able to customize their smart cards to suit their financial needs with access from their personal compouter or cellular phone. Some improtant consumer issues are :

- Smart cards are the equivalent of cash somust be guarded.
- Procedures for recovering the value of a malfunctioning smart card are unclear.

The compouter chip within the card will contain both financial and personal information. Privacy and securtiy issues could be a problem.

c) Digital cash is designed to allow the consumer to pay cash rather than use a credit card topurchase products on the Internet. One type of digital cash allows consumers to transfer money froma financial institution or a credit card into an "electronic purse". The cash is held in a special bank account that is linked to your compouter. Another type of digital cash converts money into digital coins that can be placed on your compouter's hard drive.

d) Digital checks allow consumers to use their personal computers to pay recurring bills. Consumers can use computer software provided by a bank, or theycan use personal finance software packages such as Quicken or Microsoft Money and subscribe to an electronic bill-paying service.

The technology of paying bills electronically by home compouters is advancing rapidly, but relatively few businesses currently can accept payments made directly by computers. Privacy and security issues are major consumer concerns. Encryption technologymay lessen privacy concerns in the future.

12.4.3 Disadvantages of E-banking

The 1978 Electronic Funds Transfer Act is the governing statute while the Federal Reserve Board's Regulation 'E' provides guidelines on elelctronic funds transfer card liability. The regulations require that :

a) A valid EFT card can be sent only to a consumer who requests it.

b) Unsolicited cards can be issued only if the card cannot be used until validated.

c) The financial institution must inform you of your rights and responsibilities under the law in a written Disclosure Statement, including the procedure to correct errors in your periodic statements.

d) The user is entitled to a written receipt when making deposits or withdrawals from an ATM or using a point-of-sale terminal to make a purchase. The receipt must show the amount, date and type of transfer.

e) Periodic statements must confirm the amount of all transfers, the dates and types of transfers, type of accounts to or from which funds were transferred, and the address and phone number to be used for inquireies regarding the statement.

Problems and Errors. You have 60 days from the date a problem or error appears on your written terminal receipt or on your periodic statement to notify your financial institution. If you fail to notify the financial institution of the error within 60 days, you may have little recourse. Under federal law, the financial institution has no obligation to conduct an investigation if you have missed the 60-day deadline.

Lost cards. If you report an ATM or EFT card missing before it is used without your permission, the card issuer cannot hold you responsible for any unauthorized withdrawals. If unauthorized use occurs before you report it, the amount you can be held responsible for depends upon how quickly you report the loss. If you report the loss within two business day after you realized the card is missing but you do report its loss within 60 days after your statement is mailed to you, you could lose a much as $ 500 because of an unauthorized withdrawal.

If you do not report an unauthorized withdrawal within 60 days after your statement is mailed, you risk losing all the money in your account plus the unused portion of your maximum line of credit established for overdrafts.

12.5 E-business

Electronic business, commonly referred to as *"eBusiness"* or *"e-business"*, or an internet business, may be defined as the application of information and communication technologies in support of all the activities of business. Commerce constitutes the exchange of products and services between businesses, groups and individuals and can be seen as one of the essential actvities of any business. Electronic commerece focuses on the use of ICT to enable the external activities and relationships of the business with individuals, groups and other businesses.

The term *"e-business"* was coined by IBM's marketing and Internet teams in 1996.

Electronc business methods enable companies to link their internal and external data processing systems more efficiently and flexibly, to work more closely with supplier and partners,and to better satisfy the needs and expectations of their customers.

In practice, e-business is more than just e-commerce. While e-business refers tomore strategic focus with an emphasis on the functions that occur using electronic capabilities, e-commerce is a subset of an overall e-business strategy. E-commerce seeks to add revenue streams using the World Wide Web or the Internet to build and enhance relationships with clients and partners and to improve efficiency using the Empty Vessel strategy.

12.5.1 Applications of E-business

E-Business involves business processes spanning the entire value chain :

- Electronic purchasing and supply chain management,
- Processing orders electronically,
- Handling customer service,
- Cooperating with business partners.
- Special technical standards for e-business facilitate the exchange of data between companies.
- E-business software solutions allow the integration of intra and inter firm business processes.
- E-business can be conducted using the Web.
- Internet,
- Intranet
- Extranet, or some combination of these.

Basically, electronic business (EB) is the process of buying, transferring, or exchanging products, services, and/or information via computer networks, including the internet. EB can also be beneficial from many perspectives including business process, service, learning, collaborative, community.

12.5.2 Security in E-business

E-Business systems naturally have greater securityrisks than traditional business systems, therefore it is important for e-business systems to be fully protected against these risks. A far greater number of people have access to e-businesses through the internet than would have access to a traditional business. Customers, suppliers, employees, and numberous other people use any particular e-business system daily and expect their confidential information to stay secure. Hackers are one of the great threats to the security of e-businesses. Some common security concerns for e-business include keeping business and customer information private and confidential, authenticity of data integrity. Some of the methods of protecting e-business security and keeping information secure include physical security measures as well as data storage, data transmission, anti-virus software, firewalls, and encryption to list a few.

Many different forms of security exist for e-businesses. Some general security guidelines include areas in physical security, data storage, data transmission, application development, and system administration.

a) Physical security

Despite e-business being business done online, there are still physical security measures that can be taken to protect the busness as a whole. Protecting against the environment is equally important in physical security as protecting against unauthorized users.

In addition to keeping the servers and computers safe, physical security of confidential information is important. This includes client information such as credit card numbers, checks, phone numbers, etc. It also includes any of the organization's private information. Locking physical and electronic copies ofthis data in a drawer or cabinet is one addtional measure of security. Doors and windows leading into this area should also be securely locked. Only employees that need to use this information as part of their job should be given keys.

b) Data storage

Storing data in a secure manner is very improtant to all businesses, but especially to e-businesses where most of the data is stored in an electronic manner. Data that is confidential should not be stored on the e-business' server, but instead moved to another physical machine to be stored. If possible this machine should not be directly connected to the internet, and should also be stored in a safe location. The information should be stored in an encrypted format.

Any highly sensitive informationshould not be stored if it is possible. If it does need to be stored, it should be kept on only a few reliable machines to prevent easy access. Extra security measures should be taken to protect this information (such as private keys) if possible. Additionally, information should be kept secure wiht the same security measures as the original information. Once a backupis no longer needed, it should be carefully but thoroughly destroyed.

c) Data transmission and application development

All sensitive information being transmitted should be encrypted. Businesses can opt to refuse clients who can't accept this level of encryption. Confidential and sensitive information should also never be sent through e-mail. If it must be, then it should also be encrypted.

Transferring and displaying secure information should be kept to a minimum. This can be done by never displaying a full credit card number for example. Only a few of the numbers may be shown, and changes to this information online.Source code should also be kept in a secure location. It sould not be visible to the public.Applications and changes should be tested before they are placed online for reliability and compatibility.

d) System administration

Security on default operating systems should beincreased immediately. Patches and software updates should be applied in a timely manner. All system configuration changes should be kept in a log and promptly updated.

System administrators should keep watch for suspicious activity within the business by inspecting log files and researching repeated logon failures. They can also audit their e-business system and look for any holes in the security measures. It is important to make sure plans for security are in place but also to test the security measures to make sure they actually work. With the use of social engineering, the wrong people can get a hold of confidential information. To protect against this, staff can be made aware of social engineering and trained to properly deal with sensitive information.

E-businesses may use passwords for employee logons, accessing secure information, or by customers. Passwords should be made impossible to guess. They should consist of both letters and numbers, and be at least seven to eight digits long. They should not contain any names, birth dates, etc. Passwords should be changed frequently and should be unique each time. Only the password's user should know the password and it should never be written down or stored anywhere. Users should also be locked out ofthe system after a certain number of failed logon attempts to prevent guessing of passwords.

12.6 E-commerce

In its simplest form Ecommerce is the buying and selling of products and services by businesses and consumers over the Internet. People use the term "ecommerce" to describe encrypted payments on the Internet. Sometimes these transactions include the real-time transfer of funds from buyer to seller and sometimes this is handled manually through an eft-pos terminal once a secure order is received by the merchant.

Electronic Data Interchange (EDI) is the electronic exchange of business documents in a standard, computer-processable, universally accepted format between trading partners. EDI is quite different from sending electronic mail messages or sharing files through a network, or a bulletin board. Data is exchanged in standard predefined format, it becomes possible to exchange business documents irrespective of the computerized business application at either end of communication.

Internet sales are increasing rapidly as consumers take advantage of lower prices offer by wholesalers retailing their products. This trend is set to strengthen as web sites address consumer security and privacy concerns.

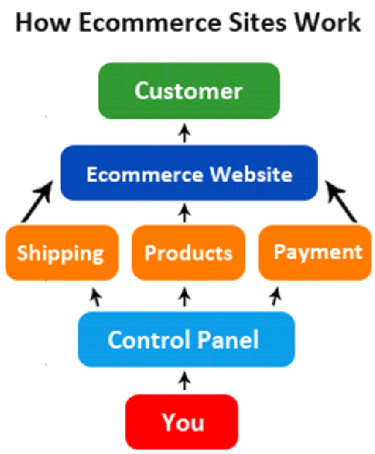


Figure 12.3 : E-commerce

12.6.1 Advantages of E-commerce:

E-commerce can provide the following benefits over non-electronic commerce:

• *Reduced costs* by reducing labour, reduced paper work, reduced errors in keying in data, reduce post costs

• *Reduced time*. Shorter lead times for payment and return on investment in advertising, faster delivery of product

• *Flexibility with efficiency*. The ability to handle complex situations, product ranges and customer profiles without the situation becoming unmanageable.

• *Improve relationships with trading partners*. Improved communication between trading partners leads to enhanced long-term relationships.

• *Lock in Customers*. The closer you are to your customer and the more you work with them to change from normal business practices to best practice e-commerce the harder it is for a competitor to upset your customer relationship.

• *New Markets*. The Internet has the potential to expand your business into wider geographical locations.

12.6.2 Disadvantages of E-commerce

• Any one, good or bad, can easily start a business. And there are many bad sites which eat up customers' money.

• There is no guarantee of product quality.

• Mechanical failures can cause unpredictable effects on the total processes.

• As there is minimum chance of direct customer to company interactions, customer loyalty is always on a check.

• There are many hackers who look for opportunities, and thus an ecommerce site, service, payment gateways, all are always prone to attack.

12.6.3 Applications of E-commerce

The term *e-commerce*, as we think of it today, refers to the buying and selling of goods or services over the Internet. For example, you may think of Amazon, which provides online shopping for various product categories, such as books, music, and electronics. This form of e-commerce is known as electronic retailing, or *e-tailing*, and usually involves the transportation of physical items. It is also referred to as *business-to-customer*, or B2C. Other well-known forms include:

• *Consumer-to-consumer (C2C) :* Transactions taking place between individuals, usually through a third-party site such as an online auction. A typical example of C2C commerce is ebay..

• *Business-to-business (B2B) :* Trade occurring between businesses, e.g., between a retailer and wholesaler, or between a wholesaler and manufacturer.

• *Business-to-government (B2G) :* Trade occurring between businesses and government agencies.

• *Business-to-customer (B2C) :* e-commerce applies the typical scenario of a small retail store seeking to create a website enabling customers to shop online. Software that accommodates a B2C scenario generally consists of two components:

(a) Store Front: The website that is accessed by customers, enabling them to purchase goods over the Internet. Data from the store catalog is typically maintained in a database, and pages requiring this data are generated dynamically.

(b) Administration Console: A password-protected area that is accessed over a secure connection by store staff for purposes of online management. This typically involves CRUD (create read update delete) access to the store catalog, management of discounts, shipping and payment options, and review of customer orders.

12.6.4 Features of E-commerce

1. Business Plan

Do not start without a business plan. Understand your product, your market, competition, obstacles, cost of effective delivery and a time frame for implementation.

- **Determine Your Objectives**

What do you wish to achieve with a web site? Is it to enhance awareness of your company brand/ s, sell goods online, provide customer support or develop and sell an electronic product. Your objectives will determine your approach to ecommerce

- **Understand your Market**

Local access is currently limited to less the 2% of the population in Pacific Island countries. This limits the effectiveness of the Internet for local usage. The overseas market is the immediate opportunity. It is important to understand the intricacies of your market. A category such as handicrafts / gifts can appeal to expatriate Pacific Islanders, collectors, bargain hunters or upper exotic art collectors. Identify your key markets and tailor your web strategy to reach them effectively

- **Product**

Your product could be services (tourism), electronic (software) or selling artifacts or gifts via a web store. Understanding the market determines how you package, present and price your product. Distance and isolation of the Pacific islands means ideal products should be portable and relatively inexpensive to deliver. Consider the value instant communications and global reach adds to your product. For some the Internet may not offer added value for your product.

VALUE to the customer is still bottom line, so avoid false expectations that the Internet is an opportunity to deliver at inflated prices or the illusion that there is a pot of gold on the end of your Internet connection.

2. Domain Name

Your domain name (www.yoursite.com) is your calling card on the web. Choose a domain name that is easy to remember. Generic domain names (*.com .net .org .edu .info .biz*) can be registered for US$35 / year at www.networksolutions.com or numerous other sites such as www.enom. If you find that your preferred domain has been taken, check other domain services such as .nu (Niue), .tv (Tuvalu), *.to* (Tonga) at tonic.to. Your web hosting service will register your domain name as part of their services if you decide to look for a hosting service at the same time.

3. Hosting Your Web site

Once you have decided on your domain name, you need to host your web pages on the Internet. There are thousands of Internet Service Providers (ISPs) that offer hosting. Host your service where your clientele or target audience will have the fastest access and you can guarantee the “up time” (reliability of service). It is usually practical to host your site on an overseas server.

Hosting costs vary with the amount of space (megabytes), traffic (how busy your site is measured in Gigabytes per month) and extra services (number of email addresses, ecommerce tools, site management tools, etc.). 30-250mb of space on a US based server (computer) will cost approximately $15 – 50 per month depending on your choice services. Ecommerce services such as shopping cart, secure transaction form and credit card processing will cost more. With a credit card one can usually register a host account within 15 minutes and have your domain name and host working within 3 days.

Beware: All ISPs claim to provide great support but few deliver satisfactory support services.

4. Design and Development

Design and content of your web site must be aimed at communicating with your customers. Speed of access, logical navigation and attractive look and feel are key objectives. Often fancy graphics will result in slow download times and result in impatient customers moving away. Your website is the only impression the customer has of your company or organization. Make sure they can see professionalism immediately. Your web site should be designed according to your customer expectations. While a travel / tourism site is expected to have lots of flashy pictures this may not be necessary for a academic web site or a web directory. A website with too much graphics will frustrate those looking for quick information by increasing download time of the web pages.

Outsourcing your web design may be the choice if you desire a professional look right from the start. For small companies, if you choose to out source your web design, insist on full access to the web site once it is launched and training on how to make basic changes. Eg. Announcements on the front page or changing product prices.

5. Managing Content

Many SMEs (Small businesses) rush to implement an online presence without considering the work involved with keeping content fresh and useful. Too often a website is literally "tacked on" as an additional task without considering the effort needed to update and maintain content. Unless a website is seen as essential for the future of your business it is probably not worth doing. An effective strategy includes the costs and process of integrating your web presence with your everyday business processes. This will ensure that information remains fresh and relevant and enables your organization to adapt to meet the demands of your online customer.

As the site gets busier, interaction with customers and order processing can take some serious staffing time. For some this is a good problem to have but be realistic and budget for employee time at all levels of your web site development.

6. Electronic Transactions

The key objective of selling is to deliver a product and receive payment. The challenge for many small companies is being able to make online transactions for credit cards. Usually this can be done by capturing necessary credit card details via a secure web then manually inputting to your local merchant account in daily batches. The process can be automated with credit cards verified online and payment immediately credited to your account.

For small businesses without merchant accounts there are online sites that provide merchant account services as well as credit card processing for a monthly fee and individual transaction charge. New services have developed that now enable transactions via email. By opening an account with these services you are able to arrange for them to receive funds on your behalf and then they pay it directly into your own account.

- **Delivery**

Distance is the key obstacle with selling online from the Pacific Islands. Delivery of electronic products (software) can be transferred instantly and certain services can be provided to distant customers. However with physical goods there are several issues to be considered. Expectations of many consumers have been formed around the overnight delivery services available in developed country markets. Customers must be made aware that delivery of your product will take 1- 3 weeks. Costs are also higher then normal and will affect your final price. Guarantees of quality and delivery times are important to overcome initial misgivings of service from new customers. Delivery of a Tourism "product" is more difficult. Ensure your product is as good as your online marketing spin. With careful marketing you can attract the right kind of visitor to a eco tourism resort without running water or electricity who will enjoy and appreciate the facilities. Just make sure they expect it or you will have a crisis situation.

7. Marketing your website– Online and Off-line

The key to a successful ecommerce website is effectively reaching your target market with services that they perceive offer value. Getting online users to visit your website will depend on your ability to raise awareness amongst potential customers. This can be done with a good online AND off-line strategy.

Online:

- List your link with key sites relevant to your target market. Online linkages from other web sites are the most effective means of bringing people to your site. A regional travel site will want to be linked from all key Pacific Island sites. .
- Pay for advertising on sections of popular websites visited by your target clientele.
- Place your site on search engines and portal sites such as Yahoo.com, Google.com, altavista.com and others – NOTE: Remember that search engines have people who are constantly developing methods to prevent others like you from "cheating" by biasing there ranking criteria to place your site. Criteria constantly changes. The best bet is to ensure you have a good set of key words in your meta data and you are linked and recognized by as many other sites as possible. Recognition will come the better your site is.

Off-line:

- Include your URL (web address) on ALL stationary of the firm
- Utilize conventional media through targeted press releases
- Place print advertisements in appropriate media.
- Utilize trade shows, travel agents and other means to publicize your URL overseas

12.7 Summary

- Teleconferncing is essentiall a means for communication and training.
- Videoconferencing is the conduct of a video conferencing is the conduct of a video conference that is a set of telecommunication technologies.
- Internet banking or e-banking means any user with a personal computer and a browser can get connected to his bank website to perform any of the virtual banking function.
- Electronic business, commonly referred toa "e-Business" or an internet business, may be defined as the application of information and communication technologies in support of all the activities ofbusiness.
- E-commerece is the buying and selling of products and services by businesses and consumers over the internet.

12.7 Self-Assessment Questions

1. What is network programming ? Define the applications of network programming.
2. What is Teleconferencing? Where it is used?
3. What is the difference between Teleconferencing and Videoconferencing ?
4. What is Electronic banking? Also define the advantages and disadvantages of E-banking.
5. What is the function of E-business? Why security is required in E-business.
6. What is the use of E-business ? what are the limitations of E-business.
7. What is E-commerce?
8. List several examples of electronic funds transfers and discuss your experiences with EFT(electronic funds transfer).
9. Describe smart cards and give examples of what they can do.
10. Describe check cards and give examples of what they can do.
11. What consumer protections apply to lost or stolen EFT cards under the federal Electronic Funds Transfer Act?
12. What information must be included in periodic EFT statements from your financial institution, and why is it important for consumers to check this information for accuracy as soon as possible after receipt?

12.8 References

1. http://www.dynamicwebs.com.au/tutorials/e-commerce.htm
2. http://www.worldjute.com/ebank.html
3. Bajaj and Nag, “E-commerce”

Unit-13

Introduction to Internet

Structure of the Unit

13.0 Objective

This chapter provides a general overview of

- Definition of Internet
- Difference between Internet and Intranet
- Internet services
- Uses of Email, WWW and net surfing

13.1 Introduction

The purpose of this unit is to serve an overview and necessary background to the detailed material that follows. It shows what is the concept of Internet.

Internet protocols : An Internet of multiple separate networks that are interconnected by routers. The TCP/IP and related protocols that are used across the Internet are designed and agreed upon by the users and administrators of the individual parts of the Internet. Next we look at the Internet services as WWW, Email and net surfing. An IP *(Internet Protocol)* address is a unique identifier for a node or host connection on an IP network.

13.2 Definition of Internet

An Internet consists of multiple separate networks that are interconnected by routers. Data are transmitted in packets from a source system to a destination across a path involving multiple networks and routers. Typically a connectionless or datagram operation is used. A router accepts datagrams and relays them on toward their destination and is responsible for determining the route, much the same way as packet-switching nodes operate.

The following terms are related to the interconnection of networks or internetworking:

Communication Network : A facility that provides a data transfer service among devices attached to the network.

Internet : A collection of communication networks interconnected by bridges and/or routers.

Intranet : A corporate internet that provides the key Internet applications, especially the World Wide Web. An intranet operates within the organization for internal purposes and can exists as an isolated, self contained internet or may have links to the Internet.

End System(ES) : A device attached to one of the networks of an internet that is used to support end-user applications or services.

Intermediate System(IS) : A device used to connect two networks and permit communication between end systems attached to different networks.

Bridge : An IS used to connect two LANs that use similar LAN protocols. The bridge acts as an address filter, picking up packets from one LAN that are intended for a destination on another LAN and passing those packets on. The bridge does not modify the contents of the packets and does not add anything to the packet. The bridge operates at layer 2 of the OSI model.

Router : An IS used to connect two networks that may or may not be similar. The router employs an internet protocol present in each router and each end system of the network. The router operates at layer 3 of the OSI model.

13.3 Internet Vs Intranet

There is one major distinction between an intranet and the Internet: The Internet is an open, public space, while an intranet is designed to be a private space. An intranet may be accessible from the Internet, but as a rule it's protected by a password and accessible only to employees or other authorized users. From within a company, an intranet server may respond much more quickly than a typical Web site. This is because the public Internet is at the mercy of traffic spikes, server breakdowns and other problems that may slow the network. Within a company, however, users have much more bandwidth and network hardware may be more reliable. This makes it easier to serve high bandwidth content, such as audio and video, over an intranet.

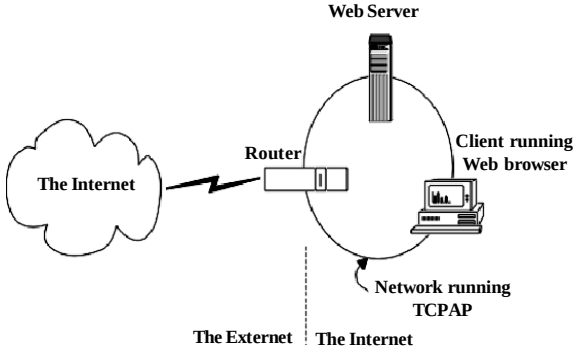


Figure13.1 : Difference between internet and intranet

Intranet is a network within and only for an organization *(for instance a big business corporation)* whereas Internet is a worldwide network and is public domain; Intranet has access to Internet but not vice-versa; and the design for Intranet is more task-orientated and less promotional.

Intranet, with sole purpose of internal communication, and a public website on the open Internet with purpose of public information are two different information spaces and also have two different interface designs. The two types of sites also differ along several dimensions:

Users differ: Intranet users are own employees of an organization who know a lot about that organization, its organizational structure and special terminology and circumstances. An Internet site is used by customers who would know much less about the same organization and also care less about it.

The tasks differ: The Intranet is used for everyday work inside the organization, including some quite complex applications. The Internet site is mainly used to find out about the organization's services or products on offer.

The type of information differs: The Intranet will have many draft reports, project progress reports, human resource information, and other detailed information, whereas the Internet site will have marketing information and customer support information.

The amount of information differs: Typically an Intranet has between ten and hundred times as many pages as the same organization's public website. The difference is due to the extensive amount of work-in-progress that is documented on the Intranet and the fact that many organizations never publish anything publicly even though they may have many internal documents.

Bandwidth and cross platform needs differ: Intranets often run between a hundred and a thousand times faster than most Internet users' Web access which is stuck at low-band or mid-band, so it is feasible to use rich graphics and even multimedia and other advanced content on Intranet pages.

It is quite clear that the Intranet has become an integral part of managing big businesses and organizations. It is an easy and quick method of communication internally. Just like the Internet, the Intranet has become part of our daily lives.

The Internet is a special example of a WAN. The Internet is a network of networks that spans the globe. It is a cooperative system in which organizations voluntarily attach their networks to the Internet in order that their users can get the benefits of extensive communications. Although many different kinds of computers and networks are attached to the Internet, the following characteristics are always true.

- The TCP/IP protocol suite is used. Network addresses are unique.
- The system uses a client/server computing architecture. This includes servers (Web, FTP, etc.) which provide the data or files, and clients (browsers, FTP, Telnet, etc.) which can make use of them.

An intranet is an organization network which uses exactly the same technology as the Internet (TCP/IP, servers, browsers, etc.). The intranet coexists with the LAN system (Novell, Windows 2003, etc.) and even uses the same physical infrastructure (Ethernet, Token Ring, etc.).

13.4 Internet Services

The Internet facilitates various services, ranging from the transfer of files from one place to another, e-mail, the World Wide Web, chat rooms, notice boards, as well as a whole range of online services from shopping to entertainment. In addition, thousands of governments, educational and commercial institutions as well as millions of individuals have information that is stored on computer systems and can be accessed over traditional telephone lines, fibre optic cables, and satellite communications.

13.4.1 E-mail

For many Internet users, electronic mail (e-mail) has practically replaced the Postal Service for short written transactions. Electronic mail is the most widely used application on the Net. You can also carry on live "conversations" with other computer users, using Internet Relay Chat (IRC). More recently, Internet telephony hardware and software allows real-time voice conversations.

In terms of the history of communication, email is a relatively new medium; to some extent, we are still discovering how best to use it in our day-to-day lives. Email has several features that distinguish it from other forms of communication, and which often create problems for new users.

Firstly, email is designed to be *asynchronous*, and as such is like "snailmail" *(ordinary paperbased post)* or voicemail; there's not meant to be an immediate reply or conversation involved, and the mail sits in the inbox until collected by the recipient. However, it's also often fast enough to be used synchronously, so that two correspondents can, if online at the same time, hold something like a conversation using email.

Secondly, and perhaps because of this first point, it is emerging in language terms as a hybrid of speech and writing. Emails tend to be more casual than letters or memos, but more formal than a phone or face-to-face conversation. This often causes problems for new users who have difficulty in finding the correct "register" for their emails, and often use too formal or too casual language in inappropriate situations.

Email is the means by which we can electronically get our messages across to one another as against the conventional mode of paper-based messaging. Messages can be prepared and sent reliably over communication networks from the desktop computer of the sender to be received at the desktop computer of the recipient. In addition to saving in time caused by not having to handle paper, the advantage of being able to send and receive mail as and when convenient is retained. Not only has Email emerged as a reliable and convenient method of inter-personal messaging, it has also been deployed in changing work processes within organization.

The main components of electronic mail systems are:

a) User agent(UA): which allows the user to prepare electronic mail.

b) Message Transfer Agent(MTA) : which is responsible for routing electronic messages to their destination.

c) Message Store(MS): where electronic mail can be stored until it is picked up by the recipient.

d) User Agent(UA): the first component of an electronic mail system is the user agent(UA). It provides service to the user to make the process of sending and receiving a message easier. Services provided by a user agent are:

Composing messages a user agent helps the user compose the e-mail message to be sent out. A user can alternatively use his or her favorite text editor or word processor to create the message and import it into the user agent template.

Reading message the second duty of the user agent is to read the incoming messages. When a user invokes a user agent, it first checks the mail in the incoming mailbox. Most user agent show a one-line summary of each received mail.

Replying to message after reading a message, a user can use the user agent to reply to a message.

Forwarding messages replying is defined as sending a message to the sender or recipients of the copy. Forwarding is defined as sending the message to a third party.

Handling mailboxes a user agent normally creates two mailboxes: *an inbox and an outbox*. Each box is a file with a special format that can be handled by the user agent. The inbox keeps all the received e-mails until they are deleted by the user. The outbox keeps all the sent e-mails until the user deletes them.

e) Message Transfer Agent(MTA) : MTA's are interconnected to each other to collectively form a message transfer system. To send electronic mail, the sender does not have to ensure that the recipient's computer system is on. It can be sent and received at the convenience of the user.

The actual mail transfer is done through message transfer agents. To send mail, a system must have the client MTA, ad to receive mail, a system must have a server MTA. The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol. MTA is used two times, between the sender and the sender's mail server and between the two mail servers.

It simply defines how commands and responses must be sent back and forth. Each network is free to choose a software package for implementation.

Commands and responses MTA uses commands and responses to transfer messages between an MTA client ad MTA server. Commands are sent from the client to the server. The format of a command consists of a keyword followed by zero or more arguments. Responses are sent from the server to the client. A response is three digit code that may be followed by additional textual information.

The process of transferring a mail message occurs in three phases: connection establishment, mail transfer and connection termination.

f) Message Store(MS): the concept of a MS was added in 1988. this is done to alleviate the problem faced by an MTA in delivering a message if the UA was not on-line. With the introduction of the MS, UA's submit and receive message to/from the MS. The MTA also picks up messages from ad delivers to the MS. The UA can then access the MS at any convenient time, and at the same time not hold up the MTA's delivery process.

Email provides a fast, efficient delivery system for text-based messages. As with all applications on the Internet, it uses certain protocols to achieve this "How email works":

• *SMTP* (Simple Mail Transfer Protocol) is used to distribute mail between servers, and by the mail client to send the message initially;

• *POP* (Post Office Protocol) is used by the mail client to download messages and headers to a local computer from the mail server. POP is useful if you want to read your mail offline (ie not connected to your mailserver), as it downloads and stores your email on your own computer.

• *IMAP* (Internet Message Access Protocol) is used by clients to access mail directly on the mail server. With IMAP, the mail usually stays stored on the recipient's server until it is deleted - the mail client only views the mail, rather than downloading it.

13.4.2 WWW(World Wide Web)

The World Wide Web(WWW) is a repository of information linked together from points all over the world. The WWW has a unique combination of flexibility, portability and user-friendly features that distinguish it from other services provided by the Internet.

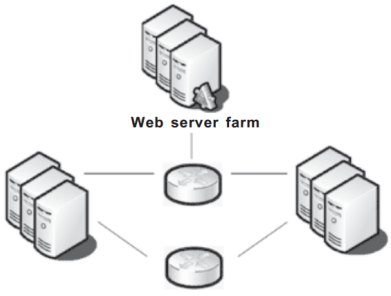


Figure 13.2 : Example of a Web server

The WWW today is a distributed client/server service, in which a client using a browser can access a service using a server. However the service provided is distributed over many locations called *sites*. Each site holds one or more documents, referred to as Web pages. Each Web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved and viewed by using browser. The client sends a request through its browser, a program that is designed to fetch web documents. The request among other information includes the address of the site and the Web page, called the URL*(Uniform Resource Locator)*.

The Web consists of many millions of internet-connected computers, each with information on them that their owner has decided to share. These documents can be formed of anything from plain text to multimedia or even 3D objects. These computers, called servers, deliver this information over the Internet to client computers (such as your PC at home) using a protocol called HTTP (*HyperText Transfer Protocol*). The HTTP protocol is very simple; essentially it just provides a mechanism that allows a client to request a document, and a server to send that document.

Client : Each browser usually consists of three parts-a controller, client protocol and interpreters. The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the documents on the screen. The client protocol can be one of the protocols as FTP or HTTP. The interpreter can be HTML, Java, Javascript, depending on the type of the document.

Server : The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client. To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than disk.

As the web has become more and more popular, its capabilities have increased to include such things as graphics, animations, scripts and even complete computer programs, all embedded into the pages of the documents. Essentially, the web is the easiest to use of all the internet toolkit —this is partly why it has become so popular. Various mechanisms allow the viewer to move around (navigate) the document easily. Clicking on a hyperlink moves you to another part of the document, or to another document altogether.

Web Documents The documents in the WWW can be grouped into three categories: Static dynamic and active. The category is based on the time at which the contents of the documents are determined.

a) Static Documents : these documents are fixed-content documents that are created and stored in a server. The client can get only a copy of the document. In other words the contents of the file are determined when the file is created, not when it is used. When the client accesses the document, a copy of the document is sent. The user can then use a browsing program to display the document.

Hypertext Markup Language(HTML): is the language of the web, was specifically designed to be easy to learn, and was based around the concept of marking text functionally, to ensure a wide authorship. Thus, when the author wrote their document, they would be able to concentrate on its structure, and not worry about its presentation. As it has grown, the web has moved away from this concept, becoming more complex and more graphical than originally envisioned, which has led to many presentational features creeping into the HTML standard. Happily though, the core functions still lie beneath all the complexity, and allow more or less anyone to write their own web pages quickly and easily, with a minimal set of software tools.

One of the most powerful features of the web is the ability to link documents together using *hyperlinks*. On clicking a hyperlink *(usually underlined)*, the browser tries to access the linked document, providing an almost instantaneous cross-referencing system. This creates a non-linear form of text, known as *hypertext*. Web pages can also contain multimedia content that can also be hyperlinked, termed *hypermedia*. Many theorists believe that hyperlinks change the way we view and read texts, and certainly

the element of choice that hyperlinks give the reader create a very different reading experience. The idea of hypertext has been around at least as long as books have contained footnotes or external references/ bibliographies, but the computer and the Internet make following hyperlinks instantaneous .

b) Dynamic Documents: these documents are created by a web server whenever a browser request the document. When a request arrives, the web server runs an application program or a script that creates the dynamic document. The server returns the output of the program or script as a response to the browser that requested the document. A very simple example of a dynamic document is the retrieval of the time and date from a server.

Common Gateway Interface(CGI): is a technology that creates and handles dynamic documents. CGI is a set of standards that defines how a dynamic document is written, how data are input to the program, and how the output result is used. A few technologies have been involved in creating dynamic documents using scripts. Among the most are Hypertext Preprocessor(PHP), Java Server Pages(JSP) and Active Server Pages(ASP).

c) Active Document: For many applications, we need a program or a script to e run at the client site. These are called active documents. For example, suppose we want to run a program that creates animated graphics on the screen or a program that interacts with the user. The program definitely needs to be run at the client site where the animation or interaction takes place. When the browser request an active document, the server sends a copy of the document or a script. The document is then run at the client(browser)site.

Java Applets: one way to create a active document is to use java applets. Java is a combination of a high level programming language, a run time environment, and a class library that allows a programmer to write a active document(an applet) and a browser to run it. An applet is a program written in java on the server. It is compiled and ready to be run. The document is in byte-code format.

Hypertext Transfer Protocol(HTTP)

The backbone of the web is the network of *webservers* across the world. These are really just computers that have a particular type of software running on them - software that knows how to speak the HTTP protocol and knows which information stored on the computer should be made accessible through the web. It's possible to turn almost any computer into a webserver by downloading and installing server software.

The *HyperText Transfer Protocol* (HTTP) is actually quite simple. The web browser (or client) makes a request of a webpage to the server, and the webserver passes the page back to the browser "How HTTP works: retrieving a web page". More cleverly, it also passes back any images, sounds or other media items back to the browser too. The web browser is also particularly clever in the way it displays what it retrieves. Web pages are written in HTML, and the browser knows how to display these correctly, whether you have a huge flat screen or a tiny screen on a handheld device or phone. The HTML language gives the browser hints on how to display things, and the browser decides the final layout itself.

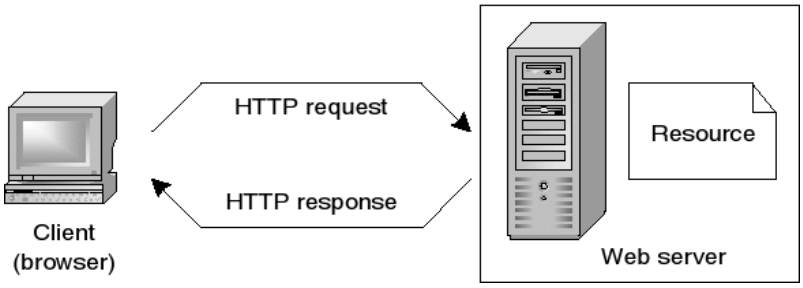


Figure 13.3 : How HTTP works: retrieving a web page

13.4.3 Net surfing

To access Internet you only need a computer: a normal PC with a CDROM player will be sufficient, but it has to be equipped with a device to connect the telephone line: the modem. Once you are connected to Internet, the Home Page, a default web page chosen by the user, opens. To surf within any Internet website, you need to "explore" its contents with the mouse pointer, which normally looks like an arrow. When the arrow is positioned on a word, a symbol, or an image which allows access to new pages in the same website (link) the pointer turns into a "hand".

At this point, in order to access the new page you need to double-click the left mouse button on the link. Website pages don't have a fixed vertical or horizontal size. The more the web designer has written, the more the page stretches out or broadens, depending on the case. If the screen in which you are surfing is not large enough, the page will be partly displayed. To see the other part of the page you are visiting you need to move up or down, right and left on the web page by using the arrow shaped cursors you can see at the right bottom end of the browser window (in the scroll bar).

It will be possible to move to other websites or pages from the first page as follows:

• move the arrow with the mouse to the box on the top of the browser's window (next to the writing "Address")

• click once on the writing you can see in the box, which is the address of the web page in which you are at the moment; the writing will become blue and it will be possible to "write over it" thus deleting and overwriting it with another address

• type the address of the website you would like to visit

• push the button "Enter" to upload the page requested

All Internet addresses are structured as follows:

www.uok.ac.in

www.name.TLDextension

where the "name" is the name of the website, and "extension" is the two or threeletter code that indicates the type of website (i.e. .org, .com where org means "organization" and com "company") or the organization's or company's country (i.e. .it for Italian websites, .uk for British websites…).

The words composing a website address must always be typed without any spaces between one and the other, while full stop (dot), dash and underscore (-, _) and "slash"(/) have to be typed as they appear in the addresses.

Let's see what the basic functions for the navigation on the "tools bar" are(which you can find in the top part of the browser's window):

Things to Be Cautious About on the Internet

Accuracy: Be cautious not to believe everything on the Internet. Almost anyone can publish information on the Internet, and some of it may be false. Check all information for accuracy through additional reputable sources.

Security: When sending information over the Internet, be prepared to let the world have access to it. There are ways to gain access to anything that you send to anyone over the Internet, including e-mail. Be extremely cautious when sending confidential information to anyone.

Copyright: Always give credit to the author of any information (including graphics) found on the Internet. Often permission can be granted from an author to use their material for educational purposes.

Viruses/Worms: These usually destructive computer programs hide inside of innocent looking programs, web pages and e-mail attachments. When triggered, often by the date or time on the computer's internal clock or calendar, it executes a nuisance or damaging function such as displaying a message on your screen, corrupting your files, or reformatting your hard disk. Today, worms access your e-mail address book and send themselves automatically. Make sure you've got virus protection software installed and that you update their "virus definition" files at least monthly

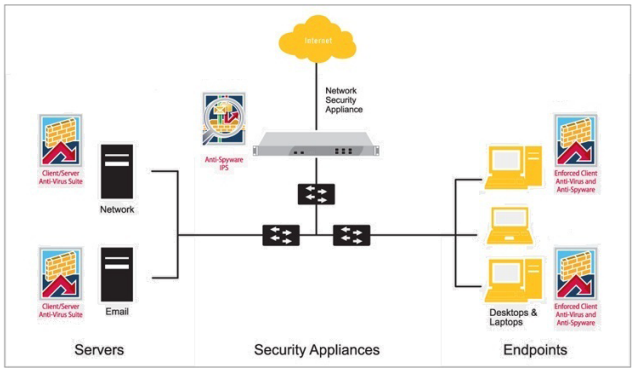


Figure 13.4 : Internet Scenario

Let's see what the basic functions for the navigation on the "tools bar" are(which you can find in the top part of the browser's window):

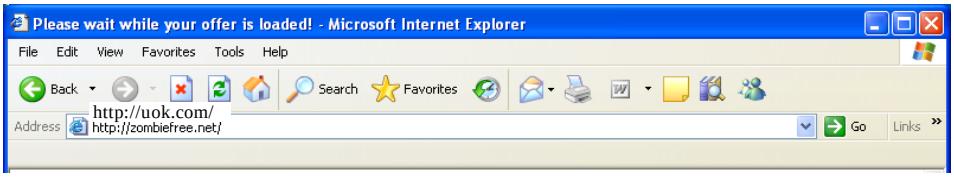


Figure 13.5 : Tools bar

• ***Forward and Back:*** These two buttons allow you to go backwards or forwards in the "navigation" path you already did *(it opens web pages already opened before)*

• ***Stop:*** it stops *"downloading"* a page (it is useful when there are problems opening a page, for example when it takes too long to open a page);

• ***Refresh:*** it allows to download *("refresh")* the page you are visiting again (it is useful when there are problems with downloading or displaying a web page's contents, or when you need the latest data);

• ***Home :*** allows you to return to the first page appearing in Internet navigation**;**

• ***Search:*** a bar on the left hand of the screen in which there is a simplified search engine, opens.

• ***Favorites:*** it allows you to save and archives the web page addresses which interest you the most and pages you may want to return to in the future;

• ***Multimedia:*** it opens a programme which you use to listen to music or watch videos; it is available only in the latest versions of Internet Explorer;

• ***History:*** it is a list of the websites visited in the last three weeks; it allows you to find a website that you don't remember but that you visited only a short while ago;

• ***Mail:*** it allows you to open directly the e-mail client or to send a friend the webpage you are visiting (or its address) via an e-mail;

• ***Print:*** it is used to print the page you are visiting.

To save a website address you need to:

• Be in the home page of the website you want to save;

• Click on the button *"Favorites";* a column on the left hand of the screen appears;

• Click on *"add"* which can be found at the top of the column;

• In the previous window the programme asks you what you want to name this address;

• If this is the case, modify the name, automatically suggested by Internet, with another one that can easily be associated to the website;

• Click on *"ok"*.

To use the "Favorites" bookmark you need to:

• click on *"Favorites"* (if the column on the left is not already open and displayed);

• click on the name of the website you wish to visit: the page will be automatically searched and downloaded.

13.5 Searching on Internet

To connect to the Internet, you will need the following things:

• A personal computer with a Web browser *(Internet Explorer).* Internet Explorer is one of the common Web browsers available. Many Web browsers can be downloaded from the Internet for free (Freeware Software).

• Access to a *host computer (server computer)* – that is a computer connected to the Internet. The host computer might be maintained by your company or by a commercial Internet Service Provider (ISP). For example, *iway Namibia.*

• A connection device such as a modem or network cable.

13.5.1 Basic Components of Internet

Each computer on the Internet must have a unique number for identification. This number, known as an IP *address,* is used for communication and connection purposes. The other components are:

• Internet host computer :

You access the Internet by using an Internet service provider to connect to an Internet host computer. A service provider supplies you with an Internet account that includes a user name and password that you use to access the host computer. There are three major types of Internet access:

• Corporate Network: If your company network is connected to the Internet, you can use the existing network cable to gain access. As a network user, you first log on to your corporate network and then you can connect to the Internet. If you are connecting from a remote location, you first need a phone line and a modem to dial into your corporate network.

• Community Network or Free Net: As part of the National Public Telecomputing Network (NPTN) organization, local communities provide Internet access at public facilities such as libraries or community centers. In this situation, you might be given a user account to log on at a walk-up terminal.

• Commercial Internet Service Provider (ISP): you can purchase Internet connection time, an Internet account, and email service from an ISP, such as *iway Namibia* or *AST Namibia.* The cost might include a one-time registration fee, a monthly fee, or charges based on how long you are connected.

Internet Service Provider: An ISP, or Internet Service Provider, is a company that provides you with a point of access to the Internet. When you connect to your ISP, your computer (or your own network) becomes an extension of the Internet itself whilst you remain connected. To connect from home you need several things. Apart from a computer you'll need a phone connection, a modem or ADSL router, and some Internet software. Things will be easier if you're using a relatively recent operation system, such as Windows Vista/XP or MacOSX, but it's possible to connect with older or more obscure systems. With a modem and the appropriate software, you can dial up another modem connected to another computer, and establish a network connection with it. Usually, this computer is linked into the Internet, and so you're online. With an ADSL modem or router, a similar procedure happens, but a filter splits the telephone line into voice and data (low and high frequencies) and your router negotiates a connection with the ADSL equipment in the telephone exchange.

Frequencies used on an ADSL line: PSTN is the normal telephone ("voice") usage, and the upstream/ downstream areas are for data. Note the unequal proportions of the data range (i.e. **Assymetric** DSL)

For broadband ISPs, there are several important factors to check, including reliability, speed of connection, how many other customers share the total bandwidth (the Contention Ratio), and of course, cost. Most charge a set-up cost, and many have a minimum contract period, so be careful you don't get locked into a poor deal for many months! There are now also variable packages, where you can control the amount of bandwidth available, paying extra for more capacity if you need it. For more recommendations and relatively independent advice I find ThinkBroadband [http://www.thinkbroadband.com/] (formerly ADSLGuide.org.uk) useful.

A recent development is the capping of Internet connections by limiting the monthly downloads to, say, 10GB. This may seem reasonable at first, but if you wish to listen to Internet radio or download video clips from the BBC, for example, then you'll hit this limit sooner than you expect. Check whether your ISP offers an "unlimited" or "unmetered" service.

Switched Network : As a *switched network*, the physical connections between computers do not matter as far as Internet traffic is concerned to the protocols ensure that guaranteed information delivery is more important than speed or use of a particular route. This means that a sequence of packets might arrive out of order, with some travelling through the net by a faster, shorter route than others. TCP/IP provides the means for your software to piece together those packets into meaningful data. The ability to take different routes through the network is a fundamental part of the original design of TCP/IP, as it allows the Internet to route around damaged areas of the network.

The Internet is based on *packet-switched* protocols. Information is carried in *packets*, which can be imagined as small parcels being passed from computer to computer. Large chunks of data are usually broken up into several smaller packets before being sent through the network. The delivery mechanism, or protocol, that is used to encode the packet ensures safe transit, and provides a way of reconstructing the data when it reaches its destination. The protocols used on the Internet are referred to as TCP/IP, standing for *Transmission Control Protocol* / *Internet Protocol*.

13.5.2 Search Engine

General purpose of search engines like Google, Yahoo!, and Bing provide broad-coverage of the Web, you will likely achieve superior results using a *specialty search engine*, when you are looking for information about a specific topic or region.

a) Choose the Right Search Tool or Technique

If you looking for Web pages containing specific words or phrases, search engines, such as Google, provide a fast and efficient means of locating those pages. For a broader view of the information on the Internet, or when you are unfamiliar with a topic, you can use subject directories, such as the World

Wide Web Virtual Library, to acquaint yourself with the field and select the most appropriate information resources. Sometimes your best approach is to intuitively guess at the name of the site that might hold the information you seek. Unfortunately, search engines, subject directories, and informed guesses cannot find the vast majority of Web pages on the Internet because they are stored in databases, inaccessible by conventional search tools and techniques. Instead, you must use specialty search resources to locate this hidden content.

b) Use Boolean Operators

The biggest mistake a search engine user makes is to enter a single nondescript keyword. If you type "car" into Google and click the Google Search button, you will receive over 900 million search results! To narrow your search, start by adding more keywords. Adding the keywords *battery dead* after *car* will return less than a million search hits. To hone your search further, you will need to construct a complex query. A complex query uses Boolean operators to define the relationships among your keywords.

Common Boolean operators include AND, OR, and NOT. The AND operator restricts your search results by telling the search engine to return only Web pages that contain all the specified keywords (e.g., car AND battery AND dead). It is unnecessary to use this Boolean operator in Google because, by default, it assumes any keywords or phrases you enter are connected by the AND operator. The OR operator let's you expand your search by locating all the pages that contain a least one of the specified keywords (e.g., car OR automobile OR vehicle). The NOT operator, symbolized by the (-) minus sign in Google, causes the search engine to exclude pages that contain certain keywords (e.g., -buy). You can combine these operators to create a complex query that will locate the exact information you desire.

c) Use advanced Search operators

The major search engines, such as Google, offer *advanced search operators* that let you really zero in what you are looking for on the Internet. For example, in Google you can use the *site:* operator to search a particular Web site for information. Type *health care crisis site:www.newsweek.com* into Google and it will return a list of articles in Newsweek.com that mention the health care crisis.

d) Use Metasearch Engines

Since each search engine covers different portions of the Internet at different times, to perform a thorough search of the Internet, you should query as many search engines as possible. However, going to each search engine and repeatedly entering the same search query is both time consuming and tedious. *Metasearch engines* let you enter your query just once and then query multiple search engines simultaneously, returning a compilation of search results from all the search engines queried.

The best metasearch engines eliminate duplicate results and even rank the results based on relevancy to your query. The potential time saved by using a metasearch engine is offset by the limitation that often the most popular search engines are not queried by a metasearch engine because of legal and fee issues. Thus, the most thorough search strategy is to employ metasearch engines in combination with the individual search engines (i.e., Google and Bing).

13.6 Introduction to IP addressing and Subnetting

An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network. As with any other network-layer protocol, the ***IP addressing*** scheme is integral to the process of routing IP datagrams through an internetwork.

13.6.1 IP addressing

Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for subnetworks. Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts: the network number and the host number. The network number identifies a network and must be assigned by the Internet Network Information

Center (InterNIC) if the network is to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the InterNIC and can itself assign address space as necessary. The host number identifies a host on a network and is assigned by the local network administrator.

Host identifiers are classified as names, addresses, or routes, where:

A name suggests what object we want

An address specifies where the object is

A route tells us how to get to the object

In the Internet, names consist of human-readable strings such as eve, Percival, or cs.wpi.edu. Addresses consist of compact, 32-bit identifiers. Internet software translates names into addresses; lower protocol layers always uses addresses rather than names. Internet addresses are hierarchical, consisting of two parts:

Network: The network part of an address identifies which network a host is on. Conceptually, each LAN has its own unique IP network number.

Local: The local part of an address identifies which host on that network. Later, we'll examine a technique called subnetting that adds a third level to the hierarchy. With subnetting, the local part may consist of a \site", which is further broken down in to local network number, local host.

Conceptually, the Internet consists of a collection of physical networks, each of which is assigned a unique number.

As datagrams travel from one gateway to another, each gateway routes the datagram based on the network number in the datagram's destination address. Only the gateway on the same network as the destination uses the local part of the address in forwarding a datagram. That is, when the datagram reaches a gateway that connects to the destination address, the gateway uses the local part of the address to forward the datagram to the appropriate host.

Anatomy of an IP address

- The IP address is a 32-bit address that consists of two components.
- One component is the network portion of the address, consisting of the network bits.
  - The network bits make up the left portion of the address.
  - They consist of the first bit up to some boundary, to be discussed later.
- The second component is the host portion of the address, consisting of the host bits.
  - The host bits make up the right portion of the address.
  - They consist of the remaining bits not included with the network bits.

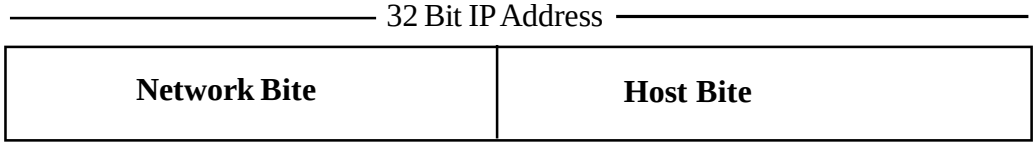


Figure 13.5 : IP Address

An IP address is a 32 bit binary number usually represented as 4 decimal values, each representing 8 bits, in the range 0 to 255 (known as octets) separated by decimal points. This is known as "dotted decimal" notation.

Example: 140.179.220.200

It is sometimes useful to view the values in their binary form.

140 .179 .220 .200

10001100.10110011.11011100.11001000

Every IP address consists of two parts, one identifying the network and one identifying the node. The Class of the address and the subnet mask determine which part belongs to the network address and which part belongs to the node address.

13.6.2 DNS in the Internet

DNS is a protocol that can be used in different platforms. In the Internet, the domain name space(tree) is divided into three different sections:

a) Host names

The IP numbers are registered with *Internet Network Information Center* (InterNIC) and given host names that are easier for people to remember. Instead of having to remember a string of numbers, you need to recall only the assigned host name. Host names are usually company names, such as Microsoft, or easy to remember abbreviations. The *Domain Name Service* (DNS) is the method of matching host names with their unique IP addresses and vice versa. At least one computer on each network is designated as the DNS server.

b) Domain names

Computer networks are divided into organizational units called *domains.* The domain name might be the same as the host name. In large networks, however, the domain name might be different. Domain can be divided into sub-domains for organizational purposes. The fully qualified domain name combines the host and domain names as shown in the example below: hostname.subdomain.domain The following table lists some of the examples of domains:

DOMAIN	DESCRIPTION
.com	Commercal business
.edu	Educational institutions
.gov	Governmental institutions
.mil	Military Institutions
.net	Networks
.org	Organizations (usually non-profit)

Figure 13.6 : Example of domains

c) Uniform Resource Locators (URL)

To locate a particular page or document on the internet, you need an internet address called a *Uniform Resource Locator*, or URL. A URL consists of three major components that provide the necessary information to find a specific document. These components are separated by a forward slash (/). For example, the URL for the page that contains downloadable files for Microsoft Internet Explorer might be as follows: http://www.microsoft.com/ie/downloads

- (http://) - is the protocol used.
- *(www.microsoft.com/)*- is the server's host name and domain.

• (ie/*downloads)*- is the directory path where the page is stored.

13.6.3 IP Address Classes

IP addressing supports five different address classes: A, B,C, D, and E. Only classes A, B, and C are available for commercial use. The left-most (high-order) bits indicate the network class. You can determine which class any IP address is in by examining the first 4 bits of the IP address.

The class of address can be determined easily by examining the first octet of the address and mapping that value to a class range in the following tables. In an IP address of 172.31.1.2, for example, the first octet is 172. Because 172 falls between 128 and 191, 172.31.1.2 is a Class B address.

Address Class	**First Octet in Decimal**	**High-Order Bits**
Class-A	1 D 126	0
Cass-B	126 D 191	10
Class-C	192 D 223	110
Class-D	224 D 239	1110
Class-E	240 D 254	1111

Figure 13.7 : A range of possible values exists for the first octat of each adress class.

Class A addresses begin with **0xxx**, or **1 to 126** decimal.

• Class A networks

First octet values range from **1 through 126**.

First octet starts with bit **0**.

Network mask is **8 bits**, written **/8** or **255.0.0.0**.

1.0.0.0 through 126.0.0.0 are class A networks with **16777214** hosts each.

Class B addresses begin with **10xx**, or **128 to 191** decimal.

•Class B networks

First octet values range from **128 through 191**.

First octet starts with binary pattern **10**.

Network mask is **16 bits**, written **/16** or **255.255.0.0**.

128.0.0.0 through 191.255.0.0 are class B networks, with **65534** hosts each.

Class C addresses begin with **110x**, or **192 to 223** decimal.

• Class C networks

First octet values range from **192 through 223**.

First octet starts with binary pattern **110**.

Network mask is **24 bits**, written **/24** or **255.255.255.0**.

192.0.0.0 through 223.255.255.0 are class C networks, with **254** hosts each.

Class D addresses begin with **1110**, or **224 to 239** decimal.

- **Class D addresses**

  First octet values range from **224 through 239**.

  First octet starts with binary pattern **1110**.

  Class D addresses are multicast addresses, which will not be discussed in this tutorial.

Class E addresses begin with **1111**, or **240 to 254** decimal.

- **Class E addresses**

  Essentially everything that's left.

  Experimental class.

- **Reserved addresses**

  0.0.0.0 is the default IP address, and it is used to specify a default route.

  Addresses beginning with 127 are reserved for internal loopback addresses. It is common to see 127.0.0.1 used as the internal loopback address on many devices. Try pinging this address on a PC or Unix station.

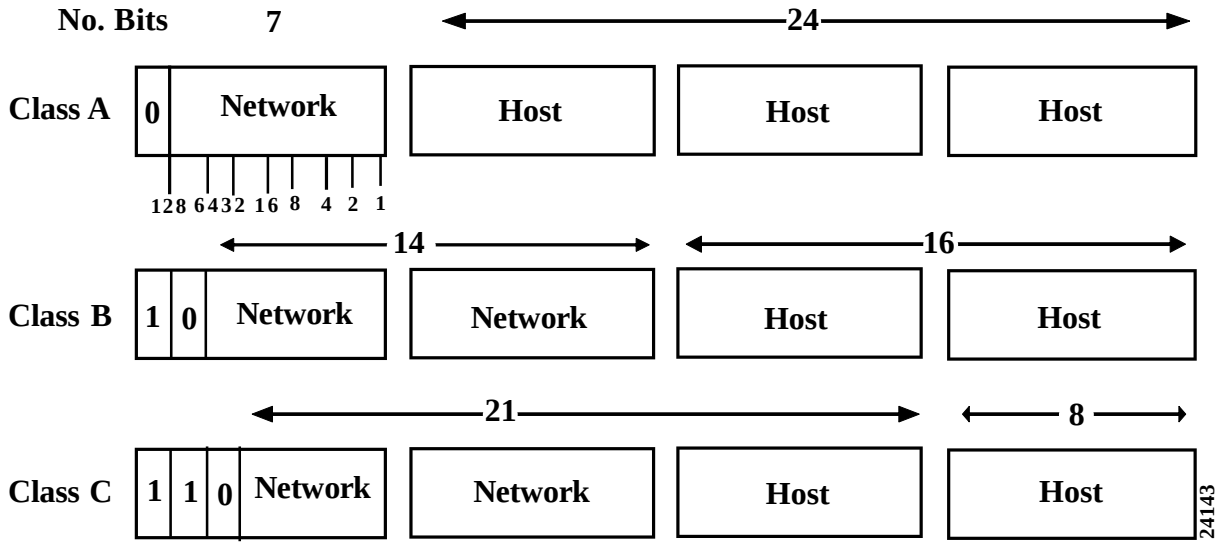


Figure 13.8 : IP address formats

IP address formats

Addresses beginning with **01111111**, or **127** decimal, are reserved for loopback and for internal testing on a local machine. [You can test this: you should always be able to ping **127.0.0.1**, which points to yourself] Class D addresses are reserved for multicasting. Class E addresses are reserved for future use. They should not be used for host addresses.

Now we can see how the Class determines, by default, which part of the IP address belongs to the network (N) and which part belongs to the node (n).

Class A — NNNNNNNN.nnnnnnnn.nnnnnnn.nnnnnnn

Class B — NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnnnnn

Class C — NNNNNNNN.NNNNNNNN.NNNNNNNN.nnnnnnnn

In the example, 140.179.220.200 is a Class B address so by default the Network part of the address (also known as the *Network Address*) is defined by the first two octets (140.179.x.x) and the node part is defined by the last 2 octets (x.x.220.200).

In order to specify the network address for a given IP address, the node section is set to all "0"s. In our example, 140.179.0.0 specifies the network address for 140.179.220.200. When the node section is set to all "1"s, it specifies a broadcast that is sent to all hosts on the network. 140.179.255.255 specifies the example broadcast address. Note that this is true regardless of the length of the node section.

13.6.4 Subnetting

Subnetting an IP Network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security. The most common reason is to control network traffic. In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment. Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

a) The Mask

The network portion of the address is separated from the host portion of the address by a mask.

- The mask simply indicates how many bits are used for the network portion, leaving the remaining bits for the host portion.
- A 24-bit mask indicates that the first 24 bits of the address are network bits, and the remaining 8 bits are host bits.
- A 16-bit mask indicates that the first 16 bits of the address are network bits, and the remaining 16 bits are host bits.
- And so forth
- The difference between a *network mask* and a *subnet mask* will be explained as this tutorial progresses.

b) Subnet Masking

A subnet address is created by *"borrowing"* bits from the host field and designating them as the subnet field. The number of borrowed bits varies and is specified by the subnet mask.

Class B Address : Befor Subnetting

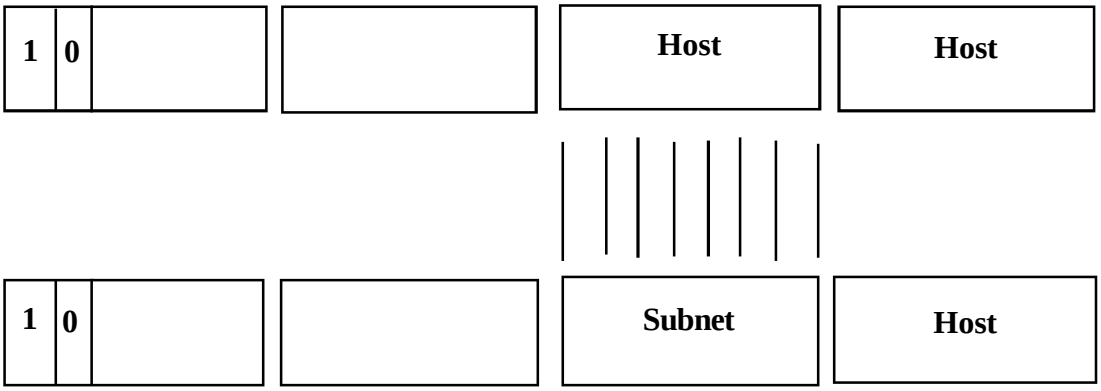


Figure 13.9 : Class B Address : After Subnetting

Subnet masks use the same format and representation technique as IP addresses. The subnet mask has binary 1's in all bits specifying the network and subnetwork fields, and binary 0s in all bits specifying the host field.

Applying a subnet mask to an IP address allows you to identify the network and node parts of the address. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the *Network Address* or Number.

For example, using our test IP address and the default Class B subnet mask, we get:

10001100.10110011.11110000.11001000 140.179.240.200 Class B IP Address

11111111.11111111.00000000.00000000 255.255.000.000 Default Class B Subnet Mask

---

10001100.10110011.00000000.00000000 140.179.000.000 Network Address

Default subnet masks:

Class A - 255.0.0.0 - 11111111.00000000.00000000.00000000

Class B - 255.255.0.0 - 11111111.11111111.00000000.00000000

Class C - 255.255.255.0 - 11111111.11111111.11111111.00000000

More Restrictive Subnet Masks

Additional bits can be added to the default subnet mask for a given Class to further subnet, or break down, a network. When a bitwise logical AND operation is performed between the subnet mask and IP address, the result defines the *Subnet Address*. There are some restrictions on the subnet address. Node addresses of all "0"s and all "1"s are reserved for specifying the local network (when a host does not know it's network address) and all hosts on the network (broadcast address), respectively. This also applies to subnets. A subnet address cannot be all "0"s or all "1"s. This also implies that a 1 bit subnet mask is not allowed. This restriction is required because older standards enforced this restriction. Recent standards that allow use of these subnets have superceded these standards, but many "legacy" devices do not support the newer standards. If you are operating in a controlled environment, such as a lab, you can safely use these restricted subnets.

To calculate the number of subnets or nodes, use the formula (2^n - 2) where n = number of bits in either field. Multiplying the number of subnets by the number of nodes available per subnet gives you the total number of nodes available for your class and subnet mask. Also, note that although subnet masks with non-contiguous mask bits are allowed they are not recommended.

Example:

10001100.10110011.11011100.11001000 140.179.220.200 IP Address

11111111.11111111.11100000.00000000 255.255.224.000 Subnet Mask

---

10001100.10110011.11000000.00000000 140.179.192.000 Subnet Address

10001100.10110011.11011111.11111111 140.179.223.255 Broadcast Address

In this example a 3 bit subnet mask was used. There are 6 subnets available with this size mask (remember that subnets with all 0's and all 1's are not allowed). Each subnet has 8190 nodes. Each subnet can have nodes assigned to any address between the Subnet address and the Broadcast address. This

gives a total of 49,140 nodes for the entire class B address subnetted this way. Notice that this is less than the 65,534 nodes an unsubnetted class B address would have.

Subnetting always reduces the number of possible nodes for a given network. There are complete subnet tables available here for Class A, Class B and Class C. These tables list all the possible subnet masks for each class, along with calculations of the number of networks, nodes and total hosts for each subnet

Every computer, server and other device that connects to the internet needs an address to be found, and these need to be unique across the whole of the network. Managing to keep these unique and ordered is the job of IANA, the *Internet Assigned Numbers Authority*.

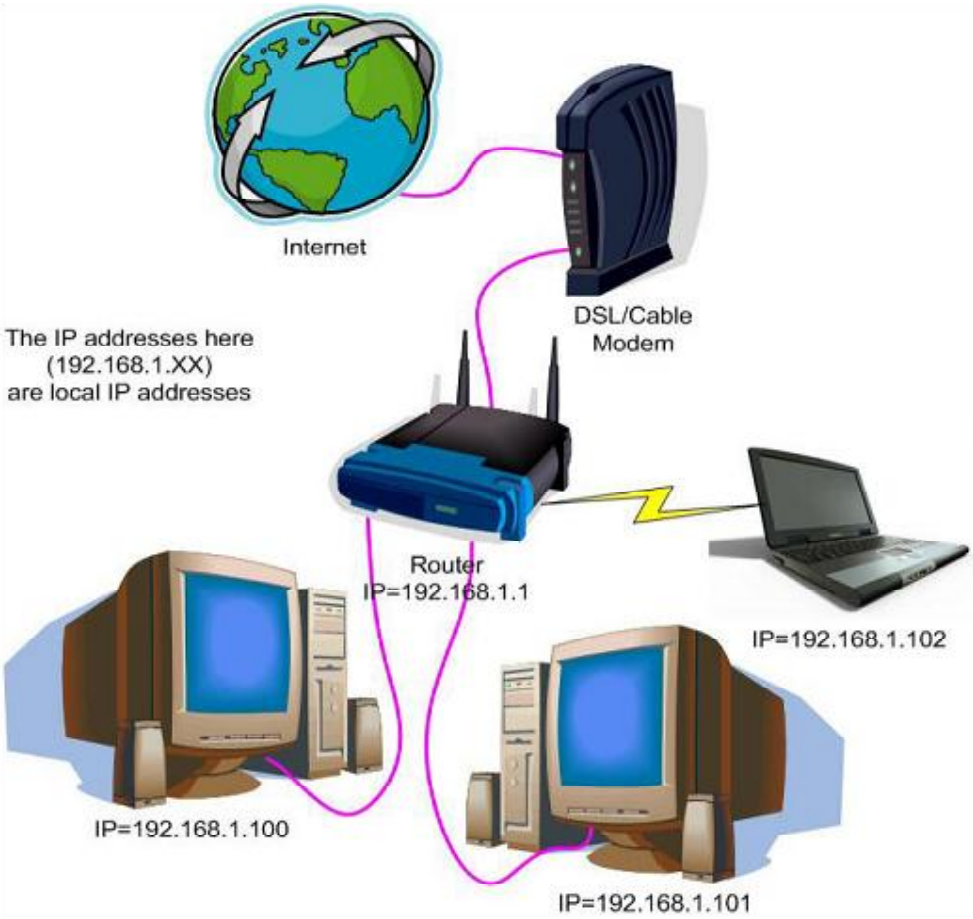


Figure 13.10: IP addressing

13.7 Summary

- A facility that provides a date transfer service among devices attached to the network.
- A collection of communication networks interconected by bridges and/or routers.
- A corporate internet that provides the key Internet applications, expecially the word wide web.
- The www is a repositing of intermation linked together from points all over the world.
- Viruses/worms usually destructive computer programms hide inside of innocent seeking programs, web pages and e-mail attachements.

- . An IP address is a unique identifier for a node or host connection on an IP network.
- The locate a particular page or document on the internet, we need a internet address called a uniform resource locator (URL).
- IP addressing supports five different address classes : A,B,C, D & E.

A submit address is creater by "bowworing" bits from the host field and designating them as the submit field.

13.7 Self Answered Questions

1. How do the layers of the Internet model correlate to the layers of the OSI model?
2. How does information get passed from one layer to the next in the Internet model?
3. What are the responsibilities of the network layer in the Internet model?
4. Name some services provided by the application layer in the Internet layer.
5. What is the number of bits in an IPv4 address?
6. What is the network address in a block of addresses? How can we find the network address if one of the addresses in a block is given?
7. What is the dotted decimal notation in IPv4 addressing. What is the number of bytes in an IPv4 address represented in dotted decimal notation.
8. What are the Internet applications ? explain in brief.
9. What is a mask in IPv4 addressing?
10. What do you know about subnet masking ?
11. What do you know about Internet services? Which services are available in Internet?
12. In electronic mail, what are the tasks of a user agent.
13. Name the common three components of a browser.
14. How is HTTP related to WWW?
15. What is a URL and what are its components?
16. What is the purpose of DNS in the Internet?

13.8 References

1. http://services.exeter.ac.uk/cmit/modules/the_internet/MITxx14-notes.pdf
2. Andrew S. Tanenbaum, "Computers Networks", PHI. India..

Unit-14
Network Security

Structure of the Unit

14.0 Objective

This Chapter primarily focuses

- Introduction to security
- Types of threats like, Trojan Horse, Denial of Service (DoS).
- Unauthorized Access on
- Risk and different types of Risks.
- How to keep our System Secure *(Firewall, Digital Signatures)*

14.1 Introduction

Securing information across a network had its roots in the late 1960s when networks only existed in the sense of huge mainframes and multiple networked terminals.

Network security, however, did initially realize its importance as a result of a white-collar crime performed by a programmer for the financial division of a large corporation. He was able to embezzle money from accounts that rounded their financial statements by transferring the money lost through rounding to a separate account. His actions illustrate the initial threats to network security, which were at the time strictly internal. It was not until the end of the 1960s and into the 1970s that the environment for network security did evolve.

Security over the Internet and over these new Local Area Networks was becoming a very serious concern at this point since an increasing amount of information was traversing many more points of access. The stage is thus set for unbelievable information sharing on both levels and so the need for network security is paramount to prevent against countless threats.

14.2 Network Security

In general Term we say:-

"Security is the quality or state of being secure-to be free from danger."

In Technical Term:-

"Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity."

" Confidentiality : Ensuring that information is not accessed by unauthorized persons"

" Integrity : Ensuring that information is not altered by unauthorized persons in a way that is not detectable by authorized users"

When connecting to a network, we need to make sure no one will easily break in to it. The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. The networks are comprised of "nodes", which are "client" terminals (individual user PCs), and one or more "servers" and/or "host" computers. They are linked by communication systems, some of which might be private, such as within a company and others which might be open to public access. The obvious example of a network system that is open to public access is the Internet, but many private networks also utilize publicly-accessible communications. Today, most companies' host computers can be accessed by their employees whether in their offices over a private communications network, or from their homes or hotel rooms while on the road through normal telephone lines.

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

14.2.1. Why do we need security?

In the ever changing world of global data communications, inexpensive Internet connections, and growing software development, security is becoming more and more of an issue. Security is now a basic requirement because global computing is very insecure. A general example can be when you buy pizza over the internet.

Security issue : Transferring credit card numbers.

As your data goes from point A to point B on the Internet, for example, it may pass through several other points along the way, giving other users the opportunity to grab, and even alter it. It does nothing to protect your data center, other servers in your network, or an unwanted user, so all you need is secure your network.

14.2.2. Why is network security important?

The good neighbor policy- Your mistakes can be someone else's headaches. If your network is insecure and someone takes control of one of your computers, they can use that machine to attack other machines.

Your privacy. Obviously, your records are of great importance. E.g.: Trust between the library and its clients can be harmed if there records are compromised.

Money and time. Tracking down a virus or a worm and eliminating it from your network is frustrating and time-consuming. You often have to rebuild your machines from the starting, reinstalling the operating system and software and restoring data from backup tapes.

14.2.3. Network security concepts

Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name -i.e. the password, which is something the user 'knows'- this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans (types of virus programs) is being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware.Communication between two hosts using a network may be encrypted to maintain privacy.

Security Management

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

What is a Network Threat?

Network Threat is any form of security breaches(break) that may include any of the following : Denial-of-Service (DoS); Unauthorized Access; Executing Commands Illicitly; Confidentiality Breaches; Destructive Behavior; Data Diddling; and Data Destruction.

14.3 Types and Sources Of Network Threat

Attacks are often maliciously used to consume and destroy the resources of a network. Sometimes, misconfigured servers and hosts can serve as network security threats as they unnecessarily consume resources. In order to properly identify and deal with probable threats, one must be equipped with the right tools and security mechanisms.

Attacks are generally classified into two types:

Passive Attacks

Active Attacks

A) Passive Attacks: Passive attacks are those attacks in which the attacker's main aim is to obtain the information which is passing over the network. In this the attackers does not modify the content.

i) Release of Message Contents: If we send a confidential email to our friend and we desire that only she should be able to access it. It means the information should be only between the Sender and Receiver. If someone get that information then the content of the message is released.

ii) Traffic Analysis: Similarly if many such messages are send over a network again and again, a passive attacker could try to figure out the similar content. This will come up with some sort of pattern that provides him some clues regarding the communication that is taking place.

B) Active Attacks: It is just opposite to Passive attacks. In this the Attacker modifies the original message in some manner. The content of the original message is modified and then the modified message passes over the network.

i) Interruption (Masquerade): This is caused when an unauthorized entity pretends to be another entity. In this the person is in the illusion that he/she is communicating with the authorized person. But all the information goes to the Attackers who act like the authorized person.

ii) Replay Attack: In this the user captures the some data units and re-sends them. It means the user capture the information and send same copy of the message to receiver on his behalf.

iii) Alteration of Messages: In this the user captures the original message and re-sends them after altering the content. It means the user capture the information, modify the information and send towards the receiver.

14.3.1 Denial-of-Service

In a denial-of-service (DoS) attack, an attacker attempts to prevent authentic users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to stop you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

DoS (Denial-of-Service) attacks are the most difficult to address. These are dangerous, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, also without refusing valid requests for service.

Denial of service attacks are used to overload a server and make it useless. The server is asked repeatedly to perform tasks that require it to use a large amount of resources until it can no longer function properly.

The attacker will install virus or Trojan software user PC's and instruct them to perform the attack on a specific server. Denial of service attacks can be used by hackers to interrupt the service of another system or by attackers who want to bring down a web server for the purpose of disabling some type of security feature. Once the server is down, they may have access to other functions of a server, such as the database or a user's system. This allows the attacker the means to install software or disable other security features.

The basis of a DoS attack is simple, it sends more requests to the machine than it can handle. The attacker's program simply makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection.

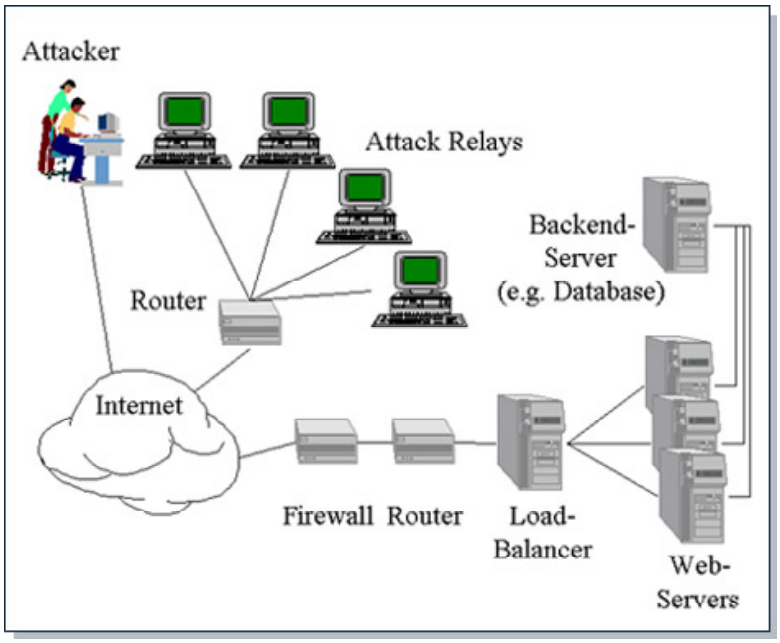


Figure 14.1

Some things that can be done to reduce the risk of being cheated by a denial of service attack include:

- Not running visible-to-the-world servers at a level too close to capacity.
- Using packet filtering to prevent already forged packets from entering into network.
- keeping up-to-date on security-related grounds for our hosts operating systems.

14.3.2. Unauthorized Access

"Unauthorized access" is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that our machine should not provide the attacker. However, that attackers will not be able to compile and install programs, update and patch your systemwithout being sure that the person making such a request is someone who should get it, such as a local administrator.

Even if you implement all security controls on access points, the possible connection of a rogue access point is a significant threat. A rogue access point is an unauthorized access point on the network. An employee might purchase an access point and install it within his office without knowing the security implications. A hacker could also plant a rogue access point within a facility by purposely connecting an unprotected access point to the corporate network.

For that reason, you should continually monitor for the presence of rogue access points.

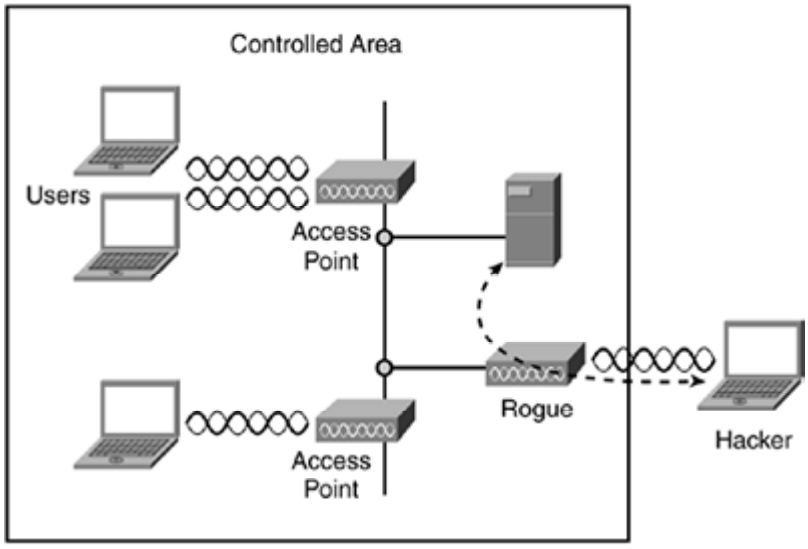


Figure 14.2 : Rogue Access Points Offer an Open Port for Hackers to Exploit

a. Executing commands illicitly:

Unlawfully executing commands is a crucial situation.

There are two main classifications of the malice of this problem:

- Normal user access, and
- Administrator access.

A normal user can do a number of things on a system (such as read files, mail them to other people, etc.) that an attacker should not be able to do. This might, then, be the overall access that an attacker needs.

On the other hand, an attacker might wish to make configuration changes to a host. In this case, the attacker will need to gain administrator privileges on the host.

b. Confidentiality Breaches

If a person without the permission of owner or any other person in charge of a computer, computer system or computer network, accesses or secures access to such computer, computer system or computer network mainly comes under security breach.

We need to examine the threat. What is it that we are trying to protect ourselves against? There is certain information that could be quite damaging if it fell into the hands of a competitor, an enemy, or the public. In these cases, it's possible that compromise of a normal user's account on the machine can be enough to cause damage.

While many of the attackers of these sorts of break-ins are merely thrill-seekers interested in nothing more than to see a shell prompt for our computer on their screen, there are those who are more malicious.

c. Destructive Behavior

Among the destructive sorts of break-ins and attacks, there are two major categories.

A. DATA DIDDLING

Data diddling is the changing of data before or during entry into the computer system. Examples include forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements.

This type of attack is likely the worst sort, since the fact of a break-in might not be immediately obvious. Perhaps the numbers in our spreadsheets or the dates in our projections and plans might be changed.

B. DATA DESTRUCTION

Some of those accomplished attacks are simply twisted jerks who like to delete things. In these cases, the impact on our computing capability -- and consequently our business -- can be nothing less than if a fire or other disaster caused our computing equipment to be completely destroyed.

14.3.3 Computer Security Risks to home users

The home computer user is often said to be the weakest link in computer security. They do not always follow security advice, and they take actions which leads there trap into threats that compromise themselves.

There are a number of pieces of malicious code spreading on the Internet through email attachments, known as software vulnerabilities.

Attackers target home users who have cable modem and DSL (digital subscriber line) connections because many home users do not keep their machines up to date with security, as they do not run current anti-virus software, and do not exercise caution when handling email attachments. Everyone should take precautions, and recover if you have been compromised.

1. What is at Risk?

Information security is concerned with four main areas:

Confidentiality - Information should be available only to those who rightfully have access to it. Loss of confidentiality is known as interception.

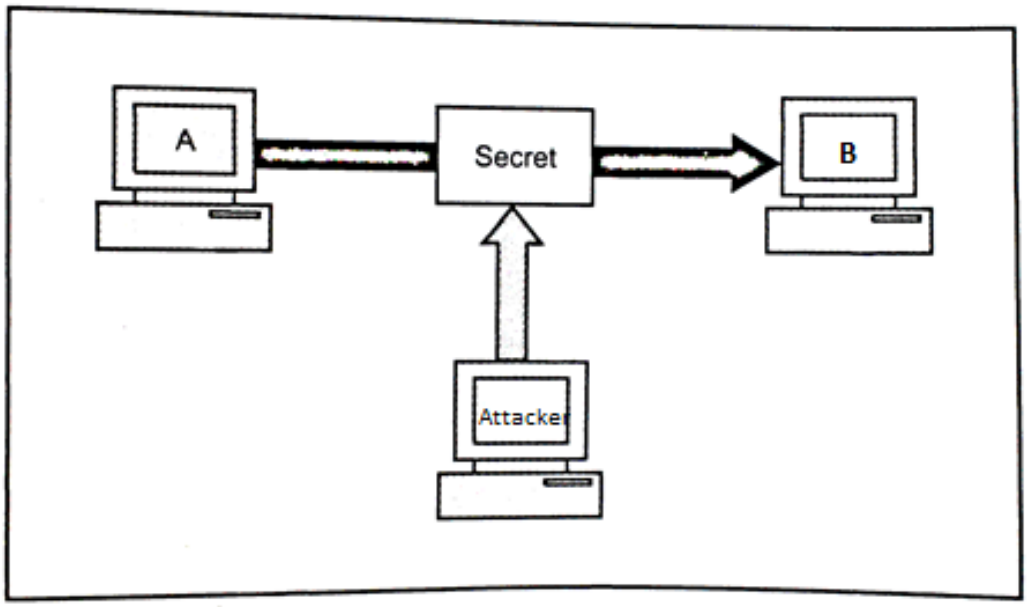


Figure 14.3 : Loss of Confidentiality

Integrity -Information should be modified only by those who are authorized to do so. Loss of Integirty is called Modification.

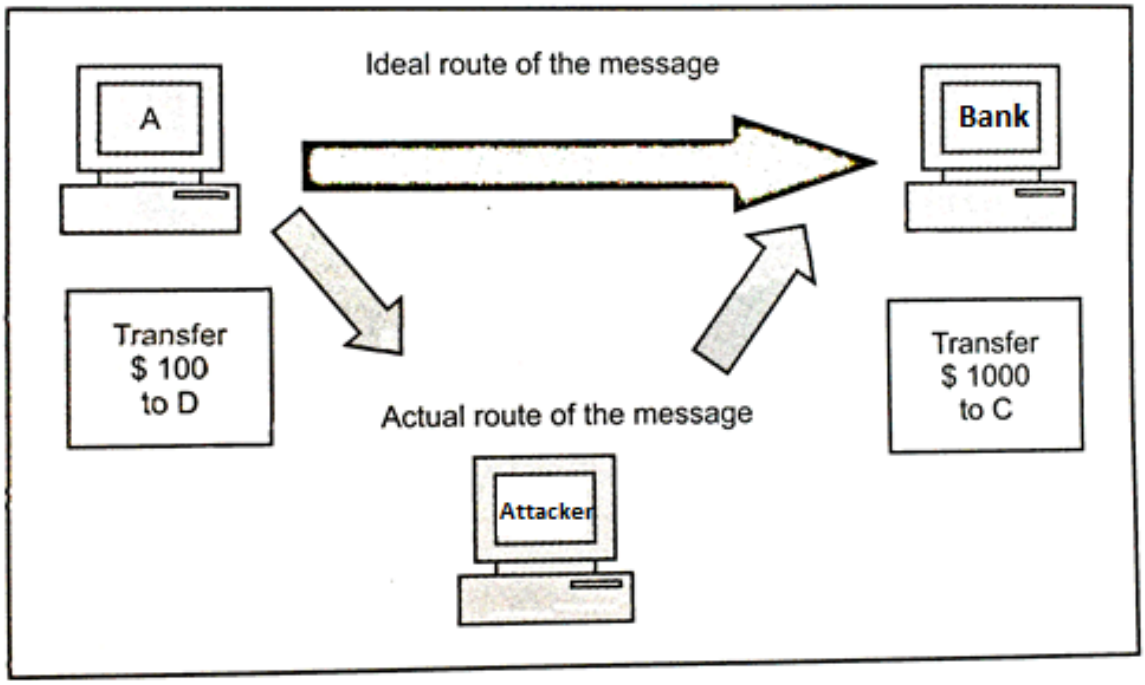


Figure 14.4 : Loss of Integrity

Authentication - It helps to prove the identity of the Sender. It ensures that the origin of a electronic message or document is correctly identified. Absence of Authentication is called Fabricartion.

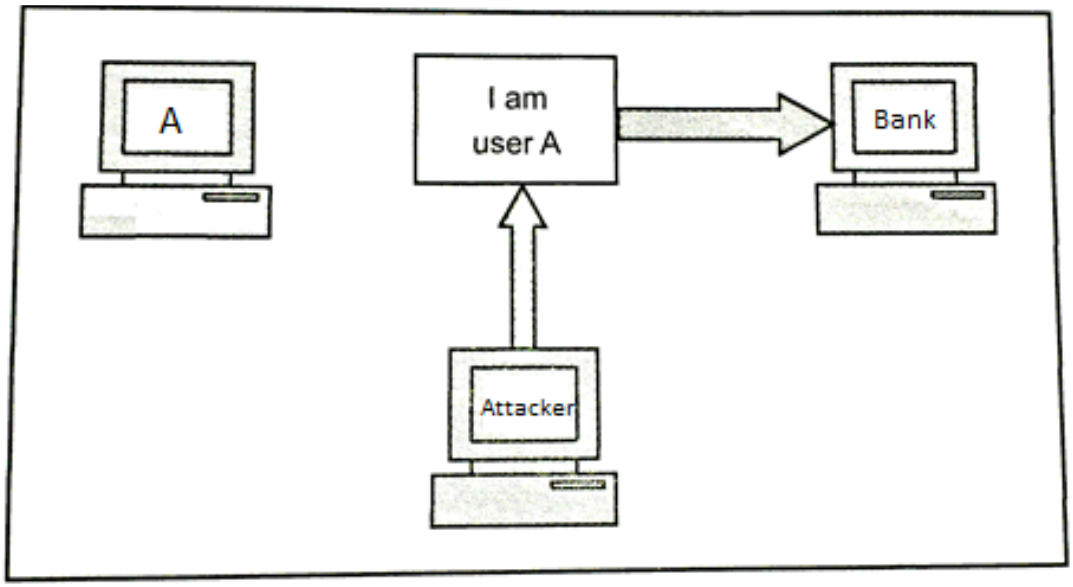


Figure 14.5 : Absence of Authentication

Non-repudiation - The sender of the message cannot deny/refuse the claim of sending the message.

These concepts apply to home Internet users just as much as they would to any corporate or government network. We probably wouldn't let a stranger look through our important documents. In the same way, we may want to keep the tasks we perform on our computer confidential, whether it's tracking our investments or sending email messages to family and friends. Also, we should have some assurance that the information we enter into our computer remains untouched and is available when we need it.

Some security risks arise from the possibility of intentional misuse of our computer by hackers via the Internet. Others are risks that we would face even if we weren't connected to the Internet (e.g. hard disk failures, theft, power down). The bad news is that we probably cannot plan for every possible risk. The good news is that we can take some simple steps to reduce the chance that we'll be affected by the most common threats -- and some of those steps help with both the intentional and accidental risks we are likely to face.

2. Types Of Risks

The most common methods used by hackers to gain control of home computers are briefly described below.

a. Trojan horse programs

Trojan software is considered to be the most harmful in terms of security due to its ability to secretly connect and send confidential information. These programs are developed for the specific purpose of communicating without the chance of detection. Trojans can be used to filter data from many different clients, servers, and database systems. Trojans can be installed to monitor emails, instant messages, and databasecommunications, of other services.

Trojan horse programs are a common way for hackers to trick us; it is also referred to as "social engineering", into installing "back door" programs. These can allow hackers easy access to our computer without our knowledge, change our system configurations, or infect our computer with a computer virus. Trojan horses can make copies of them, steal information, or harm their host computer systems.Many Trojans rely on drive-by downloads or install via online games or internet-driven applications in order to reach target computers.

b. Back door and remote administration programs

A backdoor in a computer system (or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.

On Windows computers, three tools commonly used by hackers to gain remote access to our computer are BackOrifice, Net bus, and Sub Seven. These back door or remote administration programs, once installed, allow other people to access and control our computer.

c. Denial of service

Another form of attack is called a denial-of-service (DoS) attack. This type of attack causes our computer to crash or to become so busy processing data that we are unable to use it. In most cases, the latest patches will prevent the attack.

It is important to note that in addition to being the target of a DoS attack, it is possible for our computer to be used as a participant in a denial-of-service attack on another system.

d. Being an intermediary for another attack

Hackers will frequently use compromised computers as launching pads for attacking other systems. An example of this is how distributed denial-of-service (DoS) tools are used. The hackers install an "agent" (frequently through a Trojan horse program) that runs on the compromised computer awaiting further instructions. Then, when a number of agents are running on different computers, a single "handler" can instruct all of them to launch a denial-of-service attack on another system. Thus, the end target of the attack is not our own computer, but someone else's -- our computer is just a convenient tool in a larger attack.

e. Unprotected Windows shares

Unprotected Windows networking shares can be exploited by hackers in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the Internet. The greater immediate risk to the Internet community is the potentially large number of computers attached to the Internet with unprotected Windows networking shares combined with distributed attack tools.

Another threat includes malicious and destructive code, such as viruses or worms, which leverage unprotected Windows networking shares to propagate. One such example is the 911 worm.

There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

f. Mobile code (Java/JavaScript/ActiveX)

There have been reports of problems with "mobile code" (e.g. Java, JavaScript, and ActiveX). These are programming languages that let web developers write code that is executed by our web browser. Although the code is generally useful, it can be used by hackers to gather information (such as which web sites we visit) or to run malicious code on our computer. It is possible to disable Java, JavaScript, and ActiveX in our web browser. Also be aware of the risks involved in the use of mobile code within email programs. Many email programs use the same code as web browsers to display HTML. Thus, vulnerabilities that affect Java, JavaScript, and ActiveX are often applicable to email as well as web pages.

g. Cross-site scripting

A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to us, the malicious script is transferred to our browser.

We can expose our web browser to malicious scripts by following links in web pages, email messages, or newsgroup postings without knowing what they link to using interactive forms on an untrustworthy site viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags.

h. Email spoofing

Email "spoofing" is when an email message appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Spoofed email can range from harmless pranks to social engineering. Examples of the latter include email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not comply email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information.

We should make a note that while service providers may occasionally request that we change our password, they usually will not specify what we should change it to. Also, most legitimate service providers would never ask us to send them any password information via email. If we suspect that we may have received a spoofed email from someone with malicious intent, we should contact our service provider's support personnel immediately.

i. Email borne viruses

Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, we should be sure of the source of the attachment. It is not enough that the mail originated from an address we recognize. The Melissa virus spread precisely because it originated from a familiar address.

Many recent viruses use these social engineering techniques to spread. Examples include:

o W32/Sircam

o W32/Goner

We should never run a program unless we know it to be authored by a person or company that we trust. Also, programs of unknown origin should not be sent to our friends or coworkers simply because they are amusing -- they might contain a Trojan horse program.

j. Chat clients

Internet chat applications, such as instant messaging applications and Internet Relay Chat (IRC) networks, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialog, web URLs, and in many cases, files of any type.

Because many chat clients allow for the exchange of executable code, they present risks similar to those of email clients. As with email clients, care should be taken to limit the chat client's ability to execute downloaded files. As always, we should be wary of exchanging files with unknown parties.

k. Packet sniffing

The connection between a user's computer and the web server can be "sniffed" to gather large amount of data concerning a user including credit card information and passwords. A packet sniffer is used to gather data that is passed through a network. It is very difficult to detect packet sniffers because their function is to capture network traffic as they do not manipulate the data stream. The use of a Secure

Socket Layer connection is the best way to ensure that attackers utilizing packet sniffers cannot steal sensitive data.

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travel over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, hackers can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require administrator-level access.

Relative to DSL and traditional dial-up users, cable modem users have a higher risk of exposure to packet sniffers since entire neighborhoods of cable modem users are effectively part of the same LAN. A packet sniffer installed on any cable modem user's computer in a neighborhood may be able to capture data transmitted by any other cable modem in the same neighborhood.

14.4 Digital Signature

A Digital Signature Certificate, like hand written signature, establishes the identity of the sender filing the documents through internet which sender cannot revoke or deny. Accordingly, Digital Signature Certificate is a digital equivalent of a hand written signature which has an extra data attached electronically to any message or a document.

Digital Signature also ensures that no alterations are made to the data once the document has been digitally signed. A DSC is normally valid for 1 or 2 years, after which it can be renewed.

A Digital Signature is a method of verifying the authenticity of an electronic document.

Digital signatures are going to play an important role in our lives with the gradual electronization of records and documents. The IT Act has given legal recognition to digital signature meaning, thereby, that legally it has the same value as handwritten or signed signatures affixed to a document for its verification. The Information Technology Act, 2000 provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents.

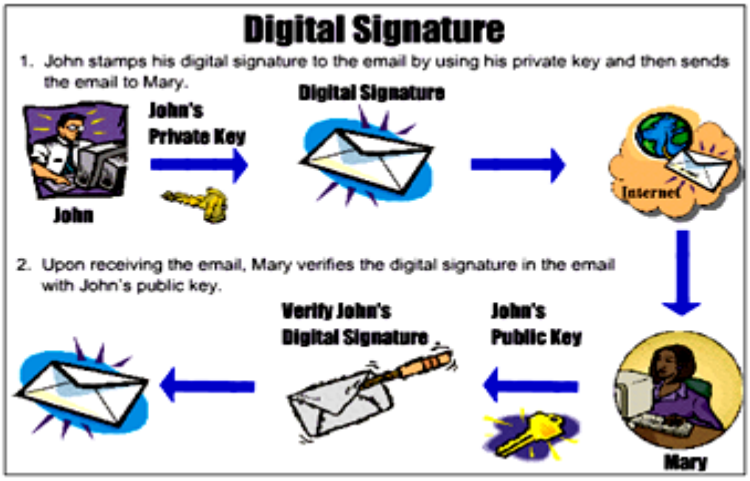


Figure 14.6 : Digital Signature

Message Digest technique is used for Digital Signature to ensure Confidentiality.

What is a message digest?

A message digest is a value consisting of a fixed number of bytes that represents a message of arbitrary length.

It is often referred to as the fingerprint of the message.

When computed two or more times using the same algorithm, the same message will always produce the same digest value.

The digital signature for a message is generated in two steps:

1. A message digest is generated. A message digest is a 'summary' of the message we are going to transmit, and has two important properties:

- It is always smaller than the message itself and
- Even the slightest change in the message produces a different digest. The message digest is generated using a set of hashing algorithms.

2. The message digest is encrypted using the sender's private key. The resulting encrypted message digest is the digital signature.

Message Digest basically use 2 algorithm named :

A) MD5

B) SHA

14.5 Firewalls

A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

A firewall's primary use is to filter out communications that may be threatening to a system. It limits traffic to a system and only allows pre-determined activity to pass through its filter. Firewalls can also be configured so that connections are only authenticated if they are from a specific source machine.

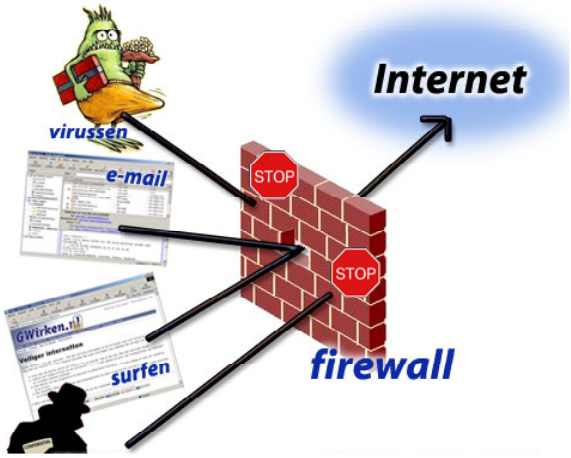


Figure 14.7 : Working of Firewall

In order to provide some level of separation between an organization's intranet and the Internet, firewalls have been employed. A firewall is simply a group of components that collectively form a barrier between two networks.

A number of terms specific to firewalls and networking are going to be used throughout this section, so let's introduce them all together.

- **Bastion host**

A general-purpose computer used to control access between the internal (private) network (intranet) and the Internet (or any other untrusted network). Typically, these are hosts running a flavor of the UNIX operating system that has been customized in order to reduce its functionality to only what is necessary in order to support its functions. Many of the general-purpose features have been turned off, and in many cases, completely removed, in order to improve the security of the machine.

- **Router**

A special purpose computer for connecting networks together. Routers also handle certain functions, such as routing, or managing the traffic on the networks they connect.

- **Access Control List (ACL)**

Many routers now have the ability to selectively perform their duties, based on a number of facts about a packet that comes to it. This includes things like origination address, destination address, destination service port, and so on. These can be employed to limit the sorts of packets that are allowed to come in and go out of a given network.

- **Demilitarized Zone (DMZ)**

The DMZ is a critical part of a firewall: it is a network that is neither part of the untrusted network, nor part of the trusted network. But, this is a network that connects the untrusted to the trusted. The importance of a DMZ is tremendous: someone who breaks into your network from the Internet should have to get through several layers in order to successfully do so. Those layers are provided by various components within the DMZ.

- **Proxy**

This is the process of having one host act in behalf of another. A host that has the ability to fetch documents from the Internet might be configured as a proxy server, and host on the intranet might be configured to be proxy clients. In this situation, when a host on the intranet wishes to fetch any web page, for example, the browser will make a connection to the proxy server, and request the given URL. The proxy server will fetch the document, and return the result to the client. In this way, all hosts on the intranet are able to access resources on the Internet without having the ability to direct talk to the Internet.

14.5.1 Types of Firewalls

There are three basic types of firewalls, and we'll consider each of them.

1. Application Gateways

The first firewalls were application gateways, and are sometimes known as proxy gateways. These are made up of bastion hosts that run special software to act as a proxy server. This software runs at the Application Layer of the ISO/OSI Reference Model, hence the name. Clients behind the firewall must be proxitized (that is, must know how to use the proxy, and be configured to do so) in order to use Internet services. Traditionally, these have been the most secure, because they don't allow anything to pass by default, but need to have the programs written and turned on in order to begin passing traffic.

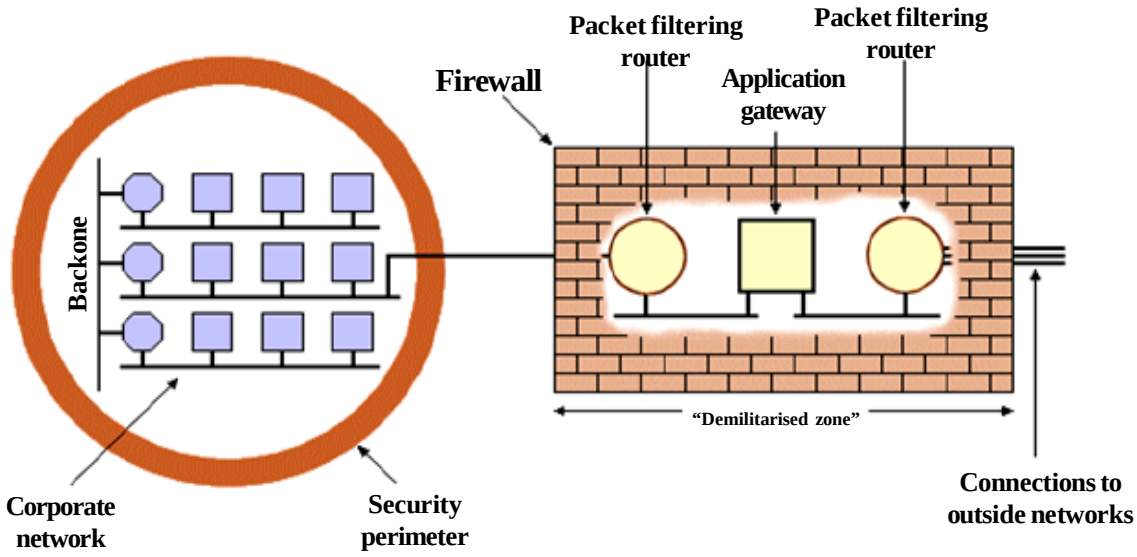


Figure 14.8 : A sample application gateway

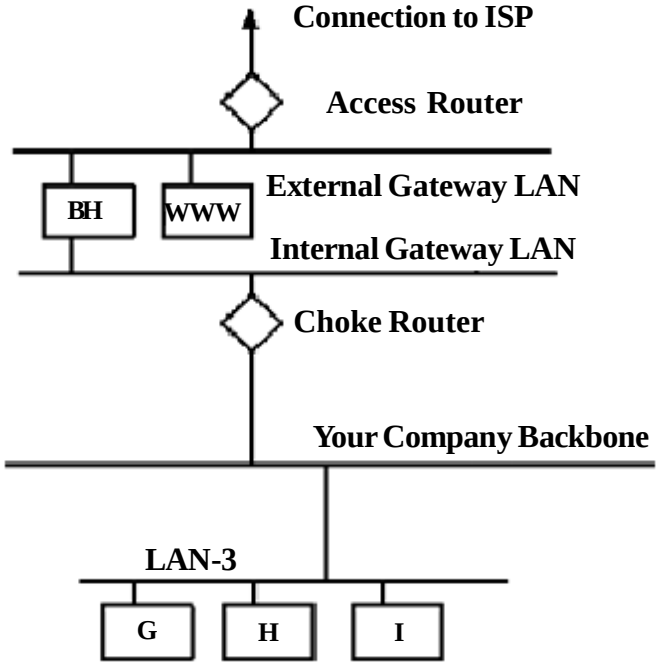


Figure 14.9 : Working of Gateways

These are also typically the slowest, because more processes need to be started in order to have a request serviced.

2. Packet Filtering

Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on. By default, a router will pass all traffic sent it, and will do so without any sort of restrictions. Employing ACLs is a method for enforcing your security policy with regard to what sorts of access you allow the outside world to have to your internal network, and vice versa.

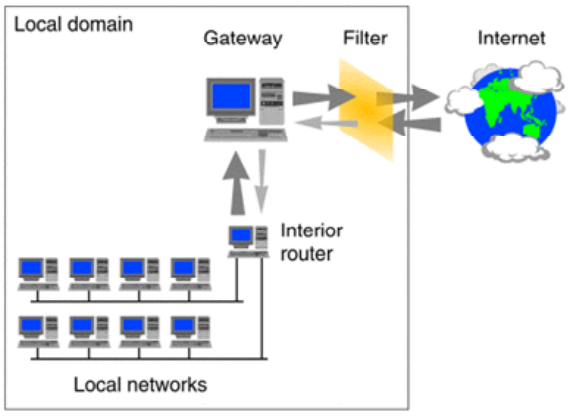


Figure 14.10 : Packet Filtering

There is less overhead in packet filtering than with an application gateway, because the feature of access control is performed at a lower ISO/OSI layer (typically, the transport or session layer). Due to the lower overhead and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins. Figure 6 shows a packet filtering gateway.

Because we're working at a lower level, supporting new applications either comes automatically, or is a simple matter of allowing a specific packet type to pass through the gateway. (Not that the possibility of something automatically makes it a good idea; opening things up this way might very well compromise your level of security below what your policy allows.)

There are problems with this method, though. Remember, TCP/IP has absolutely no means of guaranteeing that the source address is really what it claims to be. As a result, we have to use layers of packet filters in order to localize the traffic. We can't get all the way down to the actual host, but with two layers of packet filters, we can differentiate between a packet that came from the Internet and one that came from our internal network. We can identify which network the packet came from with certainty, but we can't get more specific than that.

3. Hybrid Systems

In an attempt to marry the security of the application layer gateways with the flexibility and speed of packet filtering, some vendors have created systems that use the principles of both.

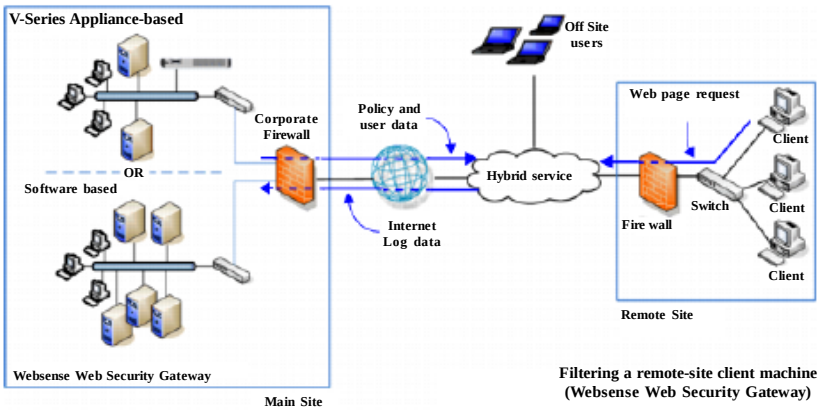


Figure14.11 : Hybrid System

In some of these systems, new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure that only packets that are part of an ongoing (already authenticated and approved) conversation are being passed.

Other possibilities include using both packet filtering and application layer proxies. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get to services on the internal network, will have to break through the access router, the bastion host, and the choke router.

So, what's best for me?

Lots of options are available, and it makes sense to spend some time with an expert, either in-house, or an experienced consultant who can take the time to understand your organization's security policy, and can design and build a firewall architecture that best implements that policy. Other issues like services required, convenience, and scalability might factor in to the final design.

Some Words of Caution

The business of building firewalls is in the process of becoming a commodity market. Along with commodity markets come lots of folks who are looking for a way to make a buck without necessarily knowing what they're doing. Additionally, vendors compete with each other to try and claim the greatest security, the easiest to administer, and the least visible to end users. In order to try to quantifythe potential security of firewalls, some organizations have taken to firewall certifications. The certification of a firewall means nothing more than the fact that it can be configured in such a way that it can pass a series of tests. Similarly, claims about meeting or exceeding U.S. Department of Defense ``Orange Book'' standards, C-2, B-1, and such all simply mean that an organization was able to configure a machine to pass a series of tests. This doesn't mean that it was loaded with the vendor's software at the time, or that the machine was even usable. In fact, one vendor has been claiming their operating system is ``C-2 Certified'' didn't make mention of the fact that their operating system only passed the C-2 tests without being connected to any sort of network devices.

Such gauges as market share, certification, and the like are no guarantees of security or quality. Taking a little bit of time to talk to some knowledgeable folks can go a long way in providing you a comfortable level of security between your private network and the big, bad Internet.

Additionally, it's important to note that many consultants these days have become much less the advocate of their clients, and more of an extension of the vendor. Ask any consultants you talk to about their vendor affiliations, certifications, and whatnot. Ask what difference it makes to them whether you choose one product over another, and vice versa. And then ask yourself if a consultant who is certified in technology XYZ is going to provide you with competing technology ABC, even if ABC best fits your needs.

Single Points of Failure

Many ``firewalls'' are sold as a single component: a bastion host, or some other black box that you plug your networks into and get a warm-fuzzy, feeling safe and secure. The term ``firewall'' refers to a number of components that collectively provide the security of the system. Any time there is only one component paying attention to what's going on between the internal and external networks, an attacker has only one thing to break (or fool!) in order to gain complete access to your internal networks.

14.6 Summary

• Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity.

• Main principals of Security is Authentication, Confidentiality, Integrity and Non Repudation.

• A Digital Signature is a method of verifying the authenticity of an electronic document.

• A Firewall is used to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set.

14.7 Self-Assessment Questions

1. Define Network Security? Explain the need of security. What are its objectives?
2. Explain the principals of Security?
3. What are Network Threats? Explain the types of Threats?
4. Write short notes on
   a) Denial of Service(DoS)
   b) Digital Signature
   c) Firewall
5. What are Risks? Explain some type of Risks?
6. What is Firewall? Explain type of Firewalls used?
7. What is Digital Signature? Explain how Message Digest is used to implement Confidentiality?

14.8 References

1. Atul Kahate, “Cryptography and Network Security”.

Unit-15

Indian Networks

Structure of the Unit

15.0 Objective

This chapter provides a general Overview :

- Introduction to NICNET
- Specialized Networks
- Researches in India
- Social Implementation & Telemetric Society.

15.1 Introduction

The world has been witnessing a knowledge and information explosion during the past few decades. Over 10 million journal articles are published every year besides news items, editorials and articles that are appearing in popular print media. Information professionals who would be the leaders in the twenty-first century depend on information for their work. Access to information holds the key to development. Libraries which are store houses of knowledge and information, and information centers which disseminate knowledge and information, form two important components of present day society.

While there is a deluge of information on one hand, the cost of collecting, processing, storing and disseminating information has been spiraling up on the other hand. This calls for heavy budgets for libraries even to maintain a reasonable level of acquisition of journals, books and reports. Estimates show that a three to fourfold rise in library budgets will be needed by AD 2000 to maintain the same acquisition level as in 1990. Information buying power of libraries has been declining year after year. Because of this, resource sharing and cooperative functioning through networking have become inescapable for libraries and information centre's worldwide. India is no exception; for that matter, it is even more necessary to network libraries in newly developing countries like India than in the developed nations. Efficient resource sharing can be achieved by using the recent advances in information technology for realizing a network of libraries. Information technology signifies the coming together of the disciplines of electronics, computer hardware and software, communications (in particular telecommunications), artificial intelligence and human/ machine interface.

This has resulted in discernible change in the information scenario. Now a large number of library resource sharing networks like the Metropolitan Area Networks, such as CALIBNET (Calcutta), DELNET (Delhi), BONET (Bombay), PUNENET (Pune), MALIBNET (Madras), MYLIBNET (Mysore), HYLIBNET (Hyderabad), ADNET (Ahmedabad), and countrywide ones like ERNET (Educational and Research Institutions), SIRNET (CSIR Laboratories), INFLIBNET (Universities and Research Institutions) and DESINET (Defense Laboratories), and sectoral ones like BTISNET (Biotechnology) and TIFACLINE (Technology per se) are under various stages of conceptualization, design and development. A host of agencies, like the National Information System for Science and Technology (NISSAT), Dept. of Electronics, INSDOC/ CSIR, DESIDOC/DRDO, DBT, NIC, and TIFAC/DST, are involved. Looking from the participant's side, it is common to find an institution participating in more than one network. The ultimate goal of information/library networks is to interlink information resources in a metropolitan area, so that user could access information irrespective of its location, format, medium, language, script etc. Further, the development of such networks requires actions in several areas such as training, rationalization of information resource acquisition, diffusion of standards, preparation of union lists, and generation of database services apart from setting up hardware, software and communication facilities.

The concept of library networking to aid information resource sharing and support activities in libraries has become a real necessity. The shortcomings observed are mainly related to two aspects:

- Non-availability of materials and services, and
- Efficient administrative control.

In India, the need for resource sharing has been well recognized but the technology options available until now were limited. NISSAT has taken up networking of libraries in Calcutta (CALIBNET), Delhi (DELNET), Madras (MALIBNET), Mysore (MYLIBNET), Hyderabad (HYLIBNET), Ahmedabad (ADNET), Pune (PUNENET), and Bombay (BONET). The present study highlights only some of the major library networks in India.

Towards library networking activities in India NISSAT has taken the initiative for promoting resource sharing activities. These initiatives are aimed at ensuring better utilization of science and technology information resources, minimization of functional load of information centre's and encouragement of motivational factors to a large extent by better means of communication. NISSAT only goes to the extent of setting up general infrastructural facilities like network service centre's including hardware, software, manpower and other organizational requirements, communication facilities etc. With a change in the development and implementation strategy, the participating institutions in a network are to arrange their own terminal hardware, software, manpower and data conversion.

The progress in networking in India has been rather slow due to the poor extension of telecommunication networks and overwhelming use of resources and expertise that are available. How-ever, the scene is changing fast. The Department of Telecommunication is setting up a Public Data Network (PDN) and has plans to expand and revamp the existing telephone system. The potential of data networks in India has already been recognized, and few networks have already come into operation.

Networks that are already in operation or in various stages of development may be classified into the following two categories depending upon their scope and objectives:

- General networks (i.e., NICNET, INDONET and VIKRAM)
- Specialized networks (i.e., CALIBNET, DELNET, BONET, ERNET, INFLIBNET, BTISNET etc.)

15.2 General Networks

15.2.1 Introduction to NICNET

National Informatics Centre (NIC) is a leading organization in the field of Information Technology (IT) in India. It provides state of the art solutions to the information management and decision support requirements of the Govemment and the corporate sector. NIC has set up a satellite-based nation-wide computer-communication network, called NICNET, with over 700 nodes connecting the national capital, the state capitals and district headquarters to one and another.

NICNET FACILITIES

NICNET was designed and implemented by NIC using state-of-the-satellite-based computer-communication technology. Keeping in view the wide geographic spread of the country, ranging from islands in Indian ocean to the highest Himalayan ranges, in design of NICNET, which is one of the largest VSAT networks of its kind in the world, ensures extremely cost effective and reliable implementation.

NICNET has now become an integral part of a large number of Government and Corporate sector organizations, providing information exchange services. NICNET services include File Transfer, Electronic Mail, Remote Database Access, Data broadcast and EDI. In times of natural calamities like cyclones, NICNET has served as the basic message communication facility in the calamity-affected areas.

A large number of users including banks, financial institutions, exporters, ports and custom houses are targeted for provision of EDI services on NICNET. NICNET provides gateway to International Networks for Electronic Mail, Database Access and EDI services.

IMPORTANT PROJECTS:

- *Inventory Management Information System for Electricity Dept.*

- *Budget Information System for Budget Dept.*
- *Election Results Information System for Election Dept.*
- *Old Age Pension Disbursement System for Social Welfare Dept.*
- *Application Monitoring System for Industries.*
- *Property Tax Information System and Birth and Death Information System for Pondicherry Municipality.*
- *Excise Information System for Excise Dept.*
- *Price Monitoring Ration Card Information System for Civil Supplies Dept.*
- *Commercial Tax Information System.*
- *Transport Information System.*

IT SERVICES BY NIC:

- *The IT services provided by NIC are: Conducting feasibility studies for computerization; Designing; Developing and Implementing computer-based information systems; to undertaking large projects.*
- *NIC is having highly skilled pool of manpower numbering more than 3000.*
- *NIC has extensive software development capabilities in the areas of databases, computer aided design, networking, geographic information systems, analytical modeling, expert systems, telemetric, multimedia etc.*
- *It has developed over 3000 databases in various sectors such as Education, Health, Transport, Agriculture etc.*
- *NIC has been instrumental in processing very large volumes of data related to the 1991 Population Census and Industrial Census.*
- *NIC has also developed a number of network-based applications; most notable are General Elections in India.*
- *Developing & hosting of Web sites of Govt. Office (Central/State) as well as of private organization, Educational, Research Institutes etc. on NIC Web Servers.*

15.2.2 INDONET

The INDONET (Basu & Saxena, 1987) data network was engineered by CMC Limited for the computer user community in India. It is an integrated information management and distributed data processing facility. The INDONET aims to provide facility for distributed data processing on all India bases to large organizations in the network using the CMC computers for their data processing operations. It also plans for provision of data communications between its users in their respective locations in the network, even if the users are not accessing CMC's nodal computers. Distributed databases in various subjects and access to specialized applications software locally, or in remote locations obviate the need for duplication of software and hardware facilities at each location. The INDONET nodes at Bangalore, Bombay, Delhi, Hyderabad and Pune are connected to the GPSS of the Videsh Sanchar Nigam Limited, thereby facilitating entry to Public Data Networks of other countries.

In phase I, an experimental INDONET Pilot Satellite Network (IPSN) incorporating all the features of the proposed INDONET was worked out. IPSN connects nodes in Bombay, Calcutta, Madras, Delhi, Hyderabad, Bangalore, Vishakhapatnam, Ahmedabad and Pune with IBM 436 computers and MUXs/

cluster controllers. The network uses IBM's Computers and Systems Net-work Architecture and 4800 bps leased lines, 9600 bps packet radio links for intra-city connection.

In the second phase, the INDONET would operate as a Star Network with control point in Delhi using root top 3-m earth stations and packet switching. Beside SNA, it will also support X.25 protocols satellite and radio communication the INDONET is expected to cover 35 major cities of India. The CMC Ltd. is closely involved with NISSAT activities in library networking programmes in Calcutta and Delhi.

15.2.3 VIKRAM

Vikram is the packet switched public data network under development by the Department of Telecommunications. This network will initially have 8 switching nodes in Delhi, Bombay, Calcutta, Madras, Bangalore, Hyderabad, Ahmedabad and Pune and 12 remote access nodes with its network management centre located at Delhi. It will support packet switching interface to CCITTs X.25, X.28, X.29 and X.75 recommendations.

15.3 Specialised Networks

15.3.1. CALIBNET

The Calcutta Library Network (CALIBNET) was inaugurated on 21 December 1993. NISSAT, Department of Scientific and Industrial Research (DSIR), Govt. of India, took the initiative in setting up CALIBNET, which has adopted a two way system for networking:

- *The networking route with a library automation and networking through its own application software "Maitrayee" and*

- *The e-mail route connecting member libraries with on-line access to various databases within network and Internet access.*

CALIBNET established a high-tech resource base and provides the following services:

- *Online/CDROM based global information search and retrieval services*
- *Full-text document delivery*
- *Database services*

15.3.2 DELNET

The limitation of financial resources and space for housing library collections in the libraries in Delhi led to the promotion of sharing of resources by automation and networking and establishment of the DELNET in 1988. NISSAT took the initiative in setting up DELNET. It has emerged as an important resource centre for the libraries in Delhi.

In Delhi the libraries have been growing very fast in number and site during the last four decades. They cater to specialized and general clientele and are of various types which include institutional libraries, research libraries, government libraries, public libraries, departmental libraries and libraries of the universities, colleges and schools. During the recent years, cumulative information has been increasing at a very fast pace and with it the increase in demands of the users. It has been noticed that in the era of information explosion the libraries in India are generally ill equipped to handle and retrieve information effectively. As already mentioned, the financial resources and the space for housing library collections are limited in almost all of the libraries. The option left with the forward looking librarians has been to promote the sharing of resources by automation and networking.

Initially, 40 libraries were directly linked to the DELNET host system through e-mail to promote library mailing, interlibrary requests, transfer of files, exchange of messages, interlibrary services, etc. Side by side with the automation of participating libraries, the functions and services have also started. Presently

about 90 libraries are members of DELNET. Almost all participating libraries are now computerized by means of acquisition and fund accounting, cataloguing, circulation, serials control and local users services. Users are able to locate books and serials through Online Public Access Catalogue (OPAC). A union catalogue of current periodicals available in Delhi libraries, and a union list of current serials available in Indian libraries are available on online for DELNET participant libraries. A central database of DELNET has been created and made operational. This central database includes the library holdings of DELNET member libraries used as union catalogues of books/monographs.

DELNET provides access to the central union catalogue for books and monographs, efficient electronic mailing facilities to access databases of member libraries. It also proposes to develop a network for accessing CD-ROM databases available at member libraries in the near future. DELNET also provides CAS and SDI services, consultancy in library computerization, training and H.R.D. and assistance to libraries on standardization, local automation, retrospective conversion etc. DELNET is likely to emerge as a co-operative network incorporating all disciplines of science, technology, social sciences and humanities.

15.3.3 ERNET(Education and Research Network)

ERNET has made significant contribution to the emergence of networking in the country. It practically brought the internet in India and has built up national capabilities in area of networking, especially in protocol software engineering. It has not only succeeded in building large network that provides various facilities to intellectual segment of Indian society - the research and education community, it has over the year become trendsetter in the field of networking. The science community of the country has recognized ERNET'S contribution both for infrastructure services as well as R &D(research & development). The scientific advisory committee to the cabinet has adopted ERNET as the platform for launching R & D network in the country.

BEGINNING

ERNET was initiated in 1986 by the Department of Electronics (DoE), with funding support from the Government of India and United Nations Development Program (UNDP), involving eight premier institutions as participating agencies-NCST (National Centre for Software Technology) Bombay, IISc (Indian Institute of Science) Bangalore, five IITs (Indian Institutes of Technology) at Delhi, Bombay, Kanpur, Kharagpur and Madras, and the DoE, New Delhi. ERNET began as a multi protocol network with both the TCP/IP and the OSI-IP protocol stacks running over the leased-line portion of the backbone. Since 1995, however, almost all traffic is carried over TCP/IP.

FOCUS

ERNET is largest nationwide terrestrial and satellite network with point of presence located at the premiere educational and research institutions in major cities of the country. Focus of ERNET is not limited to just providing connectivity, but to meet the entire needs of the educational and research institutions by hosting and providing relevant information to their users. Research and Development and Training are integral parts of ERNET activities. The activities at ERNET India are organized around five technology focus areas:

- *National Academic and Research Network*
- *Research and Development in the area of Data Communication and its Application*
- *Human Resource Development in the area of High-end Networking*
- *Educational Content*
- *Campus-wide High Speed Local Area Network*

15.3.4 INFLIBNET

Information and Library Network (INFLIBNET), a programme of the University Grants Commission, was launched in May 1991. The main aim of INFLIBNET is to establish a national computer-communication network to link libraries and information centre's in universities, colleges, universities, UGC information centre's, institutions of national importance, R&D institutions, etc., and thereby improve capability in information handling and services. It is a programme for academic excellence to be achieved through establishment of a mechanism for information transfer and access to support scholarship and academic work. It facilitates pooling, sharing and optimization of scarce library resources in the country. As a major programme it helps modernize libraries and information centre's in the country through application of information technology.

The National Centre of INFLIBNET is located in Gujarat University campus at Ahmedabad. At present, INFLIBNET aims at computerizing and networking of university/college libraries. Every year, INFLIBNET programme is identifying a number of university libraries for automation depending on the budget allocation. The selected institutions are given funds for procuring computer systems, retro conversion and networking. Application software for data entry and other library functions, library standards and formats, etc., are provided by INFLIBNET to the participating libraries. Manpower development is an important part of the programme. Training courses for core library staff engaged in computerized library operations, have been conducted since 1992-93.

Development of suitable software, standards for various library operations and communication based services (e.g., e-mail, bulletin boards) designing suitable network architecture and preparation of union catalogues of serials, books, non-book materials, and cooperation with other networking organizations like NISSAT, NICNET, etc., are other important activities.

OBJECTIVES OF INFLIBNET

INFLIBNET is an autonomous institution and aims to provide a channel to the academicians and researchers for exchange of information from sources within the country and abroad.

- Modernize libraries/information centre's in India
- Mechanization for information transfer and access
- Facilitate pooling, sharing and optimization of library resources
- Organize library services at macro level
- Speedy and efficient services to end users
- Promoting equity

The ultimate aim is to provide the end-users a mechanism for sharing and using information resources and for exploiting modern information technology.

FUNCTIONS OF INFLIBNET

- Aims to establish a nation-wide network for computer communication linking academic libraries and information
- Aims to establish a mechanism for information transfer and access to support scholarship and academic work
- Aims to organize library services at macro levels at affordable cost and maximize benefits providing speedy and efficient services to end users.

• Will include participants from colleges, universities, R&D institutes, institutes of higher learning, information centre's, institutes of national importance and document resource centre's

• Covers all disciplines such as science, technology, medicine, agriculture, fine arts, humanities, social science

• Will provide networking to members using available communication infrastructure in the country.

15.3.5 SIRNET

The SIRNET (Scientific and Industrial Network) (SIRNET NET letter., 1990-), a project of INSDOC aims at networking all 40 CSIR laboratories under SIRNET was made operational in December 1989. At present, SIRNET provides electronic mail facility as its first application service from the SIRNET servers with a mail number of user nodes. For transmitting a message, a user have to deposit message to one of the SIRNET mail service nodes situated at the INSDOC, Delhi and at its regional centre at Bangalore from where it can be transmitted to its destination which may be any of CSIR laboratory presently linked to the mail node. The SIRNET, in turn, is connected to a large network-ERNET (Educational and Research Network) which is connected to the international network UUNET (Unix User Network) through which other international networks like BITNET, CSNET and JANET are accessible. The SIRNET's mail node at the INSDOC also acts as a gateway to ERNET and through ERNET to other networks. Connections between various laboratories of CSIR are established using dial-up telephone lines, while SIRNET is directly connected to DoE mail server VIKRAM which acts as the clearing node in Delhi ERNET.

15.3.6 BTISNET

The BTISNET (Biotechnology Information System Network) (Immunoinformatics New, 1990-) was established by the Department of Biotechnology at the national level to create and maintain databases and provide network services in six different areas of biotechnology involving 10 specialized centre's in 7 cities. The project aims to bridge the inter- disciplinary gaps on information and to establish link among scientists in organizations involved in R & D and manufacturing activities in biotechnology. These specialized centre's, designated as Distributed Information Centre's, are equipped with Micro VAX II for creation and maintenance of specialized databases in their respective area of specialization. The BTISNET is being installed using the NICNET communication infrastructure for connections amongst the 10 distributed centre's and 25 odd user's centre's. Most of the DICs and the user centers have already been networked through micro earth stations using X.25 protocols.

The user centre's provide access points for information available at the specialized centre's and also provide a mechanism to keep the databases up-to-date with the findings and results from their laboratories.

15.3.7 BONET

The Bombay Library Network (BONET) was setup at the National Centre for Software Technology (NCST), Bombay, on 6 November 1992. The Network is sponsored by NISSAT. The aim of BONET is to build a low cost library information system which can possibly be used as a model for future expansion of this service even outside Bombay.

BONET also benefits significantly from the experience gained, and facilities created, by the Education and Research Networking (ERNET) project of the Department of Electronics, Govt. of India, assisted by the United Nations Development Programme (UNDP). BONET is aimed at promoting cooperation between libraries in Bombay. The focus is on inter-library activities, rather than on computerizing individual libraries, which will no doubt computerize their own operations and are likely to share their experiences with each other. BONET offers training related to library computerization and networking, and speed up computerization of Bombay libraries. BONET membership provides for access to its centralized catalogues and for E-mail among BONET members. However, access to library related services outside Bombay in India and abroad would require use of ERNET.

The services offered through BONET include the following:

- Consultation on standards
- Organized training for selected staff of participating libraries
- On-line catalogue of periodicals for the region
- On-line catalogue of books for the region
- On-line catalogue of preprints/reprints
- Inter-library lending of books and periodicals
- Inter-library request for photocopying
- Computer network support for book ordering
- Information retrieval services
- On-line document delivery of items (such as technical reports) made available by participating libraries in machine readable form
- On-line access to foreign databases, subject to the user's willingness to pay the costs incurred
- E-mail interface for inter-library queries
- E-mail facilities to order reprints from abroad, when necessary
- Dissemination of information, on new books etc, using E-mail, Bulletin boards, and SDI techniques
- Courier service for inter-library exchange of materials

Under BONET the following databases were created:

- 25,000 items in a bibliographic database on computers and software technology
- Union catalogue of journals and other periodicals in libraries in the region
- Tables of contents of 250 Indian periodicals created by the national centre for information
- A number of CDROM databases have been mounted on a Novell Server for use to members.

15.3.8 ADINET

Ahmedabad Library Network (ADINET) was formally inaugurated in February 1995 when a memorandum of understanding was signed between NISSAT and ADINET at Ahmedabad. ADINET has ten institutional members, five associate institutional members and two professional members. A centralized database has been created at ADINET which contains institute master, journal master and book databases. It also organized six work and training programs. ADINET provided e-mail connectivity to 30 libraries of Ahmedabad.

15.3.9 PUNENET

Presently, 30 libraries and 15 professionals from Pune city are accessing the PUNENET through modem. The users not only access PUNENET data, but also use the e-mail and internet facilities. Following databases are available on PUNENET for its members:

- Catalogues of holding of all member libraries
- Union catalogue of current periodicals in Pune libraries and information centre's
- Publishers and book sellers database
- Database on international grants and fellowships in the health sciences
- Hard databanks in biotechnology

• Access to NICNET and databases available on NICNET e.g., MEDLANS,AIDS database, US patent database

• Access to internet and various databases available on internet

• Patent information

• Union catalogue of books available in British libraries in India

15.3.10 MALIBNET

The need for interconnecting libraries and information centre's in Madras was visualized in the Indian National Scientific Documentation Centre (INSDOC) in 1991. Initially six major academic institutions were directly linked to the MALIBNET host system. Two important databases have been created utilizing the resources available in Madras libraries. One is a Directory Database of Current Serials in Madras covering 30 libraries, and the other is a Contents Database covering articles published in 300 journals available in Madras libraries. Both these databases are continuously updated and also expanded. They are available for online- access to any user and the information is also supplied in diskettes and hard copy. Photocopies of articles from member libraries can be supplied within two days.

Madras has about 60 important libraries besides information centre's like INSDOC. About 15 of these libraries have a holding of well over 100,000 items. These libraries act as good resource centre's on the network. As of December 1993, all the 60 libraries together invest about Rupees 8,000,000 on acquiring journals and books every year. It is estimated that 40% of the information acquired is redundant. With the libraries networked and resource sharing implemented, each user on the network can get access to a vast amount of literature, and redundancy can be brought down significantly. A novel and unique feature of MALIBNET is that the members will be permitted to offer their own innovative information services on the network. A membership in MALIBNET is open to universities, colleges, R&D institutions, industries and individuals.

MALIBNET presently offers the following information services:

• Current serials acquired in about 60 libraries

• Full journal holdings of about 60 libraries

• Contents information of about 500 important journals

• Electronic mail including internet connectivity

• Door delivery system for document photocopies

• It also offers access to about 1000 international databases

15.2.11 MYLIBNET

It is the first library network established in a small city. The launching of MYLIBNET in association with Mysore city library consortium (MCLC) took place on 12th June 1995. There are 16 institutional members. The holding list of Mysore city libraries has been computerized and software has been developed to enable users to access the catalogue and information on-line. MYLIBNET provides e-mail facilities to its members.

CONCLUSION

Following the launching of DELNET and CALIBNET, the library automation and networking movement in India is surely catching on. The objectives which are:

• Better utilization of funds through sharing of resources by creation of commonly usable data-bases and communication between libraries.

• Automating the functions of individual libraries at a local level for effective and efficient services to the users.

A number of benefits are being offered to member libraries of the particular networks. First, one gets access to a very large volume of literature without increase in the library budget because of the sharing of resources among the members. Secondly, the library budget can now be diverted to acquire the most important (even if expensive) information required by an institution, the other peripheral information being available on the network. Third, one gets near real time access to about 1000 international databases apart from the electronic mail and remote log in facilities. There are plans of these networks to connect and share the resources in the near future.

Nevertheless, the growth of these networks is slow. It is taking a long time to create and provide bibliographic databases of recognizable size, e.g., DELNET took already ten years in creating bibliographic databases of reasonably good size. Without the databases neither could networks be made effective to achieve the goals nor could resource sharing be effective.

Finally it appears that prospects are quite favorable for development of networks for better information services and resource sharing in India. In this direction lot of work has to be done. Some of the problems faced by other developing countries are common to India too, including financial constraints, inadequate communication, non-availability of equipments, less awareness of the value of information, reluctance to development and non-coordination of various kind of activities, resource building, resource sharing and exchange of information and ideas, non-standardization operational procedure, lack of dedication, motivation and knowledge on the part of available manpower.

15.4 Researchs in India

15.4.1 MYFIRE

The MyFIRE project is a part of FIRE - Future Internet Research and Experimentation, an initiative from the European Commission to address the need for early experimentation and testing in large scale environments for the construction of the Future Internet. MyFIRE project aims to develop the use of experimental facilities in Europe in particular by increasing awareness of testing related best practices. The project will ensure a balance between the requirements for researcher's collaboration and the stakeholder's expectations. MyFIRE project has eight consortium members which include four European partners and four partners from BRIC (Brazil, Russian, India and China) countries. The following are the consortium members of MyFIRE.

15.4.2 EU-IndiaGrid2 - Sustainable e-Infrastructures across Europe and India

EU-IndiaGrid2 is the second phase of the EU-IndiaGrid project, which was funded initially by the European Commission for two years starting from October, 2006.

The objective of EU-IndiaGrid was to:

• Support the interconnection and interoperability of the prominent European Grid infrastructure (EGEE) with the Indian Grid infrastructure(GARUDA) for the benefit of eScience applications

• Identify and aggregate research, scientific and industrial communities which may benefit from the use of Grid technology resulting in an eScience Network Community

• Promote the use of advanced Grid technologies within the created Network Community relying on pilot applications in Biology, High Energy and Condensed Matter Physics and specific outreach and dissemination activities

• Disseminate European EGEE Grid technology achievements in India and leverage on Indian Grid experiences and skills

This consortium project comprising of 5 European partners and 8 Indian partners was successfully completed. ERNET India's role in the project was to provide network level interconnection between Indian

grid GARUDA and European grid EGEE using ERNET-GEANT connectivity and to maintain the network connectivity between India and Europe. The project EU-InidaGrid2 proposes to capitalize on the achievements of the first phase of EU-IndiaGrid project and to make use of the momentum attained in e-Infrastructure evolution in Europe and India aiming at proceeding towards sustainable e-Infrastructures across Europe and India for the benefit of scientific, educational and technological cooperation across the two continents.

Specifically, EU-IndiaGrid2's main objectives are to:

• Enhance and increase the cooperation between European and Indian e-Infrastructures for the benefit of EU-Indian collaboration in e-Science.

• Support specific user communities in the exploitation of grid infrastructure in areas strategic for EU-Indian collaboration.

• Ensure a sustainable approach to e-Infrastructures across Europe and India through dissemination actions, meetings and workshops.

• Foster and enhance cooperation with other European Initiatives in the Asian region and worldwide.

This two year project was initiated with a kick-off meeting in January, 2010 at New Delhi. There are six European partners and 10 Indian partners in this new project. The role of ERNET India in the new project is to provide network infrastructure support using ERNET-GEANT link and subsequently provide network infrastructure support using TEIN3.

15.4.3 IPV6 Based Monitoring and Management of Wireless sensor Networks

6LoWPAN is a joint project between ERNET India and IISc Bangalore, funded by Department of Information Technology for duration of 24 months from January 2010. IEEE 802.15.4 Low-rate Wireless Personal Area Network (LoWPAN) standard supports wireless connectivity in low-cost devices that operate with limited battery power. LoWPAN networks enable emerging application functions such as agricultural field measurements, monitoring structural health of buildings, patient health monitoring and home/industrial automation. The support for IPv6 over 802.15.4 links enables integration of LoWPANs into the existing IP infrastructure. Also, the large IPv6 address space will meet the requirements of numerous LoWPAN nodes with address assignment using auto-configuration protocols. The 6LoWPAN layer performs header compression, fragmentation and layer 2 forwarding functions to adapt IPv6 packets to the resource constrained LoWPAN networks.

The objective of this project is to develop a prototype for monitoring and managing a 6LoWPAN based Wireless Sensor Network (WSN). Internet open standards such as SNMP will be utilized to build the management and monitoring framework. Considering the wide ranging WSN applications, it is proposed to develop a generic modular framework that is extensible with application-specific monitorable parameters. It will be demonstrated with an experimental test bed at IISc and an operational test bed at ERNET India. Monitoring applications in the field of agriculture and healthcare will be demonstrated.

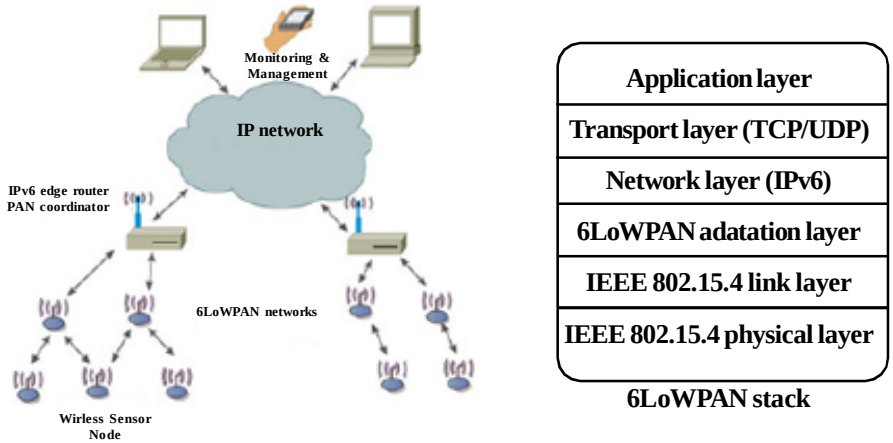


Figure15.1 : 6LoWPAN - Enabling IPv6 over Low-power Wireless Sensor Devices

15.4.4 MOBILE IPV6

Mobile IPv6 Testbed for Mobility management over heterogeneous access networks. Mobile IPv6 test bed is a joint project between ERNET India and Indian Institute of Science (IISc) Bangalore which is funded by Department of Information Technology. The main purpose of the project is to deploy Mobile IPv6 testbed to study network layer mobility management issues over heterogeneous access networks. The project activities include design and simulation of relevant mobility scenarios both independently and in hybrid network simulation model, evaluation of IPv6 mobility over heterogeneous access networks to study performance parameters such as handover latency, packet loss in different scenarios. A Testbed comprising of WiMAX, WiFi and cellular networks will be deployed and the mobility scenarios will be tested on real testbed. In the presence of ERNET's IPv6/IPv4 dual stack routers both in core and edge network, mobility between IPv4 and IPv6 network will be tested to demonstrate interoperability.

IEEE 802.21 standard provides link-layer intelligence and other related network information to upper layers to optimize handovers between heterogeneous networks. It optimizes handover between heterogeneous IEEE 802 networks and facilitates handover between IEEE 802 networks and cellular networks. Suitable IEEE 802.21 Media Independent Handover services that define generic link layer interface to support higher layer mobility will be developed. The project will study specific fast handover strategies and implement the required algorithms. By using select applications from domains such as agriculture, healthcare and e-learning, Mobile IPv6 test bed capabilities will be demonstrated.

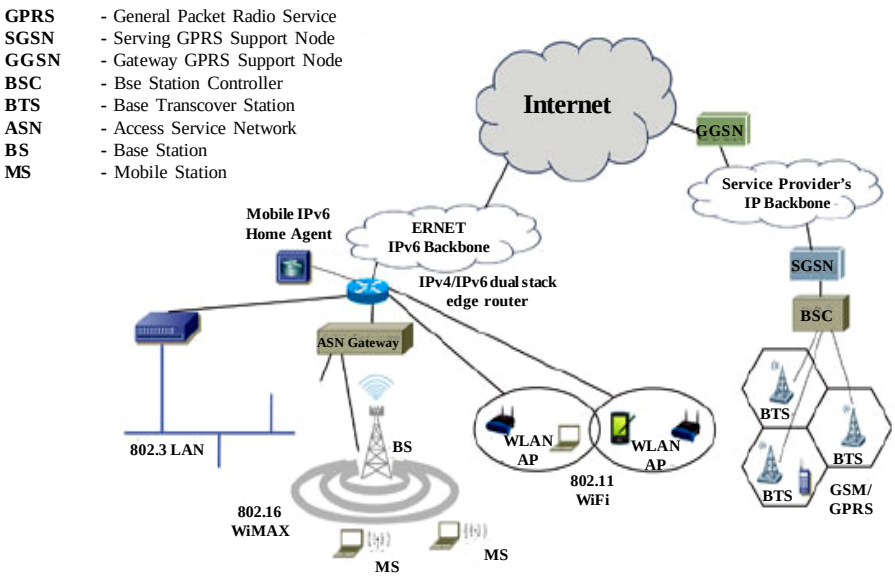


Figure 15.2 : Mobile IPv6 Test bed Infrastructure

15.4.5 National QOS Test Bed

The Department of Information Technology (DIT) has funded a project for establishing a nationwide IP based QoS network to address the growing trends of the knowledge based society to provide all resources (educational, professional, social and commercial) and Internet enabled services to the users. ERNET India in association with premier institutions including IITs, IISc, and CDAC initiated the project. Each institution has been assigned different role for development and experiment of QoS aware applications and share their expertise in the area of networking technologies. To test and experiment the concept of QoS, applications like IP Telephony and Video Conferencing for distance learning / e-Learning have been chosen.

ERNET India has setup QoS enabled network testbed among institutions with 2Mbps link from its backbone. All participating institutions are fine-tuning the network architecture and network engineering processes to lead to best practices for QoS assured network and its services. The participating institutions are linked to each other with Label Switch Paths (LSPs) for carrying out the experiments and studies on the testbed. ERNET India has also deployed MPLS on its backbone to ensure better control on bandwidth for delivering services and the project has been successfully completed.

15.4.6 Network Monitoring Tool

Internet has seen exponential growth in the last decade. It has become a preferred medium for exchange of information across the world. Effectiveness of communication over Internet has also attracted criminal elements in using this for cyber crime. With the increase of usage of Internet and cyber crime, the need to monitor the traffic especially against unwanted content also increased with time. The Internet is used by anti-social elements as a tool against legitimate usage of Internet.

Network Monitoring Tool (NMT) has been developed by ERNET India and IIT Kanpur for monitoring the illegal and unauthorized communication leading to cyber crime over Internet. The NMT will be used to collect specific information from Internet and reconstruct the same into a readable format. The data collected can be used by the investigating agencies for the purpose of evidence collection against any unlawful activities over Internet.

The tool operates in a non-intrusive manner and is capable of monitoring all packets passing through a link without injecting any data into the network. It captures information based on source/destination IP addresses, port numbers, login IDs, e-mails headers like - subject of messages, e-mail address, URLs, and text string etc.

The focus area of the research was to investigate the Internet packet capturing, filtering algorithms, encoding of packets, data communication through serial port for secure and dedicated remote control and performance measurement etc.

NMT was deployed and tested at ERNET POP and handed over to CBI for field trials. Capabilities of NMT were presented to a delegation from Cabinet Secretariat and senior DIT officials. Members showed interest in the product and the capabilities developed in the process.

15.5 Social Implementation of Telemetric Society

Telemetry is a technology that allows data measurements to be made at a distance.

The 'Telemetry' means measurement at a distance (tele + metery). The term involves conversion of a quantity into a suitable signal, the transmission of that suitable signal over a proper channel and its recon version into a display which may be recorded or viewed graphically or may be stored.

The telemetry system can be classified.

- According to characteristic of the signal i.e. voltage, current frequency, pulse.
- According to analog and digital signal.
- According to the physical connection between transmitter and receiver i.e. 'channel' which may consists of 2, 3 or 4 wires.
- According to other channels such as telegraph, telephone, radio, microwave etc.

A general electrical telemetry system is shown in fig. 15.3. It has three basic components

(i) Transmitter

(ii) Receiver

(iii) The channel interconnecting the above two

The quantity to be measured called (measurand) is detected and the output electrical signal is transmitted through the channel At receiving end the electrical signal is received and converted back into usable form as indicated, recorded or displayed by the end device.

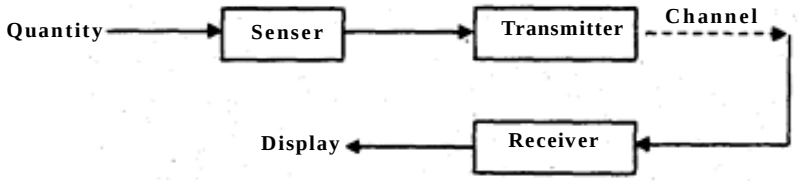


Figure 15.3 : General Electrical Telemetry System

Telematics typically is any integrated use of telecommunications and informatics, also known as ICT (Information and Communications Technology). Hence the application of telematics is with any of the following:

• The technology of sending, receiving and storing information via telecommunication devices in conjunction with affecting control on remote objects.

• The integrated use of telecommunications and informatics, for application in vehicles and with control of vehicles on the move.

• Telematics includes but is not limited to Global Positioning System technology integrated with computers and mobile communications technology in automotive navigation systems.

• Most narrowly, the term has evolved to refer to the use of such systems within road vehicles, in which case the term vehicle telematics may be used.

In contrast telemetry is the transmission of measurements from the location of origin to the location of computing and consumption, especially without effecting control on the remote objects. Telemetry is typically applied in testing of flight objects but has multiple other uses.

15.6 Summary

• The progress in networking in India has been rather slow due to the poor extension of telecommunication networks and overwhelming use of resources and expertise that are available. However, the scene is changing fast.

• Networks are classified into the following two categories depending upon their scope and objectives:

A) General networks (i.e., NICNET, INDONET and VIKRAM)

B) Specialized networks (i.e., CALIBNET, DELNET, BONET, ERNET, INFLIBNET, BTISNET etc.)

• National Informatics Centre (NIC) is a leading organization in the field of Information Technology (IT) in India. It provides state of the art solutions to the information management and decision support requirements of the Government and the corporate sector.

• The INDONET aims to provide facility for distributed data processing on all India bases to large organizations in the network using the CMC computers for their data processing operations.

• Vikram is the packet switched public data network under development by the Department of Telecommunications.

• Now a large number of library resource sharing networks like the Metropolitan Area Networks, such as CALIBNET (Calcutta), DELNET (Delhi), BONET (Bombay), PUNENET (Pune), MALIBNET (Madras), MYLIBNET (Mysore), HYLIBNET (Hyderabad), ADNET (Ahmedabad).

• Countrywide ones like ERNET (Educational and Research Institutions), SIRNET (CSIR Laboratories), INFLIBNET (Universities and Research Institutions) and DESINET (Defense Laboratories), and sectoral ones like BTISNET (Biotechnology).

• RESEARCHES IN INDIA with collaboration to other Countries are

- MyFire
- EU-IndiaGrid2 - Sustainable e-Infrastructures across Europe and India
- IPV6 BASED MONITORING AND MANAGEMENT OF WIRELESS SENSOR NETWORKS
- MOBILE IPV6
- NATIONAL QOS TEST BED
- NETWORK MONITORING TOOL

• Telemetry is a technology that allows data measurements to be made at a distance

15.7 Self Assessment Questions

1. Classify Indian Networks?
2. Explain different types of Metropolitian Area Networks(MAN) with reference to CALIBNET and DELNET in Detail?
3. Explain different types of country wide networks? Mainly focus on ERNET, INFLIBNET?
4. Write short notes on

   a) SIRNET

   b) BTISNET

   c) BONET

   d) MALIBNET
5. Give a brief description on Researches in India?
6. What is Telemetry and explain its Applications?

15.8 References

1. "ERNET" India Network Foundation www.indianetwork.org/