

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/288180515>

# DATA COMMUNICATION & NETWORKING

Book · November 2015

CITATIONS

0

READS

225,131

1 author:



**Yekini Nureni**

Yaba College of Technology

60 PUBLICATIONS 111 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



NETWORK SECURITY [View project](#)



E-Learning [View project](#)

All content following this page was uploaded by Yekini Nureni on 26 December 2015.

The user has requested enhancement of the downloaded file.

# **DATA COMMUNICATION & NETWORKING**

**YEKINI N. ASAFE  
ADEBARI F. ADEBAYO  
BELLO OLALEKAN**

**Computer Engineering Department  
Yaba College of Technology  
Lagos Nigeria**

## **Copyright**

**Copyright © 2015 by YEKINI N. ASAFE, ADEBARI F. ADEBAYO, and BELLO OLALEKAN**

**Typesetting @ YEKNUA ICT & Educational Research-Publication Centre No 07, Christ Possibility Street, Sango-Ota,  
Ogun State, Nigeria.**

**Tel: 234-8037274683, 08094204341**

**All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright holder.**

**ISBN:**

**Published In Nigeria**

## Table of Figures

<i>Figure 1: Typical Analog signal</i>	14
<i>Figure 2: Typical Digital Signal</i>	15
<i>Figure 3: Basic Block Diagram of a Data Communication System</i>	17
<i>Figure 4: Data communication and terminal equipment</i>	20
<i>Figure 5: Personal Area Network</i>	30
<i>Figure 6: Local Area Network</i>	31
<i>Figure 7: Metropolitan area Network</i>	32
<i>Figure 8: Wide Area Network</i>	33
<i>Figure 9: Network Topology categories</i>	34
<i>Figure 10: Bus Topology</i>	35
<i>Figure 11: Bus Topology with three stations</i>	37
<i>Figure 12: Ring Topology</i>	38
<i>Figure 13: Star Topology</i>	40
<i>Figure 14: Mesh topology</i>	42
<i>Figure 15: Hybrid Network</i>	44
<i>Figure 16: Data Transmission Mode</i>	65
<i>Figure 17: Data Transmission</i>	66
<i>Figure 18: Parallel transmission</i>	67
<i>Figure 19: Serial Transmission</i>	68
<i>Figure 20: Synchronous Transmission</i>	68
<i>Figure 21: Asynchronous Transmission</i>	69
<i>Figure 22: Open wire Media</i>	74
<i>Figure 23: Twisted Pair Cables</i>	76
<i>Figure 24: Coaxial Cable</i>	77
<i>Figure 25: Step Index Mode</i>	79
<i>Figure 26: Grade Index Mode</i>	80
<i>Figure 27: Single Mode</i>	80
<i>Figure 28: Ground wave Propagation</i>	81
<i>Figure 29: Sky Wave Propagation</i>	82
<i>Figure 30: Line of sight Propagation</i>	83
<i>Figure 31: effect of attenuation and amplification.</i>	86
<i>Figure 32: Crosstalk impairment</i>	86

<b>Figure 33: Cryptographic Algorithms</b>	95
<b>Figure 34: hybrid cryptographic scheme</b>	100
<b>Figure 35: Analog vs analog representation</b>	105
<b>Figure 36: Analog vs Digital Signal</b>	106
<b>Figure 37: A sine wave</b>	107
<b>Figure 38: Two signals with the same phase and frequency, but different amplitudes</b>	108
<b>Figure 39: 2 signals with the same phase and frequency, but different frequencies</b>	109
<b>Figure 40: 3 sine waves with the same amplitude and frequency, but different phases</b>	110
<b>Figure 41: The time-domain and frequency-domain plots of a sine wave</b>	112
<b>Figure 42: solution for the above</b>	114
<b>Figure 43: Two digital signals: one with two signal levels and the other with four signal levels</b>	115
<b>Figure 44: Line coding and decoding</b>	117
<b>Figure 45: Types of Line Coding</b>	118
<b>Figure 46: Unipolar NRZ</b>	118
<b>Figure 47: Polar Coding</b>	119
<b>Figure 48: Polar RZ type coding</b>	120
<b>Figure 49: Manchester and differential Manchester Coding</b>	121
<b>Figure 50: Bipolar Scheme</b>	123
<b>Figure 51: Multilevel: 2B1Q scheme</b>	124
<b>Figure 52: 9.2.5. Multiline Transmission ML-3</b>	126
<b>Figure 53: Block coding</b>	127
<b>Figure 54: AMI used with scrambling</b>	128
<b>Figure 55: Digital-to-analog conversion</b>	129
<b>Figure 56: Types of digital-to-analog conversion</b>	130
<b>Figure 57: Binary amplitude shift keying</b>	132
<b>Figure 58: Implementation of binary ASK</b>	132
<b>Figure 59: Binary frequency shift keying</b>	133
<b>Figure 60: Implementation of BFSK</b>	135
<b>Figure 61: Binary phase shift keying</b>	136
<b>Figure 62: QPSK and its implementation:</b>	137

<b>Figure 63: Concept of a constellation diagram</b>	<b>138</b>
<b>Figure 64: Categories of multiplexing</b>	<b>141</b>
<b>Figure 65: Frequency Division Multiplexing</b>	<b>142</b>
<b>Figure 66: Time Division Multiplexing</b>	<b>143</b>
<b>Figure 67: Wavelength Division Multiplexing</b>	<b>143</b>
<b>Figure 68: Switching Hub Operation</b>	<b>147</b>
<b>Figure 69: Internal Cable Structure and Color Coding</b>	<b>150</b>
<b>Figure 70: Modular Connector Plug and Jack Pin Out</b>	<b>152</b>
<b>Figure 71: Usual network topology</b>	<b>158</b>
<b>Figure 72: Direct connection of two computers</b>	<b>159</b>
<b>Figure 73: Control Panel Window</b>	<b>160</b>
<b>Figure 74: Network and Sharing Center window</b>	<b>160</b>
<b>Figure 75: Network Connections window</b>	<b>161</b>
<b>Figure 76: Network Connection Properties window</b>	<b>162</b>
<b>Figure 77: TCP/IPv4 window</b>	<b>163</b>
<b>Figure 78: IP Assigned by DHCP server</b>	<b>164</b>
<b>Figure 79: Using alternate configuration</b>	<b>165</b>
<b>Figure 80: Physical Network Setup with D-Link's DI-604 broadband router</b>	<b>167</b>
<b>Figure 81: A typical home wired network</b>	<b>173</b>
<b>Figure 82: Command Prompt window for nslookup</b>	<b>177</b>

## Table of Contents

Cover page	-----i
Copyright	-----ii
Table of figures	-----iii-v
Contents	-----vi-ix
Preface	-----x
Acknowledgements	-----xi
Ownership	-----xii

### **CHAPTER ONE -----013-023**

#### **DATA COMMUNICATION CONCEPTS**

- 1.1. Description of Data Communication
- 1.2. Analog and Digital Signal
- 1.3. Why Data Communication?
- 1.4. Components of Data Communication
- 1.5. Data Communication Criteria
- 1.6. Data Communication And Terminal Equipment
- 1.7. Data Representation
- 1.8. Review Questions

### **CHAPTER TWO-----024-046**

#### **COMPUTER NETWORKING CONCEPTS**

- 2.1. What is Computer Network?
- 2.2. Why computer networking
- 2.3. Protocol and Standards in Networking
- 2.4. Types of Network
- 2.5. Network Topologies
- 2.6. Review Questions

### **CHAPTER THREE-----047-055**

#### **COMPUTER NETWORK MODELS**

- 3.1. Description of Network Model

- 3.2. Network Model Layers
- 3.3. Review Questions

**CHAPTER FOUR-----056-063**

**DATA COMMUNICATION SOFTWARE AND PROTOCOL**

- 4.1. Data Communication Software
- 4.2. Communication Protocol
- 4.3. Review Questions

**CHAPTER FIVE-----064-069**

**TRANSMISSION MODES**

- 5.1. Description of Data Flows and Transmission Mod
- 5.2. Types of Transmission Mode and Data Flow
- 5.3. Digital Data Transmission Meth
- 5.4. Review Questions

**CHAPTER SIX-----070-088**

**DATA TRANSMISSION AND NETWORK CONNECTION MEDIA**

- 6.1. Definition of Data Transmission Media
- 6.2. Transmission Channel Parameters
- 6.3. Guided Transmission Media
- 6.4. Unguided Transmission Media (Wireless Transmission Medium)
- 6.5. Transmission Media Problems and Impairment
- 6.6. Review Questions

**CHAPTER SEVEN-----089-104**

**COMPUTER NETWORK SECURITY**

- 7.1. Description of Network Security Treat
- 7.2. Security Requirements and Attacks
- 7.3. Network Security Threats Prevention
- 7.4. Review Questions



<b>CHAPTER EIGHT-----</b>	<b>105-116</b>
<b>ANALOG VS DIGITAL TRANSMISSION</b>	
8.1. Analog and Digital Data	
8.2. Analog and Digital Signals	
8.3. Periodic Analog Signals	
8.4. Digital Signals	
8.5. Review Questions	
 <b>CHAPTER NINE-----</b>	 <b>117-128</b>
<b>DIGITAL DATA TO DIGITAL SIGNAL CONVERSION</b>	
9.1. Digital Signal Representation	
9.2. Line Coding	
9.3. Block Coding	
9.4. Scrambling	
9.5. Review Questions	
 <b>CHAPTER TEN-----</b>	 <b>129-139</b>
<b>DIGITAL-TO-ANALOG CONVERSION USING MODULATION TECHNIQUES</b>	
10.1. DIGITAL-TO-ANALOG CONVERSION	
10.2. What is Modulation Techniques?	
10.3. Types of Modulation	
10.4. Constellation Diagram	
10.5. Review Questions	
 <b>CHAPTER ELEVEN-----</b>	 <b>140-145</b>
<b>MULTIPLEXING</b>	
11.1. Definition of Multiplexing	
11.2. Types of Multiplexing Techniques	
11.3. Review Question	
 <b>CHAPTER TWELVE-----</b>	 <b>146-156</b>
<b>NETWORK IMPLEMENTATION DEVICES</b>	
12.1. Network Implementation Devices	

12.2. Cabling and Network Setup  
12.3. Network Card Configuration  
12.4. Review Questions

**CHAPTER THIRTEEN-----157-169**  
**NETWORK SET-UP & CONFIGURATION**  
**(PHYSICAL HOME LAN)**

13.1. Building Home Network  
13.2. Direct Connection of Two Computers  
13.3. Configuring of IP Address and Other Network  
Information in On Windows 7  
13.4. Physical Network Setup  
13.5. IP Logical Network Design  
13.6. Review Questions

**CHAPTER FOURTEEN-----170-179**  
**NETWORKING TROUBLESHOOTING**

14.1. Networking Troubleshooting Steps  
14.2. Ways to check if a website is down  
14.3. Troubleshoot Network Problem With “ping” Command  
14.4. nslookup  
14.5. Review Questions

Bibliography ----- 180  
Index -----

## **Preface**

The objective of this book is to introduce students of computer engineering, computer sciences and pure and applied sciences to basic concepts, principles, and practice of data communication and network.

This book introduces the basic principles, theories and practical of data communication and networking for polytechnics and colleges of technology in line with current national board for technical education curriculum (NBTE).

The book will be very useful for the readers of different categories as in undergraduate students of university, polytechnics, colleges of education and allied institutions in areas of computer Sciences and engineering, and other related disciplines.

There is no doubt that this book will be very useful to all categories of readers.

## **Acknowledgements**

**First of all we are very grateful to God almighty for his mercy and wisdom bestow on us to write this book. This book evolved from our experiences in teaching and research in engineering.**

**There are some people that contributed to the success of the research that gave birth to this book. We acknowledged all staff of Department of Computer, electrical and electronics engineering for their support.**

**We acknowledge the contribution of the management of Yaba College of Technology for providing enabling environment for research and publication in the college.**

**We also acknowledge the contribution of our students from the department of computer, electrical and electronics engineering.**

**Thank you all.**

**This Book Belongs To**

**NAME:** -----

**SCHOOL:** -----

**DEPARTMENT:** -----

**SIGNATURE:** -----

**DATE:** -----

# CHAPTER ONE

## DATA COMMUNICATION CONCEPTS

### 1.1. Description of Data Communication

Communication can be defined as the exchange of information between two or more bodies. In engineering, exchange of information is not only between people, information exchange also takes place between machines or systems. Communication has increased significantly in importance in recent years. Voice services have seen unprecedented increase in use throughout the world with the introduction of mobile phones, with embedded data services such as SMS, and web browsing.

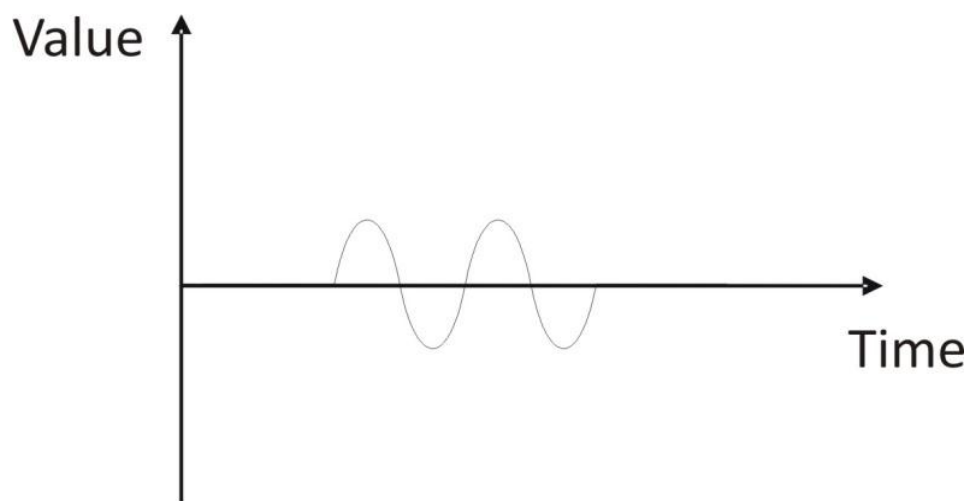
Data is referred to as a piece of information formatted in a special way. Data can exist in a variety of forms, such as numbers or text on pieces of paper, as bits and bytes stored in electronic memory, or as facts stored in a person's mind. Strictly speaking, data is the plural of *datum*, a single piece of information. In practice, however, people use *data* as both the singular and plural form of the word. In electronics terms data is a digital bit or digitized analog signal. Signals are physical quantity that changes with time.

Signal can be a voltage that is proportional to the amplitude of message. It could also be a sequence of pulses in fiber optics cable or electromagnetic wave irradiated by an antenna. When these signals are transfer between two or more points we say data is transmitted. Transmission of data from source

to destination usually takes place via some transmission media and this depends on two main factors; quality of signal being transmitted and characteristics of transmission medium. Data transmission always uses the form of electromagnetic waves and they are classified into guided electromagnetic waves and unguided electromagnetic waves. Examples of guided waves are twisted pair, coaxial cable and optical fiber. Unguided waves means transmitting electromagnetic waves but they are not guided as example propagation through air, vacuum and seawater.

## 1.2. Analog and Digital Signal

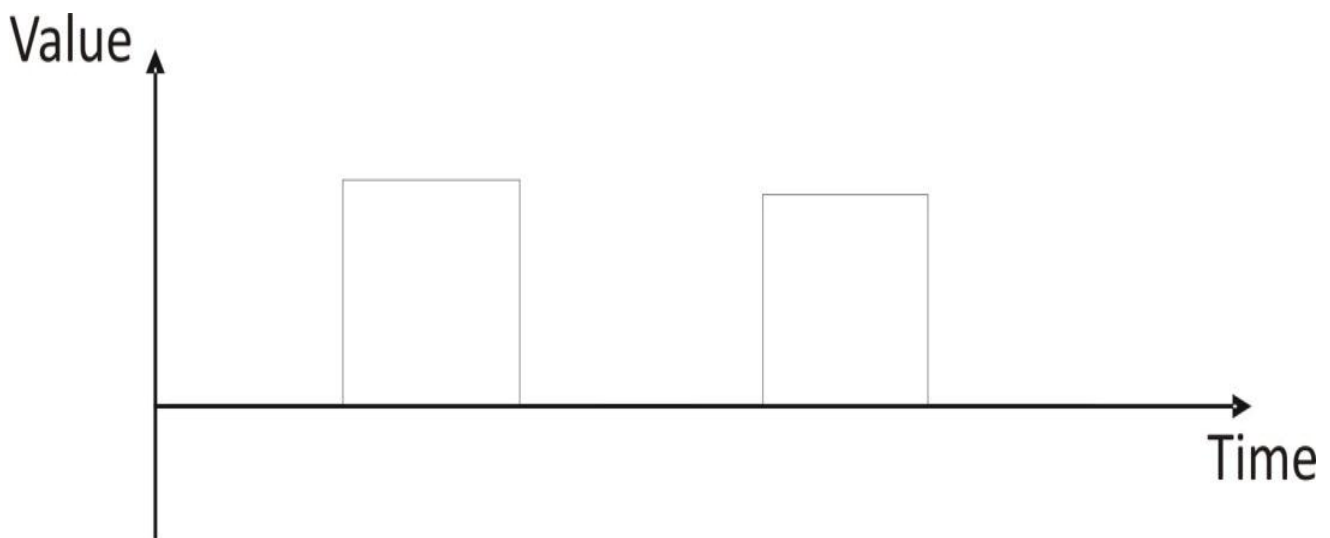
The entire world is full of signals, both natural and artificial. Signals can be analog or digital. Figure 1 illustrates an analog signal. The term analog signal refers to signal that is continuous and takes continuous value. Most phenomenon's in the world today are analog. There are an infinite amount of colours to paint an object (even if the difference is indiscernible to the eye), it is possible for us to hear different sounds and also smell different odours. The common theme among all of these analog signals is their infinite possibilities.



**Figure 1: Typical Analog signal**

Figure 1 shows a typical representation of analog signal. Because the signal varies with time, time is plotted on horizontal (x-axis), and voltage on the vertical (y-axis). While this signals may be limited to a range of maximum and minimum values. There are still an infinite number of possible values within that range. For example the analog voltage that light the bulbs is clamped between -220V and +220V, but as you increase the resolution more and more, you discover an infinite number of values that the signal can be. For example, pure audio signals are analog. The signal that comes out of a microphone is full of analog frequencies and harmonics, which combine to beautiful music.

A digital signal is a physical signal that is a representation of a sequence of discrete values. The signal must have a finite set of possible values, the number of set which can be anywhere between two and very large number that is not infinity. Digital signal is one of two voltage value (0V or 5V) timing graphs of these signals look like square waves as shown in figure 2.



**Figure 2: Typical Digital Signal**



### **1.3 Why Data Communication?**

Data communication refers to the movement of encoded information from one point to another by means of electronic transmission system. It can also be defined as the exchange of data between two devices via some form of transmission medium which can be wired or wireless. Another definition for data communications simply mean the transferring of digital information (usually in binary form) between two or more points (terminals). At both the source and destination, data are in digital form; however, during transmission, they can be in digital or analog form. Information is carried by signal, which is a physical quantity that changes with time. The signal can be a voltage proportional to the amplitude of the voice like in simple telephone, a sequence of pulses of light in an optical fiber, or a radio-electric wave radiated by an antenna.

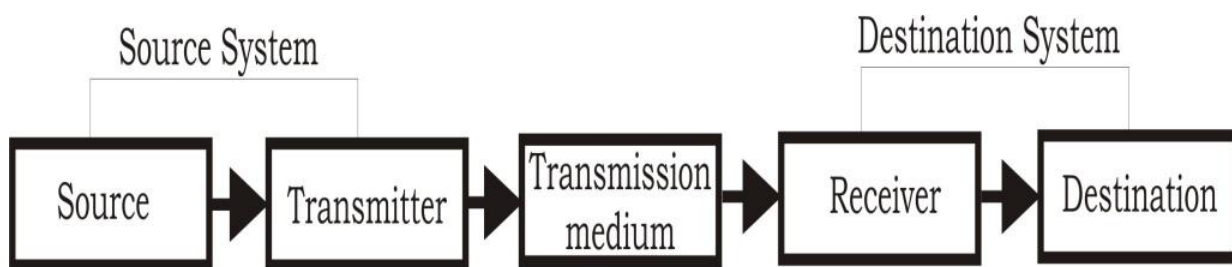
The fundamental purpose of data communication is to exchange information which is done by following certain rules and regulations called protocols and standards. Communications between devices are justified for the following reasons:

- i. Reduces time and effort required to perform business task
- ii. Captures business data at its source
- iii. Centralizes control over business data
- iv. Effect rapid dissemination of information
- v. Reduces current and future cost of doing business
- vi. Supports expansion of business capacity at reasonably incremental cost as the organization
- vii. Supports organization's objective in centralizing computer system
- viii. Supports improved management control of an organization.

As a rule, the maximum permissible transmission rate of a message is directly proportional to signal power and inversely proportional to channel noise. It is the aim of any communications system to provide the highest possible transmission rate at the lowest possible power and with the least possible noise.

#### 1.4. Components of Data Communication

Basic Components of data communication are: **Source:** It is the transmitter of data. Examples are: Terminal, Computer, Mainframe etc. **Medium:** The communications stream through which the data is being transmitted. Examples are: Cabling, Microwave, Fiber optics, Radio Frequencies (RF), Infrared Wireless etc. **Receiver:** The receiver of the data transmitted. Examples are: Printer, Terminal, Mainframe, and Computer.



**Figure 3: Basic Block Diagram of a Data Communication System**

Figure 3 shows the basic block diagram of a typical data communication system. This can further be broken down to three; the source system, transmission system and destination system.

##### 1.4.1 Source

The source generates the information or data that will be transmitted to the destination. Popular forms of information include text, numbers, pictures, audio, video or a combination

of any of these. Information are put together in analog or digital form and broken into group or segment of data called packets. Each packet consists of the following:

- i. the actual data being sent
- ii. header
- iii. information about the type of data
- iv. where the data came from
- v. where it is going, and
- vi. How it should be reassembled so the message is clear and in order when it arrives at the destination.

#### **1.4.2 Transmitter**

The transmitter a device used to convert the data as per the destination requirement. For example a modem, converts the analog (telephonic) signal to digital (computer) signals and alternatively digital to analog.

#### **1.4.3 Transmission medium**

The transmission medium is the physical path by which data travels from transmitter to receiver. Example of such channels is copper wires, optical fibers and wireless communication channels etc.

#### **1.4.4 Receiver**

This receives the signals from the transmission medium and converts it into a form that is suitable to the destination device. For example, a modem accepts analog signal from a transmission channel and transforms it into digital bit stream which is acceptable by computer system.

#### **1.4.5 Destination**

It is simply a device for which source device sends the data.

### **1.5. Data Communication Criteria**

The effectiveness of data communications system depends on four fundamental characteristics:

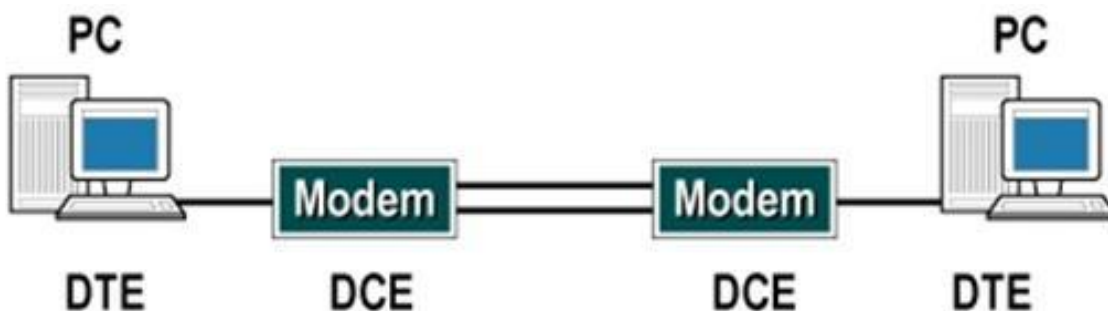
1. **Delivery.** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy.** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness.** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission and this occurs in a *real-time* system.
4. **Jitter.** Jitter refers to the variation in the packet arrival time. It is the uneven delay of delivery of audio or video packets. For example, let us assume that video packets are sent every 20ms. If some of the packets arrive with 20ms delay and others with 30ms delay, an uneven quality in the video is the result.

### **1.6. Data Communication And Terminal Equipment**

Communication facilities have an ancient history, but we tend to think of the advent of the telegraph and later the telephone as the beginning of modern communications. Extensive telegraph and telephone networks were established all over the world, decades before the emergence of computers. Data communication equipment (DCE) is the hardware devices that can be used to establish, maintain and terminate communication between a data source and its destination. Data communications equipment is most used to perform signal exchange, coding and line clocking tasks as part of intermediate equipment or DTE. A typical example of data communication equipment is the modem.

Data terminal equipment (DTE) refers to the interface equipment which is source or destination in communication. The terminal equipment is capable of converting information to signals and also reconverts received signals. Data terminal equipment does communicate directly with each other. Communication between them is done by data communication equipment. Popular examples of data terminal equipment are computers, printers, routers, servers etc.

Data communication equipment and data terminal equipment are often confused with each other. In fact the confusion is more pronounced when data communication equipment are embedded in some data terminal equipment. The truth is that when the two are separated they are interlinked. Also, data terminal equipment and data communication connectors are wired differently if a single straight cable is employed. Data communication equipment generates internal clock signals, while data terminal equipment works with externally provided signals. Figure 4 shows a typical arrangement of data communication and terminal equipment.



**Figure 4: Data communication and terminal equipment**

### **1.7. Data Representation**

Data representation is defined as the methods used to represent information in computers. Different types of data can be stored in the computer system. This includes numeric data, text, executable files, images, audio, video, etc. all

these will look different to us as human. However, all types of information or data stored in the computer are represented as a sequence of 0s and 1s.

### **Decimal Numbers**

As human we are used to writing numbers using digits 0 to 9. This is called base 10. This number system has been widely adopted, in large part because we have 10 fingers. However, other number systems still persist in modern society.

### **Binary Numbers**

Any positive integer (whole number) can be represented by a sequence of 0s and 1s. Numbers in this form are said to be in base two, and are called binary numbers. Computers are based on the binary (base 2) number system because electrical wire can only be of two states (on or off).

### **Hexadecimal Numbers**

Writing numbers in binary is tedious since this representation uses between 3 to 4 times as many digits as the decimal representation. The hexadecimal (base 16) number system is often used as shorthand for binary. Base 16 is useful because 16 is a power of 2, and numbers have roughly as many digits as in the corresponding decimal representation. Another name for hexadecimal numbers is alphadecimal because the numbers are written from 0 to 9 and A to F. where A is 10, B is 11 up to F that is 15.

### **Text**

American Standard Code for Information Interchange (ASCII code) defines 128 different symbols. The symbols are all the characters found on a standard keyboard, plus a few extra. Unique numeric code (0 to 127) is assigned to each character. In ASCII, “A” is 65, “B” is 66, “a” is 97, “b” is 98,

and so forth. When a file is save as “plain text”, it is stored using ASCII. ASCII format uses 1 byte per character 1 byte gives only 256 (128 standard and 128 non-standard) possible characters. The code value for any character can be converter to base 2, so any written message made up of ASCII characters can be converted to a string of 0s and 1s.

## **Graphics**

Graphics on computer screen are consists of pixels. The pixels are tiny dots of color that collectively paint a graphic image on a computer screen. It is physical point in a raster image, or the smallest addressable element in an all points addressable display device. Hence it is the smallest controllable element of a picture represented on the screen. The address of a pixel corresponds to its physical coordinates. LCD pixels are manufactured in two-dimensional grid, and are often represented using dots or squares, but CRT pixels correspond to their timing mechanism and sweep rates. The pixels are organized into many rows and columns on the screen.

### **1.8. Review Questions**

1. Define data and Data Communication.
2. Compare analog and digital data
3. Why data communication
4. List and explain components of data communication system.
5. Highlights any 5 examples of resources that can be share on data communication and networks
6. Define and gives example of basic components of data communication network.
7. What are the major criteria that data communication network must meet.

8. Highlights the factors that affect response time as related to performance of data communication network.
9. List various ways of data representation in computer system.
10. Define Data communication equipment and data terminal equipment. Give at least two examples in each case.



# **CHAPTER TWO**

## **COMPUTER NETWORKING CONCEPTS**

### **2.1. What is Computer Network?**

Computer network is interconnectivity of two or more computer system for purpose of sharing data. A computer network is a communication system much like a telephone system, any connected device can use the network to send and receive information. In essence a computer network consists of two or more computers connected to each other so that they can share resources. Networking arose from the need to share resources in a timely fashion.

Sharing expensive peripherals is often promoted as the primary reason to network. But this is not a sufficient reason. In considering the cost benefits of sharing, we find some impressive arguments against networking. With today more affordable technology, we can easily dedicate inexpensive peripherals and not bother with a network. Desktops and laptops are getting less expensive as their capacities increase. As a result the local hard disk is becoming common place and is frequently dedicated to a local desktop or laptop. Flash drives and external hard disks now has enough storage for uses.

### **2.2. Why computer networking**

These are serious considerations but only part of the picture. When viewed as a system, networking has some powerful arguments in its favor. In most cases organizations with

multiple computer systems should network them for the following reasons:

1. Sharing of peripherals can be justified as a “shared resource”, with the result that speed and quality are improved and Mean Time Between Failure (MTBF) is increased. Sharing in a properly designed network improves the reliability of the entire system. When a device fails, another one is ready to fill the void while repairs are being made.
2. Better response time can be achieved through networking. The speed with which a request is answered is a crucial factor in computing. After all, most jobs performed by a computer can be done with pencil and paper. When you buy a computer, you are buying speed more than capability. Better response time through networking is in no way guarantee. In fact, inefficient use of the network will quickly result in unacceptably poor response. The elements needed for superior performance, however, are part of most networks. If properly implemented, a computer network will be more efficient than stand-alone computers or network terminals and will equal or surpass stand-alone computer performance.
3. The peripherals attached to a network tend to be faster than those dedicated to stand-alone computers. The bandwidth of all the local area network far exceeds the speed capability of a stand-alone computer. For many applications the computer, not the network, is the bottleneck. But since a local area network is by definition a multiple processor system, the possibility exists for sharing the processing load across several microprocessors, which is similar to parallel processing. You may not be able to speed up the computer itself, but you can speed up the results.

4. Often overlooked in an evaluation of networking is its organization benefit. Departments, companies, corporations, and institutions are all organizations, which imply interaction and team work. Without networking, the personal computer has been a powerful but isolated device. Its output has been difficult to integrate into the organization mainstream, so its value has been limited. In some instances the isolated personal computer has even created serious threats of data loss.

Networking is a communications mechanism that ties the isolated computer systems into the organization. In a networking environment, being able to communicate and share data encourages continuity and compatibility so that administrative chores can be systematized. For example, the task of backing up the data can be assigned to a particular individual, rather than left as an afterthought to each employee.

### **2.3. Protocol and Standards In Networking**

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol.

A protocol is a set of rules that govern data communications. It defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- **Syntax.** The term *syntax* refers to the structure or format of the data, meaning the order in which they are

presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

- **Semantics.** The word *semantics* refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
- **Timing.** The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention") and *de jure* (meaning "by law" or "by regulation").

- **De facto.** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

- **De jure.** Those standards that have been legislated by an officially recognized body are de jure standards

## **Standards Organizations**

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

### ***Standards Creation Committees***

While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

- **International Organization for Standardization (ISO).** The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
- **International Telecommunication Union-Telecommunication Standards Sector (ITU-T).** By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T).

- **American National Standards Institute (ANSI).** Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.
- **Institute of Electrical and Electronics Engineers (IEEE).** The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.
- **Electronic Industries Association (EIA).** Aligned with ANSI, the Electronic Industries Association is a non-profit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signalling specifications for data communication.

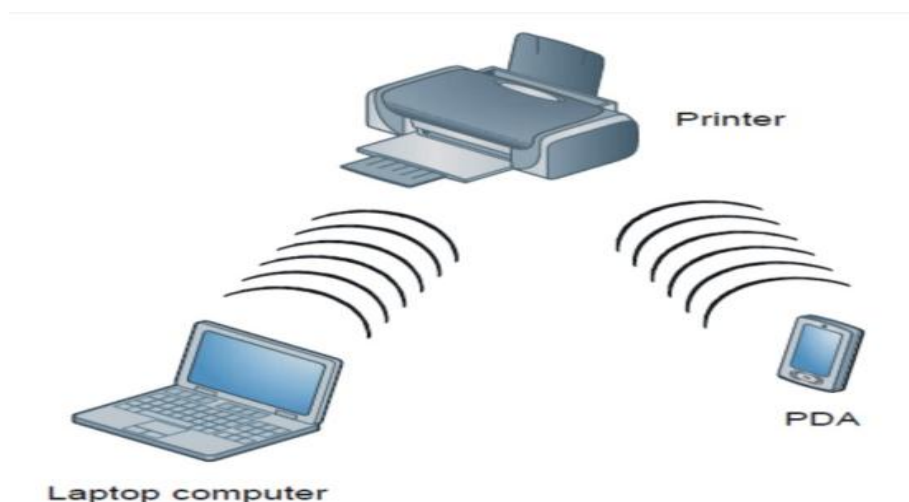
## **2.4. Types of Network**

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose. The size of a network can be expressed by the geographic area they occupy and number of computers that are part of the network. Networks can cover anything

from a handful of devices within a single room to millions of devices spread across the entire globe.

### **Personal Area Network**

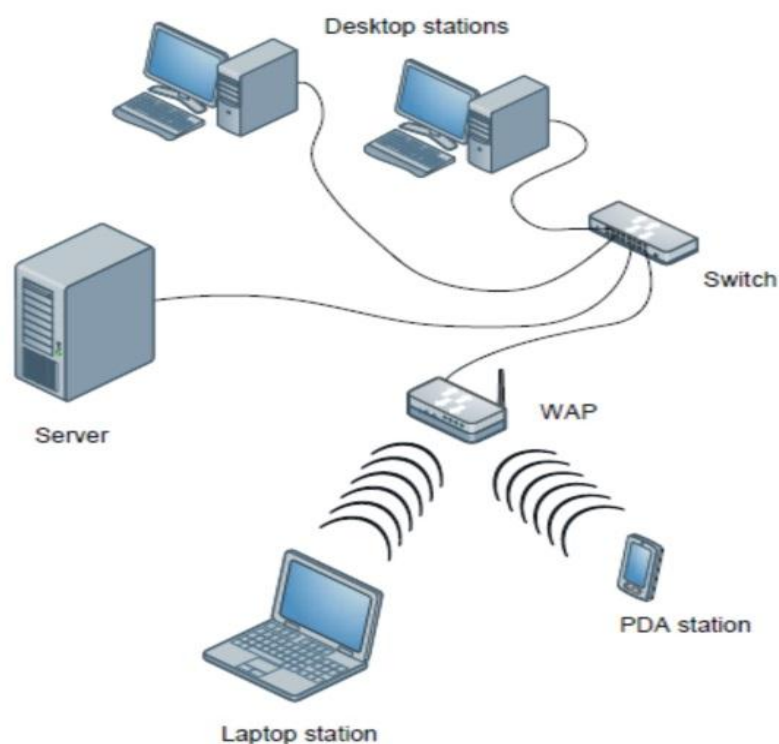
A personal area network (PAN) is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters. For example, a person traveling with a laptop, a personal digital assistant (PDA), and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology. Typically, this kind of personal area network could also be interconnected without wires to the Internet or other networks. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink). However, it is possible to have multiple individuals using this same network within a residence. If this is the case we can refer to the network as Home Area network (HAN). In this type of setup, all the devices are connected together using both wired and/or wireless. All networked devices can be connected to a single modem as a gateway to the Internet. See figure 5.



**Figure 5: Personal Area Network**

## Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and type of technology used, a LAN can be as simple as two desktops and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers. In addition to the size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. LANs are designed to allow resources to be shared between personal computers or workstations. Early LANs had data rates in the 4 to 16 mega-bits-per-second (Mbps). Today, however, speeds are normally 100Mbps or 1000Mbps. Wireless LANs (WLAN) are the newest evolution in LAN technology. See figure 6.

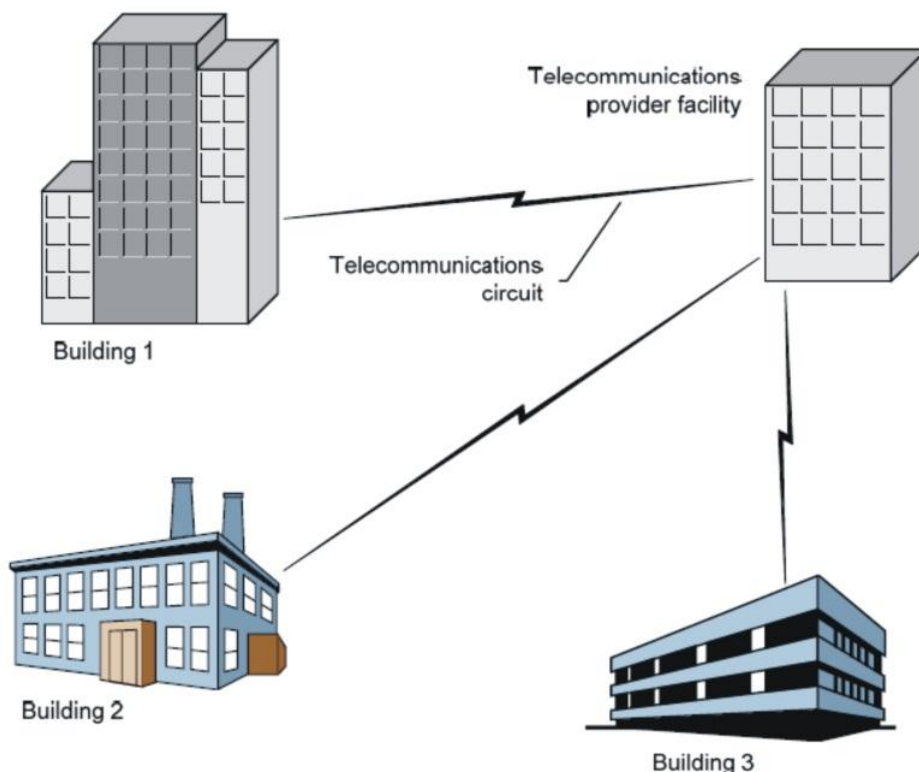


**Figure 6: Local Area Network**



## Metropolitan Area Network

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the internet, and have endpoints spread over a city or part of city. A good example of a MAN is part of the telephone company network that can provide a high-speed DSL line to the customer.



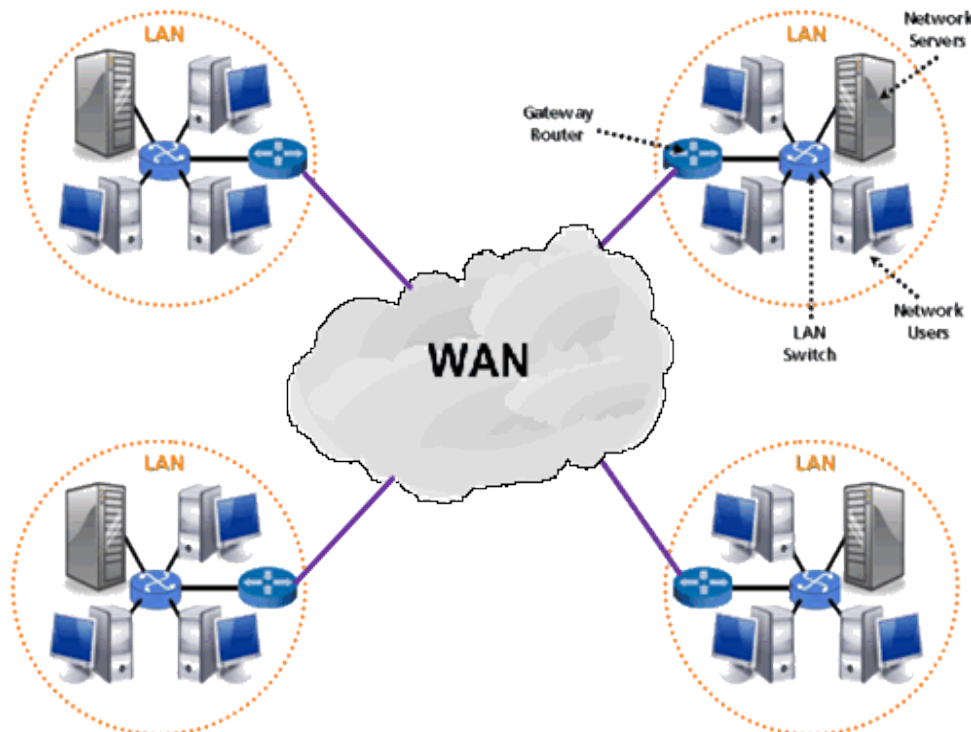
**Figure 7: Metropolitan area Network**

## Wide Area Network

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the internet.

We normally refer to the first one as a switched WAN and to the second as a point-to-point WAN.

The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an internet service provider (ISP). A good example of a switched WAN is X.25, the asynchronous transfer mode (ATM) network. See figure 8.

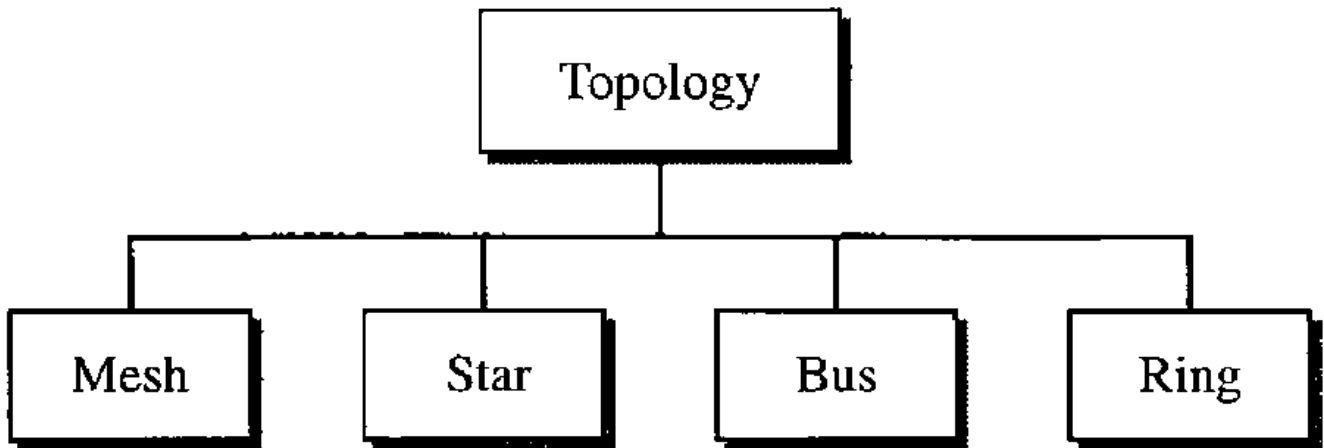


**Figure 8: Wide Area Network**

## 2.5. Network Topologies

The term topology in computer networking refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all links and linking devices (usually called nodes) to one another. The cost and flexibility of a network

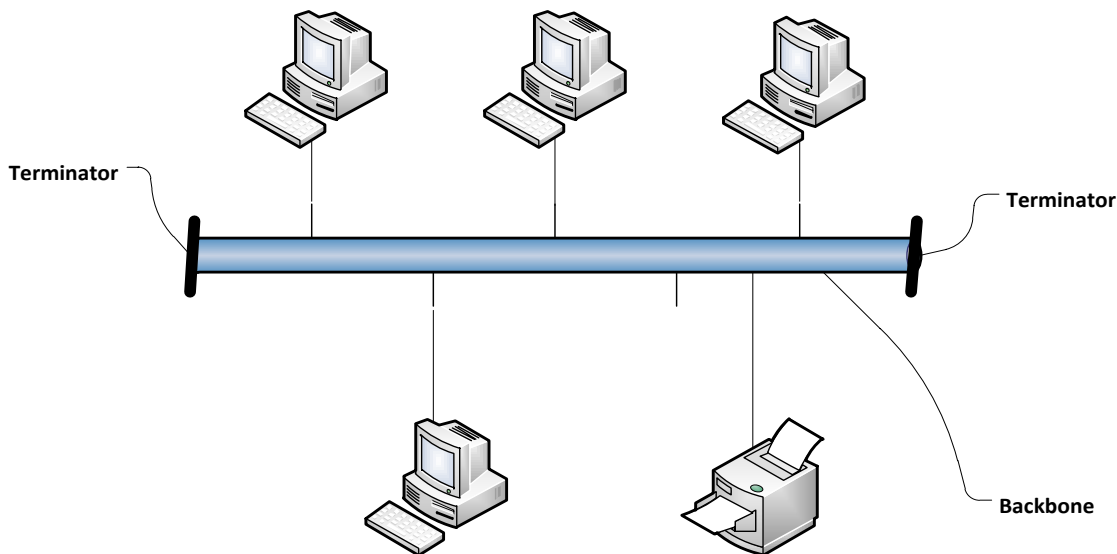
installation are partly affected by as is system reliability. Many network topologies are commonly used, but they all have certain similarities. Information is carried either through space (wireless) or cable. The cable must control the movement of information on the network so that data can be transmitted in a reliable manner. There are four basic topologies possible: mesh, star, bus, and ring. See Figure 9.



**Figure 9: Network Topology categories**

### **2.5.1. Bus Topology**

The Bus topology consists of a single cable that runs to every work-station. See figure 10. The bus topology is also known as linear bus. In other words, all the nodes (computers and servers) are connected to the single cable (called bus), by the help of interface connectors. This central cable is the back bone of the network and every workstation communicates with the other device through this bus.



**Figure 10: Bus Topology**

Computers on a bus topology network communicate by addressing data to a particular computer and putting that data on the cable in the form of electronic signals. To understand how computers communicate on a bus you need to be familiar with three concepts:

- i. **Sending the signal:** Network data in the form of electronic signals is sent to all of the computers on the network; however, the information is accepted only by the computer whose address matches the address encoded in the original signal. Only one computer at a time can send messages.

Because only one computer at a time can send data on a bus network, network performance is affected by the number of computers attached to the bus. The more computers on a bus, the more computers there will be waiting to put data on the bus, and the slower the network.

There is no standard measure for the impact of numbers of computers on any given network. The amount the network slows down is not solely related to the number of computers on the network. It depends on numerous factors including:

- Hardware capacities of computers on the network
- Number of times computers on the network transmit data
- Type of applications being run on the network
- Types of cable used on the network
- Distance between computers on the network

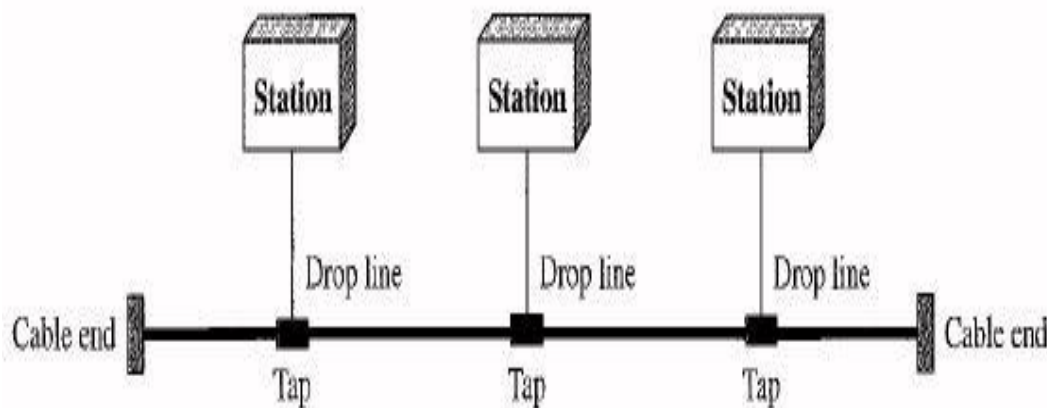
The bus is a passive topology. Computers on a bus only listen for data being sent on the network. They are not responsible for moving data from one computer to the next. If one computer fails, it does not affect the rest of the network. In active topology computers regenerate signals and move data along the network.

- ii. **Signal Bounce:** Because the data, or electronic signal, is sent to the entire network, it will travel from one end of the cable to the other. If the signal were allowed to continue uninterrupted, it would keep bouncing back and forth along the cable and prevent other computers from sending signals. Therefore, the signal must be stopped.

**The Terminator:** To stop the signal from bouncing, a component called a terminator is placed at each end of the cable to absorb free signals. Absorbing the signal clears the cable so that other computers can send data. Every cable end on the network must be plugged into something. For example, a cable end could be plugged into a computer or a connector to extend the cable length. Any open cable ends not plugged into something – must be terminated to prevent signal bounce.

In bus topology nodes are connected to the bus cable by drop lines and taps. See figure 11. A drop line is a connection running between the device and the main cable. A tap is a

connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.



**Figure 11: Bus Topology with three stations**

#### **Advantages of Linear Bus Topology**

- 1) It is easy to set-up and extend bus network.
- 2) Cable length required for this topology is the least compared to other networks.
- 3) Bus topology very cheap.
- 4) Linear Bus network is mostly used in small networks.

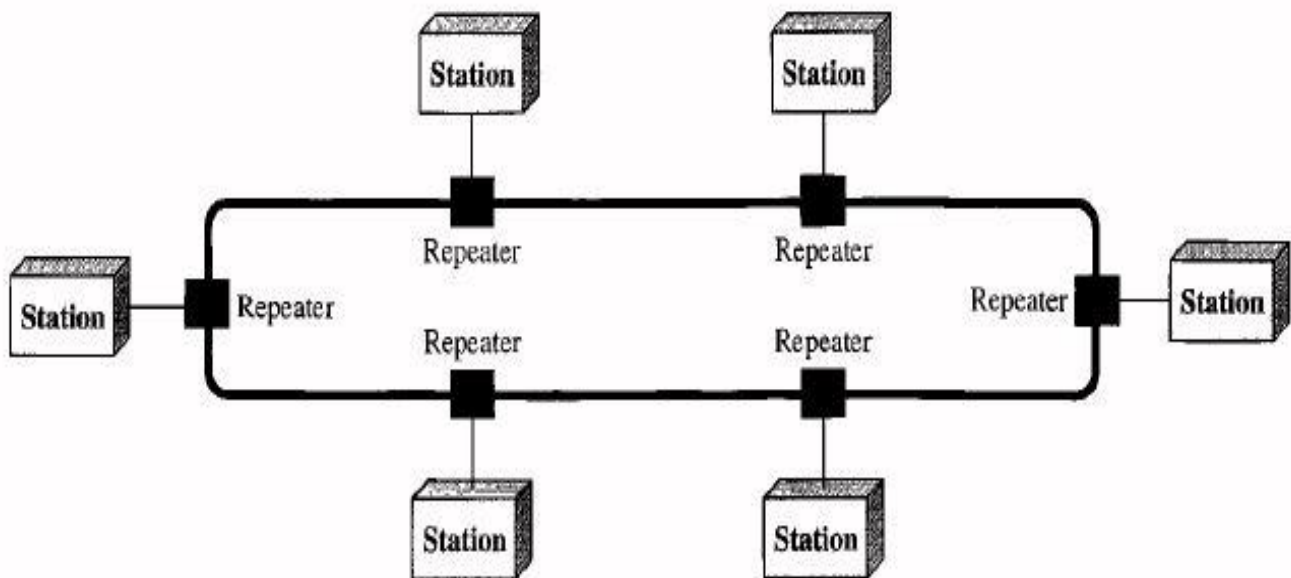
#### **Disadvantages of Linear Bus Topology**

- 1) There is a limit on central cable length and number of nodes that can be connected.
- 2) Dependency on central cable in this topology has its disadvantages. If the main cable (i.e. bus) encounters some problem, whole network breaks down.

- 3) Proper termination is required to dump signals. Use of terminators is must.
- 4) It is difficult to detect and troubleshoot fault at individual station.
- 5) Maintenance costs can get higher with time.
- 6) Efficiency of Bus network reduces, as the number of devices connected to it increases.
- 7) It is not suitable for networks with heavy traffic.
- 8) Security is very low because all the computers receive the sent signal from the source.

### 2.5.2. Ring Topology

The ring topology connects computers on a single circle of cable. There are no terminated ends. A ring topology connects one host to the next and the last host to the first. The signal travels around the loop in one direction and pass through each computer. Unlike the passive bus topology, each computer acts like a repeater to boost the signal and send it on to the next computer. Because the signal passes through each computer, the failure of one computer can impact the entire network.



**Figure 12: Ring Topology**

One method of transmitting data around a ring is called token passing. The token is passed from computer to computer until it gets to a computer that has data to send. The sending computer modifies the token, puts an electronic address on the data, and sends it around the ring.

### **Advantages of Ring Topology**

- 1) This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduce chances of collision. Also in ring topology all the traffic flows in only one direction at very high speed.
- 2) Even when the load on the network increases, its performance is better than that of Bus topology.
- 3) There is no need for network server to control the connectivity between workstations.
- 4) Additional components do not affect the performance of network.
- 5) Each computer has equal access to resources.

### **Disadvantages of Ring Topology**

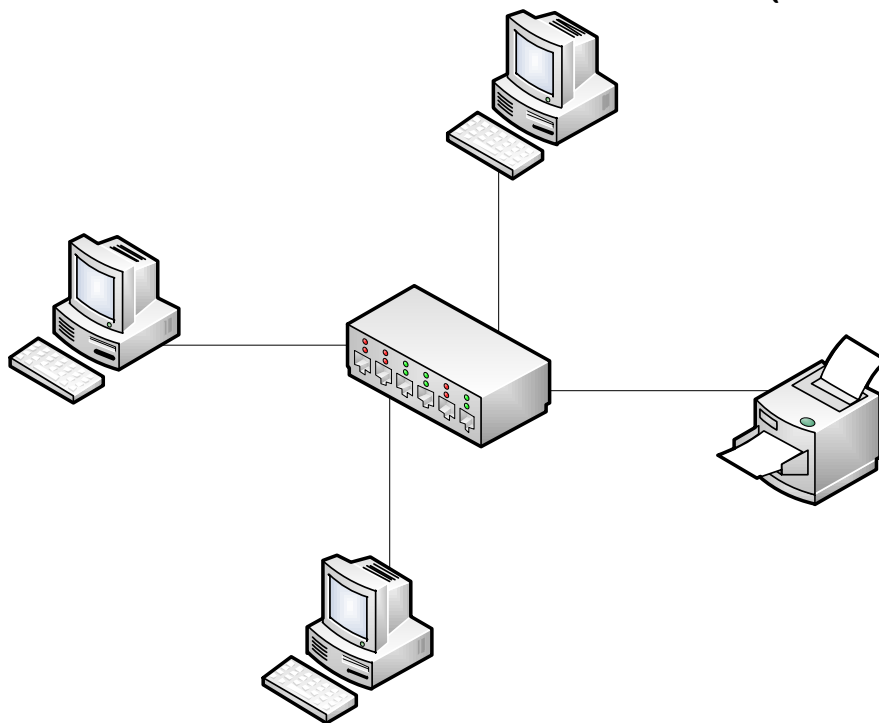
- 1) Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.
- 2) If one workstation or port goes down, the entire network gets affected.
- 3) Network is highly dependent on the wire which connects different components.
- 4) MAU's and network cards are expensive as compared to Ethernet cards and hubs.

### **2.5.3. Star Topology**

In the star topology, computers are connected by cable segments to centralized component, called a hub or switch.



Signals are transmitted from the sending computer through the hub or switch to all computers on the network. This topology originated in the early days of computing with computers connected to a centralized mainframe computer. It is now a common topology in microcomputer networking. Each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure 11)



**Figure 13: Star Topology**

The star network offers centralized resources and management. However, because each computer is connected to a central point, this topology requires a great deal of cable in a large network installation. Also, if the central point fails, the entire network goes down.

## **Advantages of Star Topology**

- 1) As compared to Bus topology it gives far much better performance, signals don't necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of central hub.
- 2) Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network. Similarly components can also be removed easily.
- 3) Centralized management. It helps in monitoring the network.
- 4) Failure of one node or link doesn't affect the rest of network. At the same time it is easy to detect the failure and troubleshoot it.

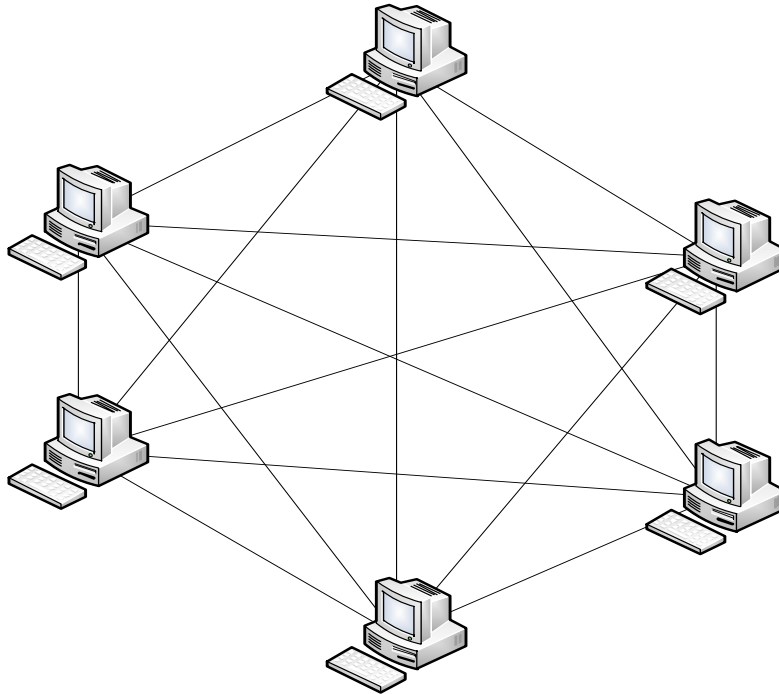
## **Disadvantages of Star Topology**

- 1) Too much dependency on central device has its own drawbacks. If it fails whole network goes down.
- 2) The use of hub, a router or a switch as central device increases the overall cost of the network.
- 3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device.

### **2.5.3. Mesh Topology**

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. In a mesh topology, Node1 must be connected to  $n-1$  nodes, node2 must be connected to  $(n-1)$  nodes, and finally node  $n$  must be connected to  $(n-1)$  nodes. We need  $n$

$(n - 1)$  physical links. In other words, we can say that in a mesh topology, we need  $n(n - 1) / 2$ .



**Figure 14: Mesh topology**

To accommodate many links, every device on the network must have  $(n - 1)$  input/output (I/O) ports to be connected to the  $(n - 1)$  stations as shown in Figure above. For these reasons a mesh topology is usually implemented in a limited fashion, as a backbone connecting the main computers of a hybrid network that can include several other topologies. One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

#### **Advantages of Mesh topology**

- 1) Data can be transmitted from different devices simultaneously. This topology can withstand high traffic.

- 2) Even if one of the components fails there is always an alternative present. So data transfer doesn't get affected.
- 3) Expansion and modification in topology can be done without disrupting other nodes.

#### **Disadvantages of Mesh topology**

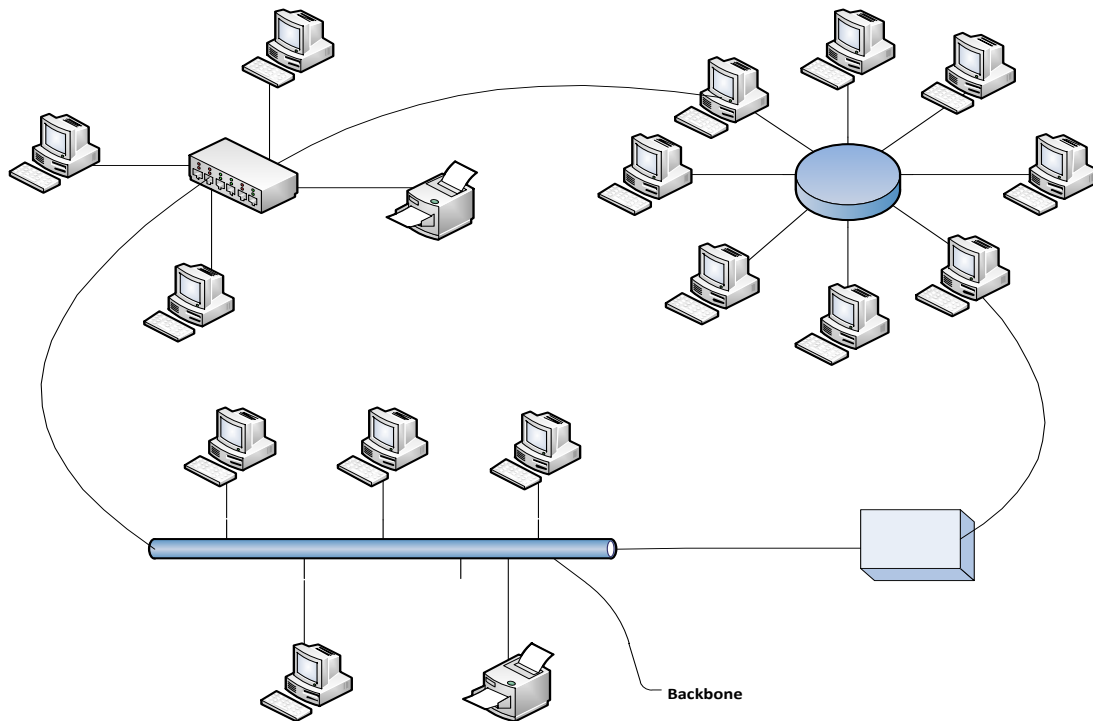
- 1) There are high chances of redundancy in many of the network connections.
- 2) Overall cost of this network is way too high as compared to other network topologies.
- 3) Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

#### **2.5.5. Hybrid Topology**

Before starting about Hybrid topology, we saw that a network topology is a connection of various links and nodes, communicating with each other for transfer of data. We also saw various advantages and disadvantages of Star, Bus, Ring, Mesh. Hybrid, as the name suggests, is mixture of two different things. Similarly in this type of topology we integrate two or more different topologies to form a resultant topology which has good points (as well as weaknesses) of all the constituent basic topologies rather than having characteristics of one specific topology. This combination of topologies is done according to the requirements of the organization.

For example, if there is an existing ring topology in one office department while a bus topology in another department, connecting these two will result in Hybrid topology. Remember connecting two similar topologies cannot be termed as Hybrid topology. Star-Ring and Star-Bus networks

are most common examples of hybrid network. (see figure 12).



**Figure 15: Hybrid Network**

### **Advantages of Hybrid Network Topology**

- 1) **Reliable:** Unlike other networks, fault detection and troubleshooting is easy in this type of topology. The part in which fault is detected can be isolated from the rest of network and required corrective measures can be taken, **WITHOUT** affecting the functioning of rest of the network.
- 2) **Scalable:** It's easy to increase the size of network by adding new components, without disturbing existing architecture.
- 3) **Flexible:** Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of

fault are high.  
4) Effective: Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while their weaknesses are neutralized. For example we saw Ring Topology has good data reliability (achieved by use of tokens) and Star topology has high tolerance capability (as each node is not directly connected to other but through central device), so these two can be used effectively in hybrid star-ring topology.

### **Disadvantages of Hybrid Topology**

- 1) **Complexity of Design:** One of the biggest drawbacks of hybrid topology is its design. It is not easy to design this type of architecture and it's a tough job for designers. Configuration and installation process needs to be very efficient.
- 2) **Costly Hub:** The hubs used to connect two distinct networks, are very expensive. These hubs are different from usual hubs as they need to be intelligent enough to work with different architectures and should be function even if a part of network is down.
- 3) **Costly Infrastructure:** As hybrid architectures are usually larger in scale, they require a lot of cables; cooling systems, sophisticated network devices, etc.

### **2.6. Review Questions**

1. Enumerates five components of a data communications system.
2. Define key element of protocol.
3. Define two types of standards.
4. Describe the role of the following standards creation committee.

- i. International Organization for Standardization (ISO).
  - ii. International Telecommunication Union
  - iii. American National Standards Institute (ANSI).
  - iv. Institute of Electrical and Electronics Engineers (IEEE).
- 1) What are the three criteria necessary for an effective and efficient network?
  - 2) Categorize the four basic topologies in terms of line configuration.
  - 3) Name the four basic network topologies, and cite an advantage of each type.
  - 4) For  $n$  devices in a network, what is the number of cable links required for a mesh, ring, bus, and star topology?
  - 5) What are some of the factors that determine whether a communication system is a LAN or WAN?
  - 6) Assuming you get a job as a network engineer in a multinational company that has five (5) regional station that must be interconnected with others for smooth operation of the organization. The company is about to network the regional offices together. Each physical link must allow communication in both directions. Use the knowledge acquired in this course to advice the management of the company based on the following:
    - a) Recommend the most suitable Network topology for the organization.
    - b) Give detail explanation of the recommended Topology.
    - c) Illustrate the explanation in (b) with a diagram to show the interconnectivity of the five (5) regional offices.
    - d) Explain four (4) major advantages of the topology named in (a) over other network topology.

# **CHAPTER THREE**

## **COMPUTER NETWORK MODELS**

### **3.1. Description of Network Model**

When dealing with networking, you may hear the terms "network model" and "network layer" used often. Network models define a set of network layers and how they interact. There are several different network models depending on what organization or company started them. The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1. The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer.

### **3.2. Network Model Layers**

The Open Systems Interconnect (OSI) model has seven layers. This article describes and explains them, beginning with the 'lowest' in the hierarchy (the physical) and proceeding to the 'highest' (the application). The layers are stacked as follows:



- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

### **3.2.1. PHYSICAL LAYER**

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

- Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
  - What signal state represents a binary 1
  - How the receiving station knows when a "bit-time" starts
  - How the receiving station delimits a frame
- Physical medium attachment, accommodating various possibilities in the medium:
  - Will an external transceiver (MAU) be used to connect to the medium?
  - How many pins do the connectors have and what is each pin used for?
- Transmission technique: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.

- **Physical medium transmission:** transmits bits as electrical or optical signals appropriate for the physical medium, and determines:
  - What physical medium options can be used
  - How many volts/db should be used to represent a given signal state, using a given physical medium

### **3.2.2. DATA LINK LAYER**

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

- **Link establishment and termination:** establishes and terminates the logical link between two nodes.
- **Frame traffic control:** tells the transmitting node to "back-off" when no frame buffers are available.
- **Frame sequencing:** transmits/receives frames sequentially.
- **Frame acknowledgment:** provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- **Frame delimiting:** creates and recognizes frame boundaries.
- **Frame error checking:** checks received frames for integrity.
- **Media access management:** determines when the node "has the right" to use the physical medium.

### **3.2.3. NETWORK LAYER**

The network layer controls the operation of the subnet, deciding which physical path the data should take based on

network conditions, priority of service, and other factors. It provides:

- **Routing:** routes frames among networks.
- **Subnet traffic control:** routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- **Frame fragmentation:** if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- **Logical-physical address mapping:** translates logical addresses, or names, into physical addresses.
- **Subnet usage accounting:** has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

**Communications Subnet:** The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet). In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

### **3.2.4. TRANSPORT LAYER**

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers. The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

- **Message segmentation:** accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- **Message acknowledgment:** provides reliable end-to-end message delivery with acknowledgments.
- **Message traffic control:** tells the transmitting station to "back-off" when no message buffers are available.
- **Session multiplexing:** multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

#### **End-to-end layers**

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

#### **3.2.5. SESSION LAYER**

The session layer allows session establishment between processes running on different stations. It provides:

- **Session establishment, maintenance and termination:** allows two application processes on different machines to establish, use and terminate a connection, called a session.
- **Session support:** performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

### **3.2.6. PRESENTATION LAYER**

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

- Character code translation: for example, ASCII to EBCDIC.
- Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.

### **3.2.7. APPLICATION LAYER**

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Inter-process communication
- Network management
- Directory services
- Electronic messaging (such as mail)
- Network virtual terminals

### **3.3. Review Questions**

1. What are the concerns of the physical layer in the Internet model?
2. What are the responsibilities of the data link layer in the Internet model?
3. What are the responsibilities of the network layer in the Internet model?
4. What are the responsibilities of the transport layer in the Internet model?
5. What is the difference between a port address, a logical address, and a physical address?
6. Name some services provided by the application layer in the Internet model.
7. How do the layers of the Internet model correlate to the layers of the OSI model?
8. How are OSI and ISO related to each other?
9. Match the following to one or more layers of the OSI model:
  - a) Route determination
  - b) Flow control
  - c) Interface to transmission media
  - d) Provides access for the end user
9. Match the following to one or more layers of the OSI model:
  - a) Reliable process-to-process message delivery
  - b) Route selection
  - c) Defines frames
  - d) Provides user services such as e-mail and file transfer
  - e) Transmission of bit stream across physical medium
10. Match the following to one or more layers of the OSI model:
  - a) Communicates directly with user's application program

- b) Error correction and retransmission**
- c) Mechanical, electrical, and functional interface**
- d) Responsibility for carrying frames between adjacent nodes**



# **CHAPTER FOUR**

## **DATA COMMUNICATION SOFTWARE AND PROTOCOL**

### **4.1. Data Communication Software**

#### **4.1.1. Description of Communication Software**

The basic concept behind data communication and network is for the two or more computer or electronic devices to see each other and share resources. For that to be achieved there must be a program or software responsible for the communication to take place. The software in this case is referred to as data communication software. Data communication Software is basically a computer program that.

1. It is a computer program required on DTE (PC) to bridge the gap and interpret the bits/bytes that are transmitted via the communication media through the interface.
2. The Core of Data Communication is Communication Software without software, Data communication is incomplete.
3. Communication Software is responsible for controlling data formatting, data transmission, and total communication control.
4. It may completely reside on central PC or part of it may be located on the front end communication PC, a concentrator, remote concentrator or in intelligent terminals.

#### **4.1.2. Significance of Data Communication Software**

Major significance of data Communication software are:

- i. Defines the communication parameters like communication speed, error rate, bandwidth, protocols, etc.
- ii. Controls the user accessibility to information. It means how a user can access the information and how information shall be presented to user.
- iii. It controls the optimal configuration of communication hardware and makes the effective utilization of network resources.

#### **4.1.3. Function of Communication software**

General functions of communication software are:

- i. Establish logical data paths.
- ii. Check accuracy of each transmission, and arrange retransmission if necessary (e.g. TCP/IP).
- iii. Exercise flow control to avoid congestion and loss of data.
- iv. Maintaining the statistics on traffic volumes over all links, and on network reliability
- v. Transmission initiation and termination is done by communication software when user prompts it. In case of modem, modem initialization and making it ready function come under this category.
- vi. Establishment of logical connections over physical line like dialing the number on phone lines.
- vii. Message Assembly and De-assembly.
- viii. Data Transmission & receipt. It means Modulation of digital data into analog and vice versa by modem).
- ix. Code conversion is done by communication software where it format the data
- x. Error Detection is also done by it. It checks for lost bits and other error introduced while transmitting.
- xi. Data Editing
- xii. Control Character Recognition

- xiii. **Data Delivery and output.** Communication software control the output and delivery of data at the destination)
- xiv. **Transmission monitoring and maintenance**

#### **4.1.4. Categories of Communication Software**

Data communication software can be categories into two:

1. **Application Software:** These are the software that enables end users to perform one task or the other on data communication and network system. For example Email Software - all types for email software's which include the following, Broadcast Software - including MP3s, audio recording and call recording software, and Wireless Software - all types of wireless related software's
2. **System Software:** Software that allows you to connect with other computers or mobile devices via text, video or audio formats in either a synchronous or asynchronous manner. They are set of software that enable data communication system to function and meet the require objective of resources sharing and other functionability. Data communication system software can be classified in into development software, and management software e.g. networks traffic analyzer, a ping/traceroute program, firewall etc.

### **4.2. Communication Protocol**

#### **4.2.1. Description of Communication Protocol**

A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking Igbo cannot be understood by a person who speaks only Yoruba. A

communication protocol is a description of the rules that communication devices must follow to communicate with each other. A Protocol is one of the components of a data communications system. Without protocol communication cannot occur. The sending device cannot just send the data and expect the receiving device to receive and further interpret it correctly. Protocol was mentioned briefly in chapter two of this book but discussed fully in this chapter.

#### **4.2.2. Elements of a Protocol**

There are three key elements of a protocol:

- a. Syntax is the structure or format of the data. It is the arrangement of data in a particular order.
- b. Semantics gives the meaning of each section of bits and indicates the interpretation of each section. It also tells what action/decision is to be taken based on the interpretation.
- c. Timing tells the sender about the readiness of the receiver to receive the data. It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

#### **4.2.3. Transmission Control Protocol (TCP)**

TCP/IP is the basic communication protocol for two or more computers or electronic devices (e.g. mobile phone) to communicate with one another on a network setup. TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP defines how electronic devices (like computers) should be connected to the Internet, and how data should be transmitted between them. TCP/IP is the major protocol in communication network that communication can do without. Inside the TCP/IP standard there are several protocols for handling data communication these are: TCP (Transmission Control Protocol) communication between applications; UDP

(User Datagram Protocol) simple communication between applications; IP (Internet Protocol) communication between computers; ICMP (Internet Control Message Protocol) for errors and statistics; DHCP (Dynamic Host Configuration Protocol) for dynamic addressing; and TCP Uses a Fixed Connection.

**Transmission Control Protocol:** Transmission Control Protocol takes care of the communication between your application software (i.e. your browser) and your network software. TCP is responsible for breaking data down into IP packets before they are sent, and for assembling the packets when they arrive. TCP is for communication between applications. If one application wants to communicate with another via TCP, it sends a communication request. This request must be sent to an exact address. After a "handshake" between the two applications, TCP will set up a "full-duplex" communication between the two applications. The "full-duplex" communication will occupy the communication line between the two computers until it is closed by one of the two applications.

**Internet Protocol:** Internet Protocol is Connection-Less i.e, it does not occupy the communication line between two computers. The Network Layer protocol for TCP/IP is the Internet Protocol (IP). It uses IP addresses and the subnet mask to determine whether the datagram is on the local or a remote network. If it is on the remote network, the datagram is forwarded to the default gateway which is a router that links to another network. IP keeps track of the number of transverse through each router that the datagram goes through to reach its destination. Each transverse is called a hop. If the hop count exceeds 255 hops, the datagram is removed and the destination considered unreachable. IP

reduces the need for network lines. Each line can be used for communication between many different computers at the same time. With IP, messages (or other data) are broken up into small independent "packets" and sent between computers via the Internet. IP is responsible for "routing" each packet to the correct destination.

#### **4.2.4. Special Purpose Protocol**

The special purpose protocols are the set of protocols design to perform a single task on communication network system. Some of these protocols and their function are listed below:

- i. **HTTP - Hyper Text Transfer Protocol:** HTTP takes care of the communication between a web server and a web browser. HTTP is used for sending requests from a web client (a browser) to a web server, returning web content (web pages) from the server back to the client.
- ii. **HTTPS - Secure HTTP:** HTTPS takes care of secure communication between a web server and a web browser. HTTPS typically handles credit card transactions and other sensitive data.
- iii. **SSL - Secure Sockets Layer:** The SSL protocol is used for encryption of data for secure data transmission.
- iv. **MIME - Multi-purpose Internet Mail Extensions:** The MIME protocol lets SMTP transmit multimedia files including voice, audio, and binary data across TCP/IP networks.
- v. **IMAP - Internet Message Access Protocol:** IMAP is used for storing and retrieving e-mails.
- vi. **FTP - File Transfer Protocol:** FTP takes care of transmission of files between computers.
- vii. **NTP - Network Time Protocol:** NTP is used to synchronize the time (the clock) between computers.

- viii. **DHCP - Dynamic Host Configuration Protocol:** DHCP is used for allocation of dynamic IP addresses to computers in a network.
- ix. **SNMP - Simple Network Management Protocol:** SNMP is used for administration of computer networks.
- x. **LDAP - Lightweight Directory Access Protocol:** LDAP is used for collecting information about users and e-mail addresses from the internet.
- xi. **ICMP - Internet Control Message Protocol:** ICMP takes care of error-handling in the network.
- xii. **ARP - Address Resolution Protocol:** ARP is used by IP to find the hardware address of a computer network card based on the IP address.
- xiii. **RARP - Reverse Address Resolution Protocol:** RARP is used by IP to find the IP address based on the hardware address of a computer network card.

#### **4.3. Review Questions**

1. Define communication software
2. What are general functions of communication Software
3. Give examples and function of the following communication Software.
  - i. Broadcast software
  - ii. Messaging software
  - iii. Instant communication Software
4. TCP/IP Protocol is communication software. Yes or NO discuss your answer.
5. What are the elements of communication protocol
6. Compare TCP and IP, hence highlights and gives function of basic protocol for handling data communication
7. Describe the communication between one application and other via TCP/IP

8. What happen when a new domain name is registered together with TCP/IP address
9. Give the full meaning and function of the following protocols
  - i. HTTP
  - ii. SSL
  - iii. MIME
  - iv. BOOTP
  - v. SMTP
  - vi. LDAP



# **CHAPTER FIVE**

## **TRANSMISSION MODES**

### **5.1. Description of Data Flows and Transmission Mode**

A transmission may be simplex, half duplex, or full duplex. In simplex transmission, signals are transmitted in only one direction; one station is transmitter and the other is receiver. In half-duplex operation, both stations may transmit, but only one at a time. In full-duplex operation, both stations may transmit simultaneously.

### **5.2. Types of Transmission Mode and Data Flow**

Transmission mode is of three types as discussed in section 5.2.1 to 5.2.3.

#### **5.2.1. Simplex Transmission**

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction. Examples are Radio and Television broadcasts. They go from the TV station to your home television.

#### **5.2.2. Half Duplex Transmission**

In half-duplex mode, each station can both transmit and receive, but not at the same time.

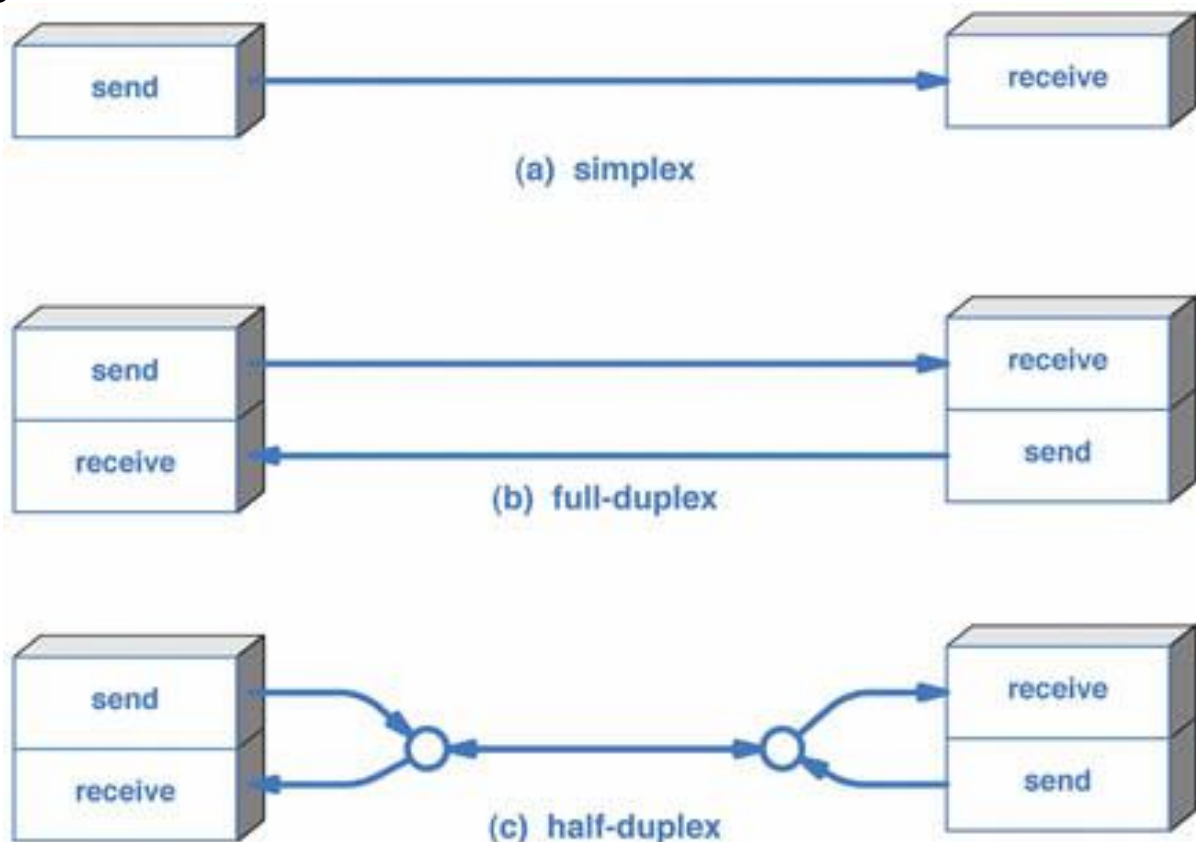
When one device is sending, the other can only receive, and vice versa. The half-duplex mode is like a one-lane road with

traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.

### 5.2.3. Full Duplex Transmission

In full-duplex mode, both stations can transmit and receive simultaneously. The full-duplex mode is like a two way street with traffic flowing in both directions at the same time. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

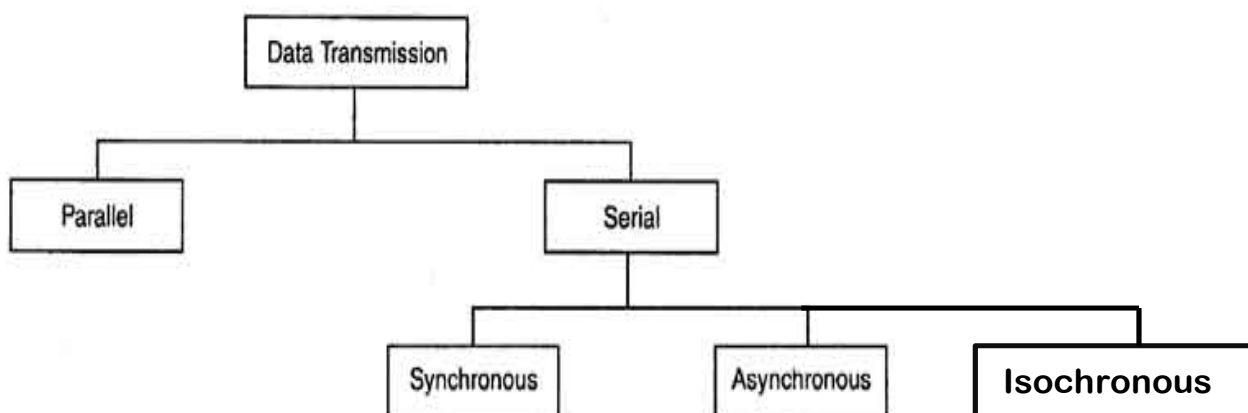
Figure 16 illustrate the data flow in section 5.2.1 to 5.2.3.



**Figure 16: Data Transmission Mode**

### 5.3. Digital Data Transmission Methods

In section 5.2, we see that for communication to occur there will be a channel of communication through which the devices are interconnected. In digital data transmission where we have more than one bits to send from sender to receiver. Our primary when we are considering the wiring is the data **stream**. Do we send 1 bit at a time; or do we group bits into larger groups and, if so, how? The transmission of binary data across a link can be accomplished in either parallel or serial mode. In parallel mode, multiple bits are sent with each clock tick. In serial mode, 1 bit is sent with each clock tick. While there is only one way to send parallel data, there are three subclasses of serial transmission: asynchronous, synchronous, and isochronous. See figure17.

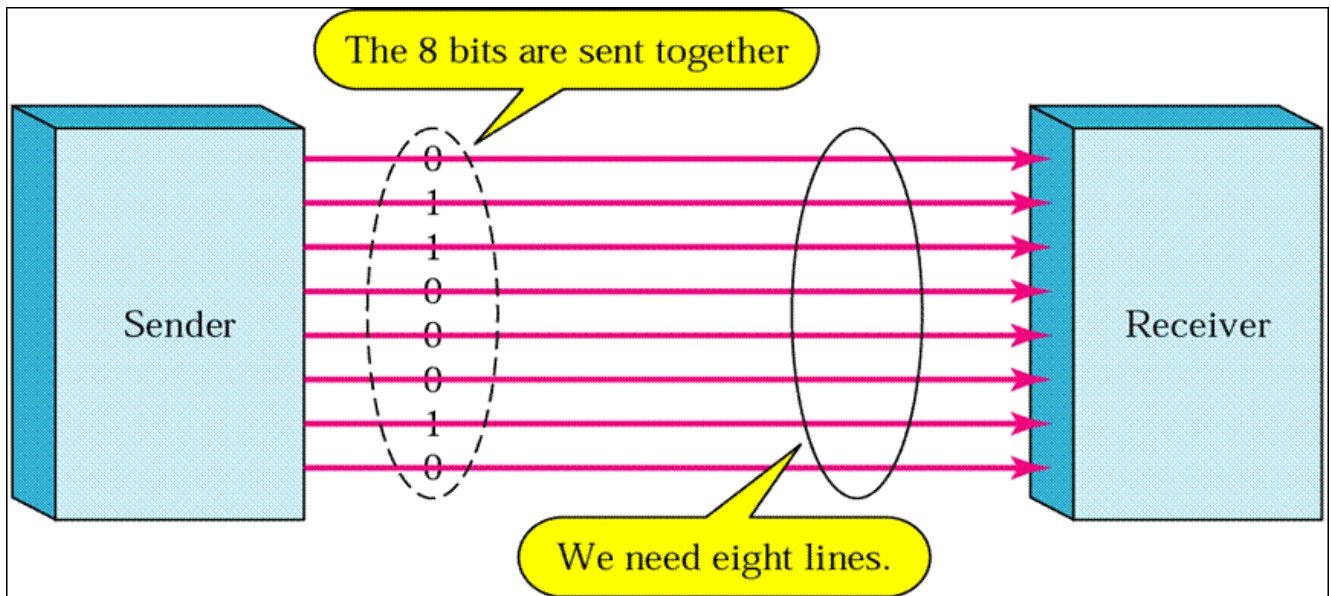


**Figure 17: Data Transmission**

#### 5.3.1. Parallel Transmission

Binary data, consisting of 1s and 0s, will be organized into groups of  $n$  bits each. Computers produce and consume data in groups of bits. By grouping, we can send data  $n$  bits at a time instead of 1. This is called parallel transmission. The advantage of parallel transmission is speed. All else being equal, parallel transmission can increase the transfer speed by a factor of  $n$  over serial transmission. Shortcoming of

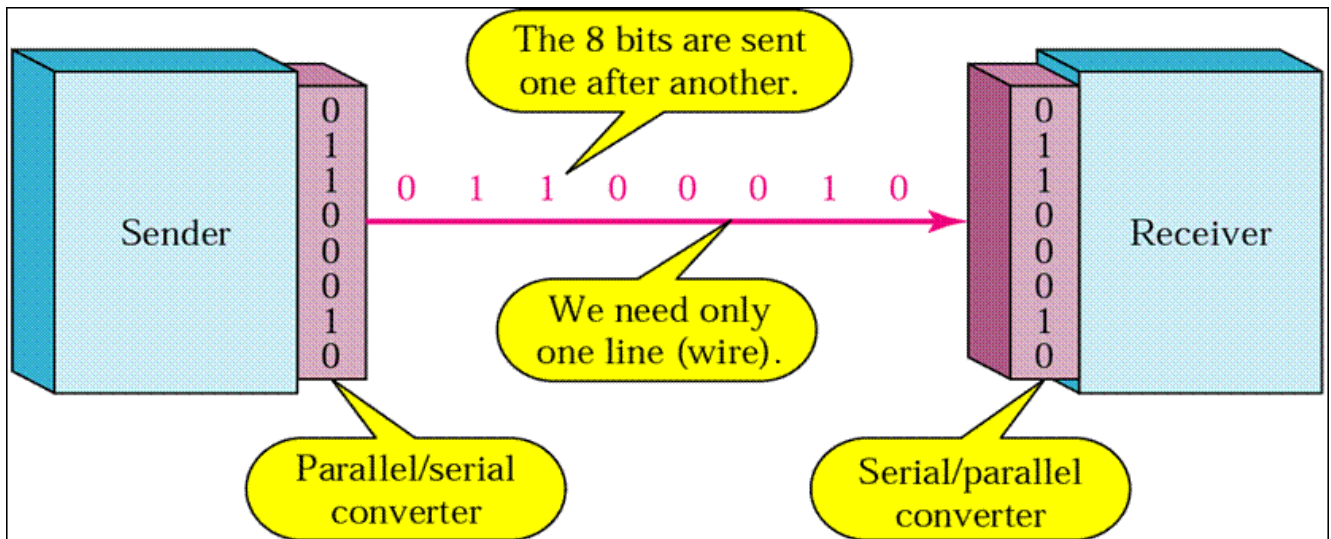
parallel transmission it requires  $n$  communication lines just to transmit the data stream. Hence it is expensive, parallel transmission is usually limited to short distances. See figure 18.



**Figure 18: Parallel transmission**

### 5.3.2. Serial Transmission

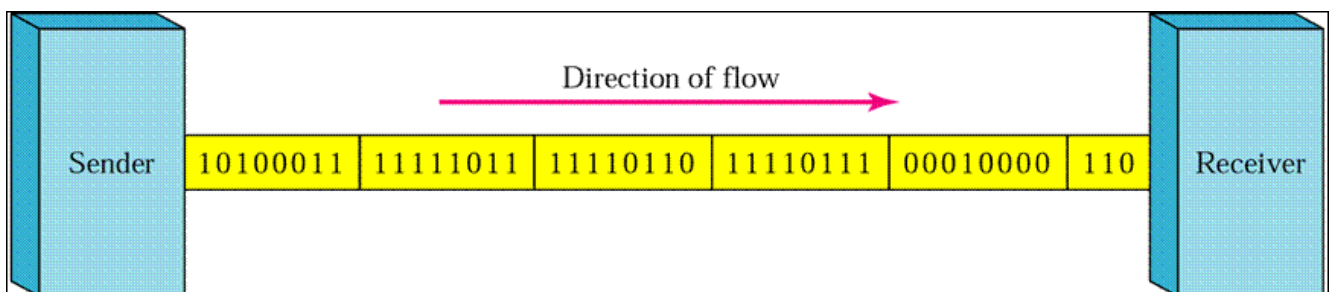
In serial transmission one bit follows another, so we need only one communication channel rather than  $n$  to transmit data between two communicating devices. The advantage of serial over parallel transmission is that with only one communication channel, serial transmission reduces the cost of transmission over parallel by roughly a factor of  $n$ . Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel-to-serial) and between the line and the receiver (serial-to-parallel). Serial transmission occurs in one of three ways: asynchronous, synchronous, and isochronous.



**Figure 19: Serial Transmission**

### 5.3.2.1. Synchronous Transmission

In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits.



**Figure 20: Synchronous Transmission**

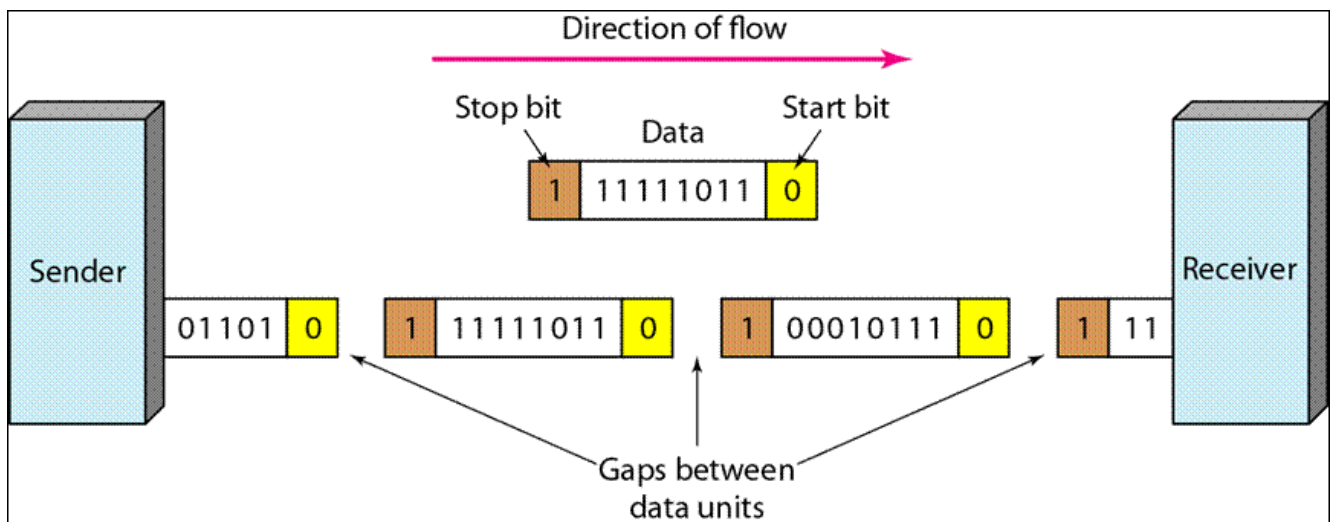
### 5.3.2.2. Isochronous Transmission

A sequence of events is isochronous if the events occur regularly, or at equal time intervals. The isochronous transmission guarantees that the data arrive at a fixed rate. In real-time audio and video, in which uneven delays between frames are not acceptable, synchronous transmission fails. For example, TV images are broadcast at the rate of 30 images per second; they must be viewed at the same rate. If

each image is sent by using one or more frames, there should be no delays between frames.

### 5.3.2.3. Asynchronous Transmission

In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (1) at the end of each byte. There may be a gap between each byte.



**Figure 21: Asynchronous Transmission**

## 5.4. Review Questions

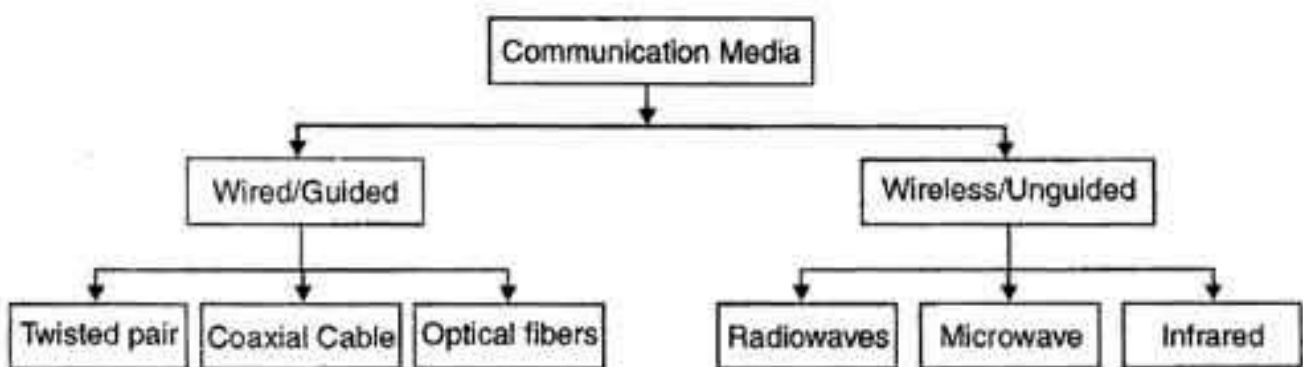
1. Describe with diagram the data transmission type.
2. Compare a 10K Byte data transmission using Asynchronous transmission & Synchronous Transmission. Determine the efficiency (10 Kbytes = 80 kbits)
3. Compare synchronous and asynchronous transmission
4. What is data flow? Hence describe three major types of data flow in data communication network.
5. Describe briefly with diagram and relevant example, three major data flow approaches.
6. If an Ethernet frame has overhead of 64bytes including start and stop frames, and the data size is 2500 bytes. Determine the Ethernet frame efficiency.

# CHAPTER SIX

## DATA TRANSMISSION AND NETWORK CONNECTION MEDIA

### 6.1. Definition of Data Transmission Media

Transmission media is a pathway that carries the information from sender to receiver. We use different types of cables or waves to transmit data. Data is transmitted normally through electrical or electromagnetic signals. An electrical signal is in the form of current. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum Different Medias have different properties like bandwidth, delay, cost and ease of installation and maintenance. Transmission media is also called Communication channel. Transmission media is broadly classified into two groups. Wired or Guided Media or Bound Transmission Media and Wireless or Unguided Media or Unbound Transmission Media. (See the diagram below).



The data transmission capabilities of various Medias vary differently upon: Bandwidth. It refers to the data carrying capacity of a channel or medium. Higher bandwidth communication channels support higher data rates; Radiation. It refers to the leakage of signal from the medium due to undesirable electrical characteristics of the medium; Noise Absorption. It refers to the susceptibility of the media to external electrical noise that can cause distortion of data signal; Attenuation. It refers to loss of energy as signal propagates outwards. The amount of energy lost depends on frequency. Radiations and physical characteristics of media contribute to attenuation.

## **6.2. Transmission Channel Parameters**

Some parameters are required in description of transmission channel. Some of the parameter is discussed below.

**Bandwidth:** The range of frequencies contained in a composite signal is its bandwidth. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 2000 and 6000, its bandwidth is  $6000 - 2000$ , or 4000. The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal. The bandwidth determines the channel capacity.

**Bit Rate:** Most digital signals are non-periodic, and thus period and frequency are not appropriate characteristics. Bit rate is used to describe digital signals. The bit rate is the number of bits sent in 1s, expressed in bits per second (bps).

Assume we need to download text documents at the rate of 100 pages per minute. What is the required bit rate of the channel?



**Solution:**

A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires

8 bits, the bit rate is

$$100 \times 24 \times 80 \times 8 = 1,636,000 \text{ bps} = 1.636 \text{ Mbps}$$

A digital signal can have more than two levels. If a signal has L levels, each level needs  $\log_2 L$  bits. A digital signal with eight levels will need 3 bits per level. i.e.  $\log_2 8 = 3$

**Bit Length:** The bit length is the distance one bit occupies on the transmission medium.

$$\text{Bit length} = \text{propagation speed} \times \text{bit duration}$$

**Data Rate Limits:** one of the most important consideration in data communications is how fast we can send data, in bits per second over a channel. Data rate depends on three factors:

- a. The bandwidth available
- b. The level of the signals we use
- c. The quality of the channel (the level of noise)

Two theoretical formulas were developed to calculate the data rate: one by Nyquist for a noiseless channel, another by Shannon for a noisy channel.

**Noiseless Channel: Nyquist Bit Rate.** For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

$$\text{BitRate} = 2 \times \text{bandwidth} \times \log_2 L$$

In this formula, bandwidth is the bandwidth of the channel, L is the number of signal levels used to represent data, and Bit Rate is the bit rate in bits per second.

**Example:**

Consider a noiseless channel with a bandwidth of 6000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as:

$$\text{BitRate} = 2 \times 6000 \times \log_2 2 = 12000 \text{ bps}$$

**Noisy Channel:** In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

$$\text{Capacity} = \text{bandwidth} \times \log_2 (1 + \text{SNR})$$

In this formula, bandwidth is the bandwidth of the channel, SNR is the signal-to-noise ratio, and capacity is the capacity of the channel in bits per second. Note that in the Shannon formula there is no indication of the signal level, which means that no matter how many levels we have, we cannot achieve a data rate higher than the capacity of the channel. In other words, the formula defines a characteristic of the channel, not the method of transmission.

**Example:**

Consider an extremely noisy channel in which the value of the signal-to-noise ratio is almost zero. In other words, the noise is so strong that the signal is faint. For this channel the capacity C is calculated as:

$$C = B \log_2 (1 + \text{SNR}) = B \log_2 (1 + 0) = B \log_2 1 = B \times 0 = 0$$

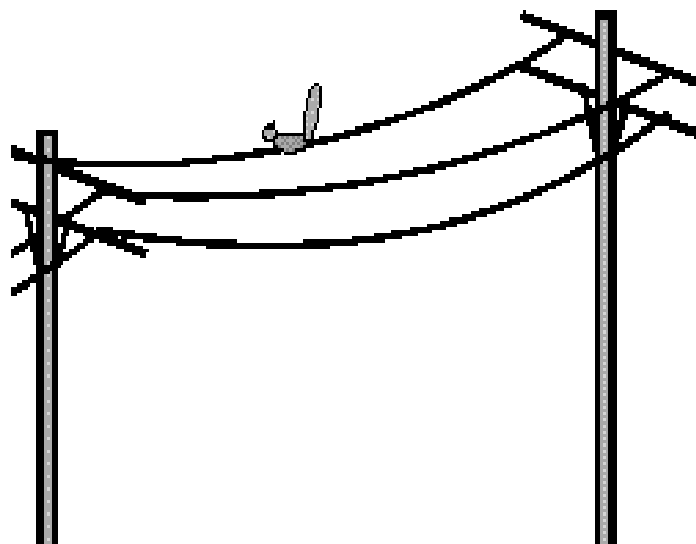
This means that the capacity of this channel is zero regardless of the bandwidth. In other words, we cannot receive any data through this channel.

### **6.3. Guided Transmission Media**

**Wired or Guided Media or Bound Transmission Media:** Bound transmission media are the cables that are tangible or have physical existence and are limited by the physical geography. Popular bound transmission media in use are twisted pair cable, co-axial cable and fiber optical cable. Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.

#### **6.3.1. Open Wire**

Open Wire is traditionally used to describe the electrical wire strung along power poles. There is a single wire strung between poles. No shielding or protection from noise interference is used. We are going to extend the traditional definition of Open Wire to include any data signal path without shielding or protection from noise interference. This can include multiconductor cables or single wires. This media is susceptible to a large degree of noise and interference and consequently not acceptable for data transmission except for short distances under 20 ft.



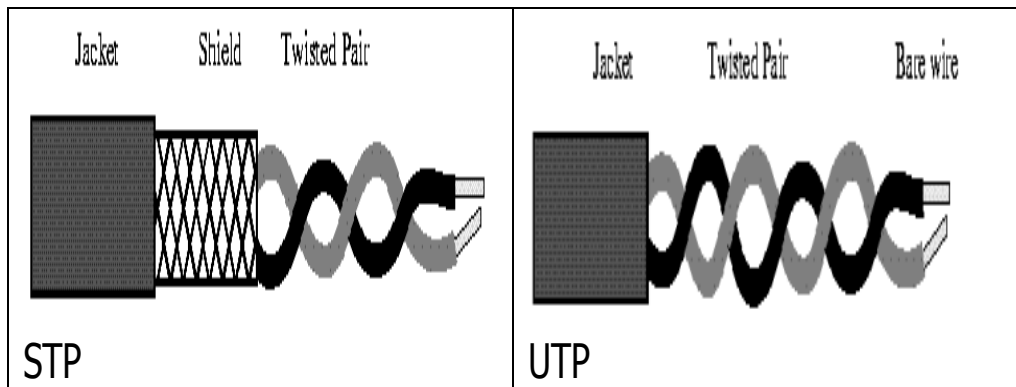
**Figure 22: Open wire Media**

### **6.3.2. Twisted Pair**

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in below figure. One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals. Each pair would consist of a wire used for the +ve data signal and a wire used for the -ve data signal. Any noise that appears on 1 wire of the pair would occur on the other wire. Because the wires are opposite polarities, they are 180 degrees out of phase (180 degrees - phasor definition of opposite polarity). When the noise appears on both wires, it cancels or nulls itself out at the receiving end. Twisted Pair cables are most effectively used in systems that use a balanced line method of transmission. The degree of reduction in noise interference is determined specifically by the number of turns per foot. Increasing the number of turns per foot reduces the noise interference. To further improve noise rejection, a foil or wire braid shield is woven around the twisted pairs. This "shield" can be woven around individual pairs or around a multi-pair conductor (several pairs).

### **Unshielded Versus Shielded Twisted-Pair Cable**

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.



**Figure 23: Twisted Pair Cables**

## **Applications**

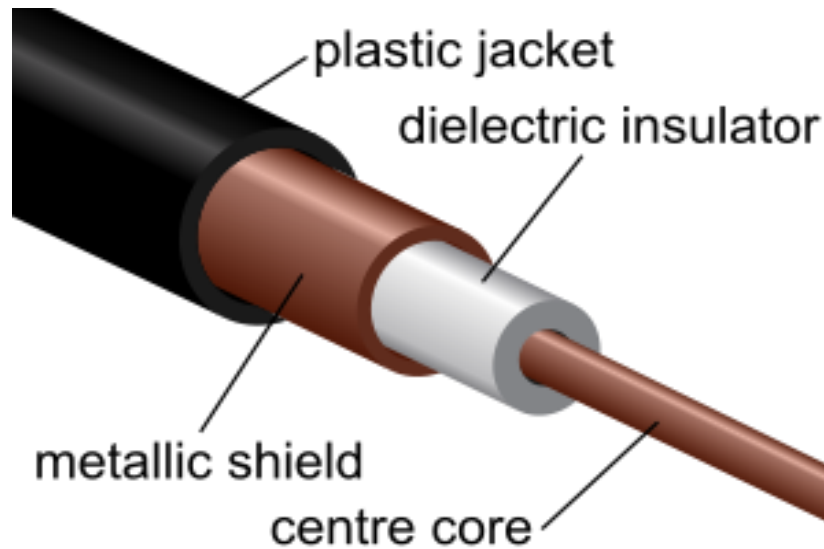
Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop—the line that connects subscribers to the central telephone office – commonly consists of unshielded twisted-pair cables. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.

### **6.3.3. Coaxial Cable**

Coaxial Cable consists of 2 conductors. The inner conductor is held inside an insulator with the other conductor woven around it providing a shield. An insulating protective coating called a jacket covers the outer conductor.

The outer shield protects the inner conductor from outside electrical signals. The distance between the outer conductor (shield) and inner conductor plus the type of material used for insulating the inner conductor determine the cable properties or impedance. Typical impedances for coaxial cables are 75ohms for Cable TV, 50 ohms for Ethernet Thinnet and Thicknet. The excellent control of the impedance

characteristics of the cable allow higher data rates to be transferred than Twisted Pair cable.



**Figure 24: Coaxial Cable**

#### **6.3.4. Optical Fiber**

##### **6.3.4.1. Description of Optical fiber cable**

Optical fiber is a cable that accepts and transports signals in the form of light. Optical fiber consists of thin glass fiber that can carry information at frequencies in the visible light spectrum. Optical fiber work on the principle that the core refracts the light and the cladding reflects the light. The core refracts the light and guides the light along its path. The cladding reflects any light back into the core and stops light from escaping through it - it bounds the media. The basic features of optical fiber are:

- The typical optical fiber consists of a very narrow strand of glass called the cladding.
- A typical core diameter is 62.5 microns.
- Typically cladding has a diameter of 125 minors. Coating the cladding is a protective coating consisting of plastic, it is called the jacket.

- The device generating the message has it in electromagnetic form (electrical signal); this has to be converted into light (i.e. optical signal) to send it on optic fiber cable. The process of converting light to electric signal is done on the receiving side.

#### **6.3.4.2. Advantages Optical Fiber**

Some of the advantages of using fiber optical cable are:

- i. **Small size and light weight:** The size of the optical fibers is very small. Therefore a large number of optical fibers can fit into a cable of small diameter.
- ii. **Easy availability and low cost:** The material used for the manufacturing of optical fibers is Silica glass. This material is easily available. So the optical fibers cost lower than the cables with metallic conductors.
- iii. **No electrical or electromagnetic interference:** Since the transmission takes place in the form of light rays the signal is not affected due to any electrical or electromagnetic Interference
- iv. **Large Bandwidth:** As the light rays have a very high frequency in GHz range, the bandwidth of the optical fiber is extremely large.
- v. **No cross talk inside the optical fiber cable.** Signal can be sent up to 100 times faster.

#### **6.3.4.3. Disadvantages of Optical Fiber**

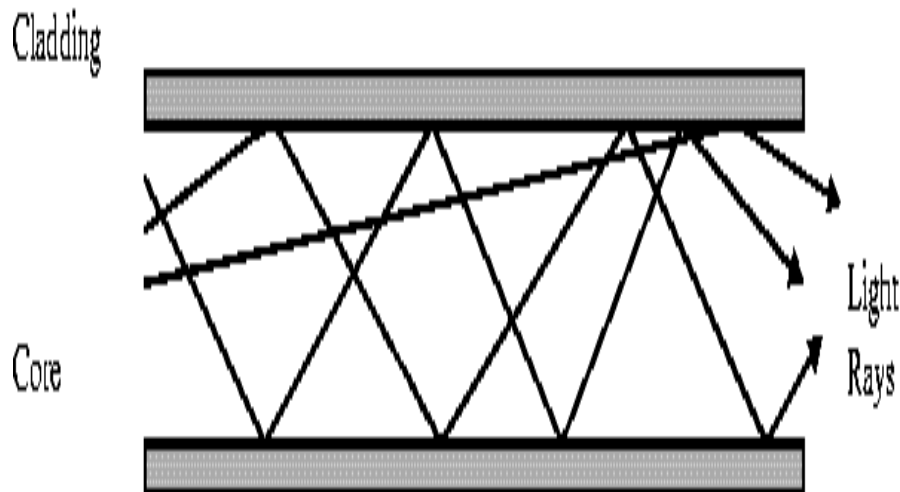
Disadvantages of optical fiber cable include the following.

- i. **Physical vibration will show up as signal noise.**
- ii. **Limited physical arc of cable.** Bend it too much & it will break.
- iii. **Difficult to splice**

#### 6.3.4.4. Optical Transmission Modes

There are 3 primary types of transmission modes using optical fiber.

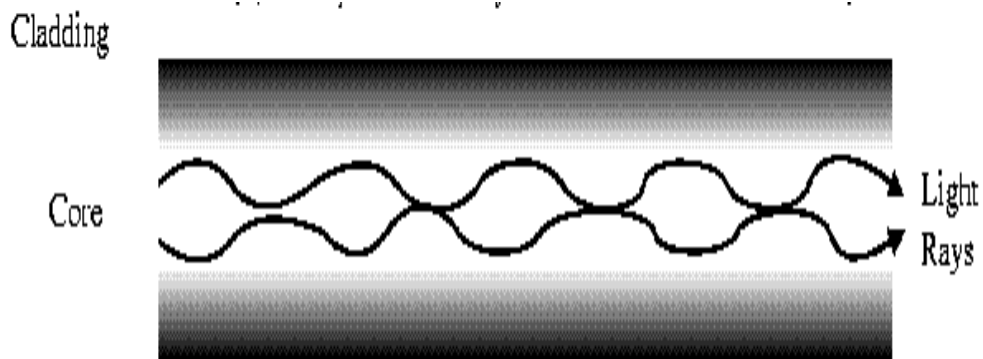
- i. **Step Index Mode:** Step Index has a large core the light rays tend to bounce around, reflecting off the cladding, inside the core. This causes some rays to take a longer or shorter path through the core. Some take the direct path with hardly any reflections while others bounce back and forth taking a longer path. The result is that the light rays arrive at the receiver at different times. The signal becomes longer than the original signal. LED light sources are used. Typical Core: 62.5 microns.



**Figure 25: Step Index Mode**

- ii. **Grade Index Mode:** Grade Index has a gradual change in the Core's Refractive Index. This causes the light rays to be gradually bent back into the core path. This is represented by a curved reflective path in the attached drawing. The result is a better receive signal than Step Index. LED light sources are used. Typical Core: 62.5 microns.

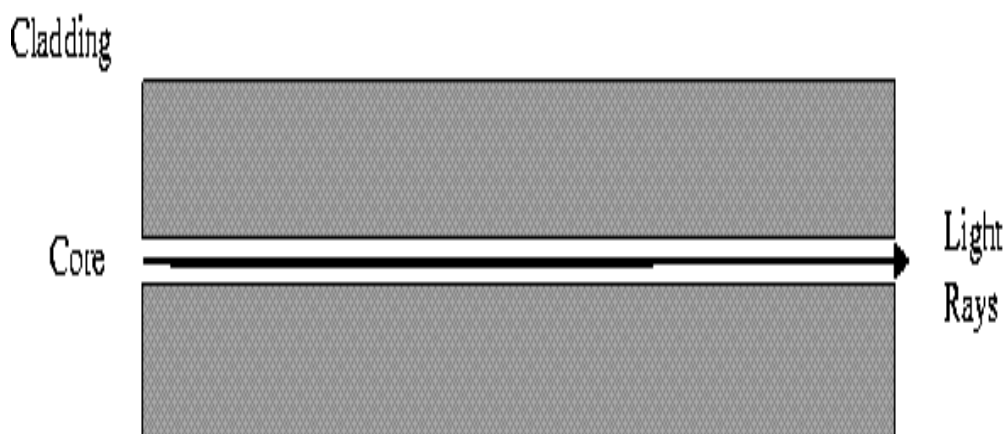




**Figure 26: Grade Index Mode**

**Note: Both Step Index and Graded Index allow more than one light source to be used (different colours simultaneously). Multiple channels of data can be run simultaneously.**

- iii. **Single Mode:** Single Mode has separate distinct Refractive Indexes for the cladding and core. The light ray passes through the core with relatively few reflections off the cladding. Single Mode is used for a single source of light (one colour) operation. It requires a laser and the core is very small: 9 microns.



**Figure 27: Single Mode**

## **6.4. Unguided Transmission Media (Wireless Transmission Medium)**

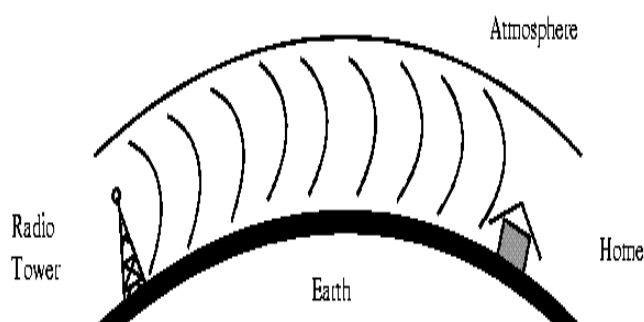
### **6.4.1. Description of Unguided Transmission Media**

In unguided Transmission Media data signals flows through the air. Wireless or Unguided Media or Unbound Transmission Media: Unbound transmission media are the ways of transmitting data without using any cables. These media are not bounded by physical geography. This type of transmission is called Wireless communication. Nowadays wireless communication is becoming popular. Wireless LANs are being installed in office and college campuses. This transmission uses Microwave, Radio wave, Infrared are some of popular unbound transmission media.

### **6.4.2. Wireless Signal Propagation**

Wireless signals travel or propagated in three ways:

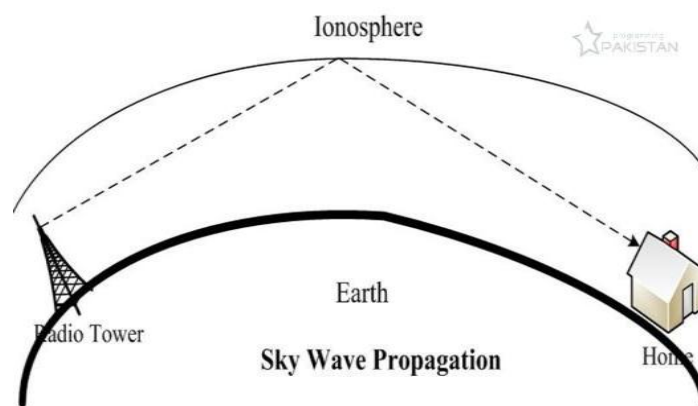
1. **Ground-wave propagation:** Ground Wave Propagation follows the curvature of the Earth. Ground Waves have carrier frequencies up to 2MHz. AM radio is an example of Ground Wave Propagation.



**Figure 28: Ground wave Propagation**

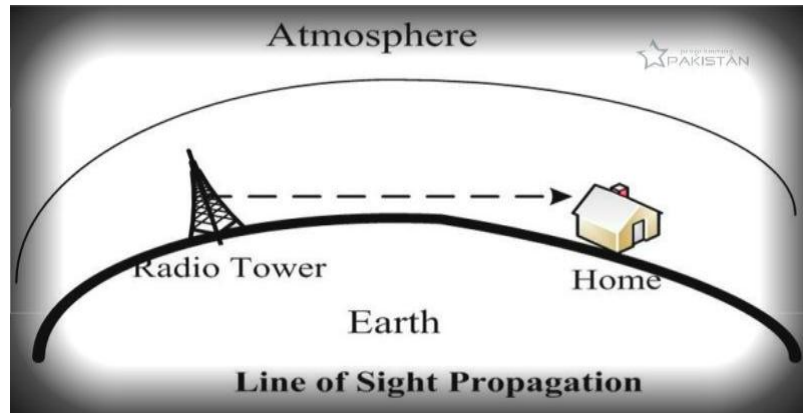
2. **Sky-wave propagation:** Ionospheric Propagation bounces off of the Earth's Ionospheric Layer in the

upper atmosphere. It is sometimes called Double Hop Propagation. It operates in the frequency range of 30 - 85MHz. Because it depends on the Earth's ionosphere, it changes with weather and time of day. The signal bounces off of the ionosphere and back to earth. Ham radios operate in this range. Characteristics of Sky Propagation are as follows: Signal reflected from ionized layer of atmosphere back down to earth; Signal can travel a number of hops, back and forth between ionosphere and earth's surface; Reflection effect caused by refraction.



**Figure 29: Sky Wave Propagation**

3. **Line-of-sight propagation:** Line of Sight Propagation transmits exactly in the line of sight. The receive station must be in the view of the transmit station. It is sometimes called Space Waves or Tropospheric Propagation. It is limited by the curvature of the Earth for ground based stations (100 km: horizon to horizon). Reflected waves can cause problems. Examples of Line of Sight Propagation are: FM Radio, Microwave and Satellite. Transmitting and receiving antennas must be within line of sight.



**Figure 30: Line of sight Propagation**

### **6.4.3. Types of Wireless Signal**

#### **6.4.3.1. Radio waves**

Electromagnetic wave ranging in frequencies between 3 KHz and 1GHz are normally called radio waves. Radio waves are omni-directional when an antenna transmits radio waves they are propagated in all directions. This means that sending and receiving antenna do not have to be aligned. A sending antenna can send waves that can be received by any receiving antenna. Radio waves particularly those waves that propagate in sky mode, can travel long distances. This makes radio waves a better choice for long-distance broadcasting such as AM radio. Radio waves particularly those of low and medium frequencies can penetrate walls. It is an advantage because; an AM radio can receive signals inside a building. It is the disadvantage because we cannot isolate a communication to first inside or outside a building.

#### **6.4.3.2. Microwave**

Microwave transmission is line of sight transmission. The Transmit station must be in visible contact with the receive station. This sets a limit on the distance between stations depending on the local geography. Typically the line of sight due to the Earth's curvature is only 50 km to the horizon. Repeater stations must be placed so the data signal can hop,

skip and jump across the country. Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional; when an antenna transmits microwaves they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. Microwaves propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall, the curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate using microwaves. Repeaters are often needed for long distance communication. Very high frequency microwaves cannot penetrate walls. Parabolic dish antenna and horn antenna are used for this means of transmission.

Microwaves operate at high operating frequencies of 3 to 10 GHz. This allows them to carry large quantities of data due to the large bandwidth.

### **Advantages**

- i. They require no right of way acquisition between towers.
- ii. They can carry high quantities of information due to their high operating frequencies.
- iii. Low cost land purchase: each tower occupies small area.
- iv. High frequency/short wavelength signals require small antenna.

### **Disadvantages**

- i. Attenuation by solid objects: birds, rain, snow and fog.
- ii. Reflected from flat surfaces like water and metal.

- iii. Diffracted (split) around solid objects
- iv. Refracted by atmosphere, thus causing beam to be projected away from receiver.

#### **6.4.3.3. Infrared**

Infrared signals with frequencies ranges from 300 GHz to 400 GHz can be used for short range communication. Infrared signals, having high frequencies, cannot penetrate walls. This helps to prevent interference between one system and another. Infrared Transmission in one room cannot be affected by the infrared transmission in another room. Infrared band has an excellent potential for data transmission. Transfer digital data is possible with a high speed with a very high frequency. There are number of computer devices which are used to send the data through infrared medium e.g. keyboard mice, PCs and printers. There are some manufacturers provide a special part called the IrDA port that allows a wireless keyboard to communicate with a PC.

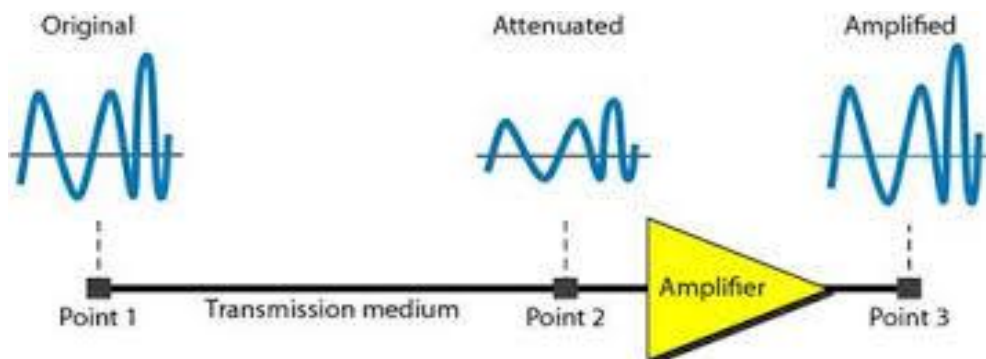
### **6.5. Transmission Media Problems and Impairment**

Data is transmitted through transmission medium which are not perfect. The imperfection causes signal impairment. Due to the imperfection error is introduced in the transmitted data i.e. the original signal at the beginning of the transmission is not the same as the signal at the Receiver. Some of the transmission media/impairment problems are:

#### **6.5.1. Attenuation Distortion**

Attenuation results in loss of energy. When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium. The electrical energy in the signal may convert to heat. To compensate for this loss, amplifiers are used to amplify the signal. Figure below shows

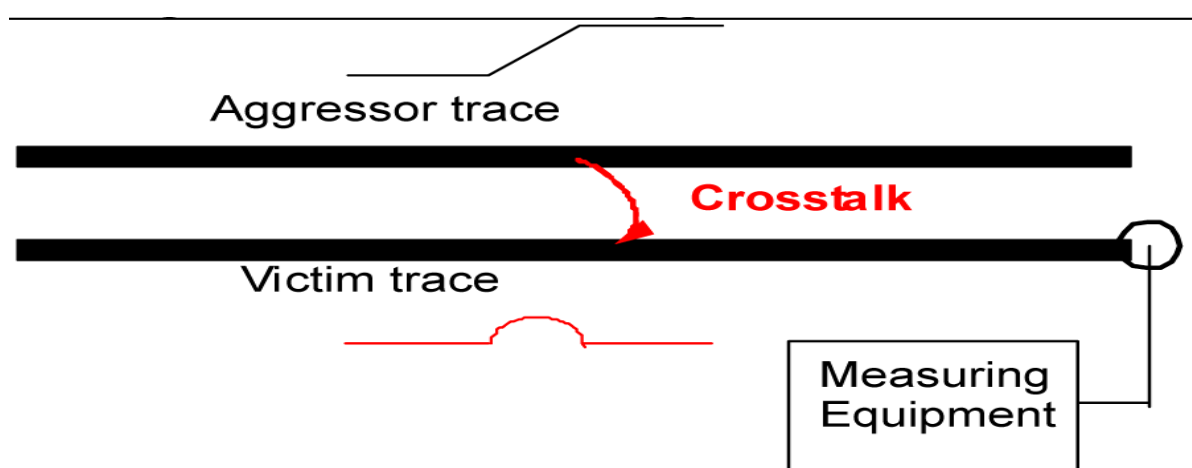
the effect of attenuation and amplification. The loss of signal or attenuation is measured at the receiving end and compared to a standard reference frequency.



**Figure 31: effect of attenuation and amplification.**

### 6.5.2. Crosstalk

Crosstalk is when one line induces a signal into another line. In voice communications, we often hear this as another conversation going on in the background. In digital communication, this can cause severe disruption of the data transfer. Cross talk can be caused by overlapping of bands in a multiplexed system or by poor shielding of cables running close to one another. There are no specific communications standards applied to the measurement of crosstalk.



**Figure 32: Crosstalk impairment**

### **6.5.3. Echo or Signal Return**

All media have a preferred termination condition for perfect transfer of signal power. The signal arriving at the end of a transmission line should be fully absorbed otherwise it will be reflected back down the line to the sender and appear as an Echo. Echo Suppressors are often fitted to transmission lines to reduce this effect. Normally during data transmission, these suppressors must be disabled or they will prevent return communication in full duplex mode. Echo suppressors are disabled on the phone line if they hear carrier for 400ms or more. If the carrier is absent for 100 mSec, the echo suppressor is re-enabled. Echo Cancellers are currently used in Modems to replicate the echo path response and then combine the results to eliminate the echo. Thus no signal interruption is necessary.

### **6.5.4. Noise**

Noise is any unwanted signal that is mixed or combined with the original signal during transmission. Due to noise the original signal is altered and signal received is not same as the one sent. Noise is sharp quick spikes on the signal caused from electromagnetic interference, lightning, sudden power switching, electromechanical switching, etc. These appear on the telephone line as clicks and pops which are not a problem for voice communication but can appear as a loss of data or even as wrong data bits during data transfers. Impulse noise has duration of less than 1 mSec and their effect is dissipated within 4mSec.

## **6.6. Review Questions**

1. Explain briefly the following:
  - i. Attenuation
  - ii. Propagation delay



- iii. Crosstalk
- iv. Echo
- 3. Compare Guided and Unguided transmission with relevant examples
- 4. Compare coaxial and twisted pair cable transmission based on the following:
  - a. Attenuation
  - b. Propagation delay
  - c. Crosstalk
  - d. Echo
- 5. Describe with diagram the following transmission mode in optical fiber
  - a) Grade index
  - b) Step index
  - c) Single mode
- 7. What are the reasons why Telecommunication Companies are investing in Optical fiber transmission?
- 8. Describe with diagram:
  - a) Ground wave propagation
  - b) Ionospheric
  - c) Line of sight
- 9. Highlights 4 major types of microwave transmission.

# **CHAPTER SEVEN**

## **COMPUTER NETWORK SECURITY**

### **7.1. Description of Network Security Treat**

Network security has become increasingly important with the growth in the number and importance of networks. Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses. Network security is expensive. It is also very important. An institution network would possibly be subject to more stringent security requirements than a similarly-sized corporate network, because of its likelihood of storing personal and confidential information of network users, the danger of which can be compounded if any network users are minors. A great deal of attention must be paid to network services to ensure all network content is appropriate for the network community it serves.

### **7.2. Security Requirements and Attacks**

#### **7.2.1. Network Security Requirements**

To understand the types of threats to security that exist, we need to have a definition of security requirements. Computer and network security address four requirements:

1. **Confidentiality:** Requires that data only be accessible by authorized parties. This type of access includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object.

2. **Integrity:** Requires that only authorized parties can modify data. Modification includes writing, changing, changing status, deleting, and creating.
3. **Availability:** Requires that data are available to authorized parties.
4. **Authenticity:** Requires that a host or service be able to verify the identity of a user.

### **7.2.2. Network Security Threats**

Some of the network security is discussed below

#### **Attacks against IP**

A number of attacks against IP are possible. Typically, these exploit the fact that IP does not perform a robust mechanism for authentication, which is proving that a packet came from where it claims it did. A packet simply claims to originate from a given address, and there isn't a way to be sure that the host that sent the packet is telling the truth. This isn't necessarily a weakness, per se, but it is an important point, because it means that the facility of host authentication has to be provided at a higher layer on the ISO/OSI Reference Model. Today, applications that require strong host authentication (such as cryptographic applications) do this at the application layer. An attack against IP includes:

1. **IP Spoofing:** This is where one host claims to have the IP address of another. Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address, this is a useful technique to an attacker: he can send packets to a host, perhaps causing it to take some sort of action. Additionally, some applications allow login based on the IP address of the person making the request (such as the Berkeley r-commands).

- 2. IP Session Hijacking:** This is a relatively sophisticated attack, first described by Steve Bellovin. This is very dangerous, however, because there are now toolkits available in the underground community that allow otherwise unskilled bad-guy-wannabes to perpetrate this attack. IP Session Hijacking is an attack whereby a user's session is taken over, being in the control of the attacker. If the user was in the middle of email, the attacker is looking at the email, and then can execute any commands he wishes as the attacked user. The attacked user simply sees his session dropped, and may simply login again, perhaps not even noticing that the attacker is still logged in and doing things.

### **Denial-of-Service**

DoS (Denial-of-Service) attacks are probably the nastiest, and most difficult to address. These are the nastiest, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, without also refusing legitimate requests for service. The premise of a DoS attack is simple: send more requests to the machine than it can handle. There are toolkits available in the underground community that make this a simple matter of running a program and telling it which host to blast with requests. 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. If the host is able to answer 20 requests per second, and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests, much less any legitimate requests (hits on the web site running there, for example). Such attacks were fairly common in late 1996 and early 1997, but are now becoming less popular. Some things that can be

done to reduce the risk of being stung by a denial of service attack include

- Not running your visible-to-the-world servers at a level too close to capacity
- Using packet filtering to prevent obviously forged packets from entering into your network address space. Obviously forged packets would include those that claim to come from your own hosts, addresses reserved for private networks as defined in RFC 1918 and the loopback network (127.0.0.0).
- Keeping up-to-date on security-related patches for your hosts' operating systems.

### **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 your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

### **Executing Commands Illicitly**

It's obviously undesirable for an unknown and untrusted person to be able to execute commands on your server machines. There are two main classifications of the severity 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 all the access that an attacker needs. On the other hand, an attacker might wish to make configuration changes to a host (perhaps changing its IP address, putting a start-up script in

place to cause the machine to shut down every time it's started, or something similar). In this case, the attacker will need to gain administrator privileges on the host.

### **Confidentiality Breaches**

We need to examine the threat model: what is it that you're trying to protect yourself 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 (perhaps in the form of PR, or obtaining information that can be used against the company, etc.)

While many of the perpetrators of these sorts of break-ins are merely thrill-seekers interested in nothing more than to see a shell prompt for your computer on their screen, there are those who are more malicious, as we'll consider next. (Additionally, keep in mind that it's possible that someone who is normally interested in nothing more than the thrill could be persuaded to do more: perhaps an unscrupulous competitor is willing to hire such a person to hurt you.)

### **Destructive Behavior**

Among the destructive sorts of break-ins and attacks, there are two major categories.

- a) **Data Diddling:** The data diddler is likely the worst sort, since the fact of a break-in might not be immediately obvious. Perhaps he's toying with the numbers in your spreadsheets, or changing the dates in your projections and plans. Maybe he's changing the account numbers for the auto-deposit of certain paychecks. In any case, rare is the case when you'll come in to work one day, and simply know that something is wrong. An accounting procedure might

turn up a discrepancy in the books three or four months after the fact. Trying to track the problem down will certainly be difficult, and once that problem is discovered, how can any of your numbers from that time period be trusted? How far back do you have to go before you think that your data is safe?

- b) **Data Destruction:** Some of those perpetrators are simply twisted jerks who like to delete things. In these cases, the impact on your computing capability -- and consequently your business -- can be nothing less than if a fire or other disaster caused your computing equipment to be completely destroyed.

### **7.3. Network Security Threats Prevention**

#### **7.3.1. Encryption Method**

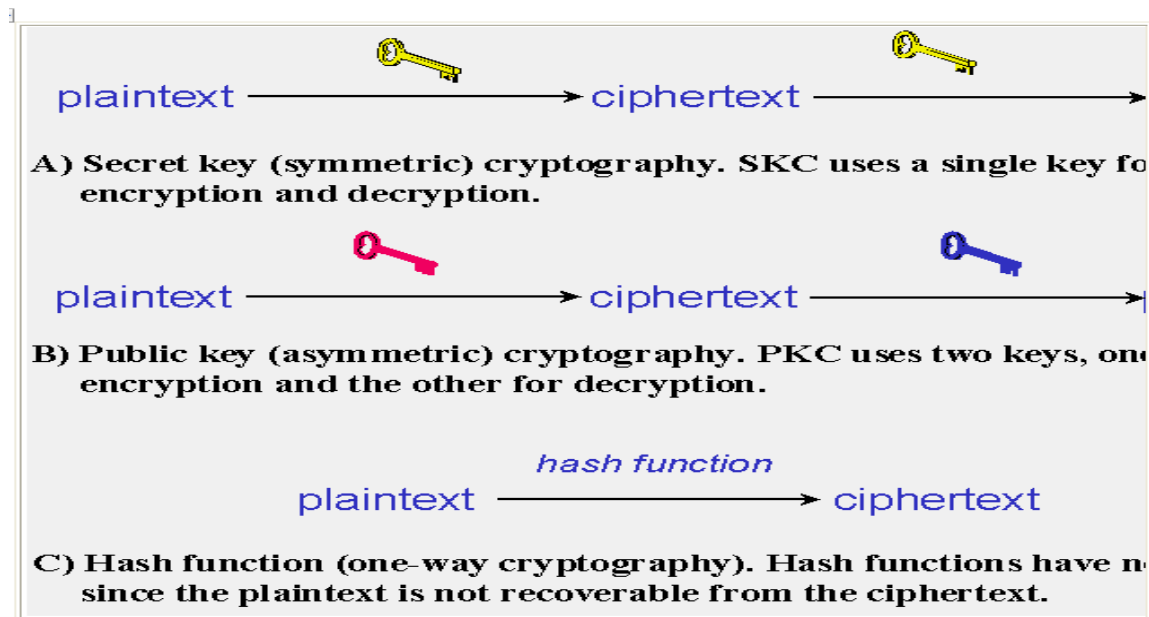
The universal technique for providing confidentiality for transmitted data is symmetric encryption. A symmetric encryption scheme has five components.

- a. **Plaintext:** This is the original message or data that is fed into the algorithm as input.
- b. **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- c. **Secret key:** The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- d. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
- e. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

## Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 33):

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information



**Figure 33: Cryptographic Algorithms**

### Secret Key Cryptography

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 33A, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the



message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

Stream ciphers come in several flavors but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the keystream as a function of the previous  $n$  bits in the keystream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the  $n$ -bit keystream it is. One problem is error propagation; a garbled bit in transmission will result in  $n$  garbled bits at the receiving side. Synchronous stream ciphers generate the keystream in a fashion independent of the message stream but by using the same keystream generation function at sender and receiver. While stream ciphers do not propagate transmission errors, they are, by their nature, periodic so that the keystream will eventually repeat.

Block ciphers can operate in one of several modes; the following four are the most important:

- **Electronic Codebook (ECB)** mode is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a ciphertext block. Two identical plaintext blocks, then, will always generate the same ciphertext block. Although this is the most common mode of block ciphers, it is susceptible to a variety of brute-force attacks.
- **Cipher Block Chaining (CBC)** mode adds a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusively-ORed (XORed) with the previous ciphertext block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same ciphertext.
- **Cipher Feedback (CFB)** mode is a block cipher implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register the same size as the block, encrypted, and the block transmitted. At the receiving side, the ciphertext is decrypted and the extra bits in the block (i.e., everything above and beyond the one byte) are discarded.
- **Output Feedback (OFB)** mode is a block cipher implementation conceptually similar to a synchronous stream cipher. OFB prevents the same plaintext block from generating the same ciphertext block by using an internal feedback mechanism that is independent of both the plaintext and ciphertext bitstreams.

## **Public-Key Cryptography**

PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to

computer whereas their inverse function is relatively difficult to compute. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme. Suppose Yekini wants to send Adebari a message. Yekini encrypts some information using Adebari's public key; Adebari decrypts the ciphertext using his private key. This method could be also used to prove who sent a message; Yekini, for example, could encrypt some plaintext with his private key; when Adebari decrypts using Yekini's public key, he knows that Yekini sent the message and Yekini cannot deny having sent the message (non-repudiation).

### **Hash Functions**

Hash functions, also called message digests and one-way encryption, and are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

### **Why Three Encryption Techniques?**

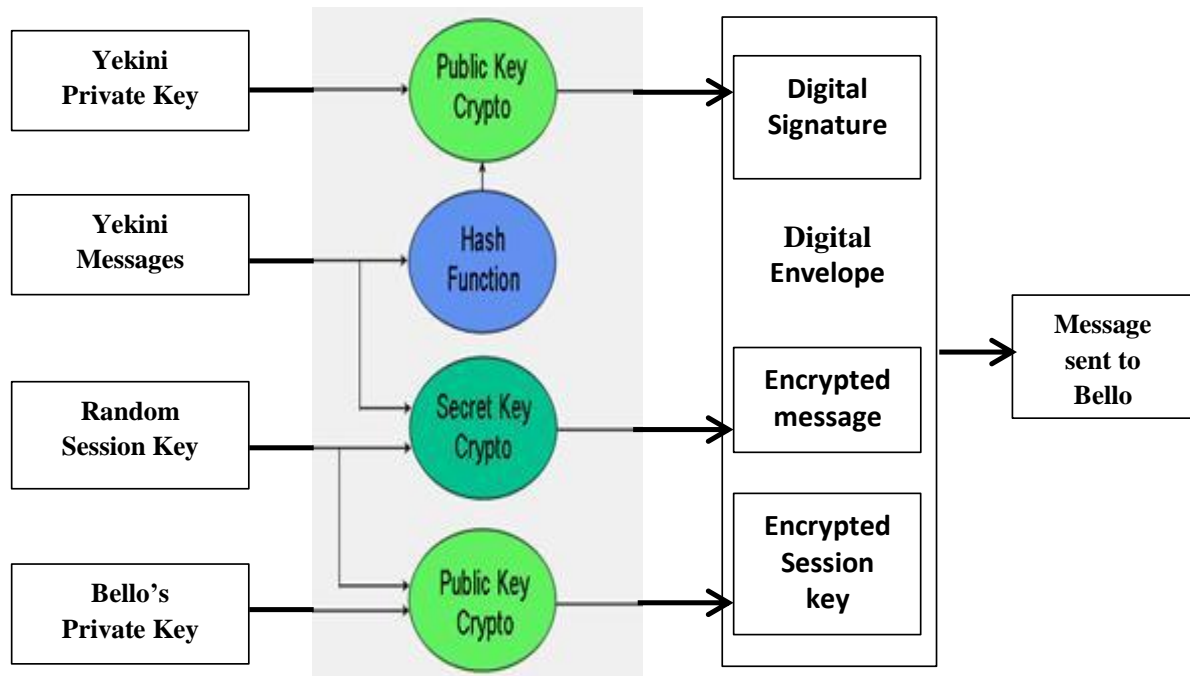
So, why are there so many different types of cryptographic schemes? Why can't we do everything we need with just one? The answer is that each scheme is optimized for some specific application(s).

- Hash functions, for example, are well-suited for ensuring data integrity because any change made to

the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages will yield the same hash value, data integrity is ensured to a high degree of confidence.

- Secret key cryptography, on the other hand, is ideally suited to encrypting messages, thus providing privacy and confidentiality. The sender can generate a session key on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message.
- Public-key cryptography asymmetric schemes can also be used for non-repudiation and user authentication; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography.

Figure 34 puts all of this together and shows how a hybrid cryptographic scheme combines all of these functions to form a secure transmission comprising digital signature and digital envelope. In this example, the sender of the message is Yekini and the receiver is Bello.



**Figure 34: hybrid cryptographic scheme**

A digital envelope comprises an encrypted message and an encrypted session key. Yekini uses secret key cryptography to encrypt his message using the session key, which he generates at random with each session. Yekini then encrypts the session key using Bello's public key. The encrypted message and encrypted session key together form the digital envelope. Upon receipt, Bello recovers the session secret key using his private key and then decrypts the encrypted message.

The digital signature is formed in two steps. First, Yekini computes the hash value of her message; next, he encrypts the hash value with his private key. Upon receipt of the digital signature, Bello recovers the hash value calculated by Yekini by decrypting the digital signature with Yekini's public key. Bello can then apply the hash function to Yekini's original message, which he has already decrypted. If the resultant hash value is not the same as the value supplied by Yekini, then Bello knows that the message has been altered; if the

hash values are the same, Bello should believe that the message he received is identical to the one that Yekini sent. This scheme also provides nonrepudiation since it proves that Yekini sent the message; if the hash value recovered by Bello using Yekini's public key proves that the message has not been altered, then only Yekini could have created the digital signature. Bello also has proof that he is the intended receiver; if he can correctly decrypt the message, then he must have correctly decrypted the session key meaning that his is the correct private key.

### **7.3.2. Firewall**

A firewall is simply a group of components that collectively form a barrier between two networks. A firewall is a hardware or software system that prevents unauthorized access to or from a network. They can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All data entering or leaving the Intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.

#### **Types of Firewall**

Firewalls can be divided into five basic types:

- i. Packet filters
- ii. Stateful Inspection
- iii. Proxys
- iv. Dynamic
- v. Kernel firewall

The divisions above however are not quite well defined as most modern firewalls have a mix of abilities that place them in more than one of the categories listed.

To simplify the most commonly used firewalls, expert breaks them down into three categories:

- i. Application firewalls
- ii. Network layer firewalls
- iii. Proxy firewall

## **NETWORK LAYER FIREWALLS**

Network layer firewalls generally make their decisions based on the source address, destination address and ports in individual IP packets. A simple router is the traditional network layer firewall, since it is not able to make particularly complicated decisions about what a packet is actually talking to or where it actually came from. Modern network layer firewalls have become increasingly more sophisticated, and now maintain internal information about the state of connections passing through them at any time.

One important difference about many network layer firewalls is that they route traffic directly through them, which means in order to use one, you either need to have a validly-assigned IP address block or a private Internet address block. Network layer firewalls tend to be very fast and almost transparent to their users.

## **APPLICATION LAYER FIREWALLS**

Application layer firewalls defined, are hosts running proxy servers, which permit no traffic directly between networks, and they perform elaborate logging and examination of traffic passing through them. Since proxy applications are simply software running on the firewall, it is a good place to do lots of logging and access control. Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other, after having passed through an application that effectively masks the origin of the initiating connection. However, run-of-the-mill network firewalls can't

properly defend applications. As Michael Cobb explains, application-layer firewalls offer Layer 7 security on a more granular level, and may even help organizations get more out of existing network devices.

In some cases, having an application in the way may impact performance and may make the firewall less transparent. Early application layer firewalls are not particularly transparent to end-users and may require some training. However, more modern application layer firewalls are often totally transparent. Application layer firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network layer firewalls.

The future of firewalls sits somewhere between both network layer firewalls and application layer firewalls. It is likely that network layer firewalls will become increasingly aware of the information going through them, and application layer firewalls will become more and more transparent. The end result will be kind of a fast packet-screening system that logs and checks data as it passes through.

## **PROXY FIREWALLS**

Proxy firewalls offer more security than other types of firewalls, but this is at the expense of speed and functionality, as they can limit which applications your network can support. Why are they more secure? Unlike stateful firewalls, or application layer firewalls, which allow or block network packets from passing to and from a protected network, traffic does not flow through a proxy. Instead, computers establish a connection to the proxy, which serves as an intermediary, and initiate a new network connection on behalf of the request. This prevents direct connections between systems on either side of the firewall and makes it harder for an attacker to discover where the network is, because they will



never receive packets created directly by their target system. Proxy firewalls also provide comprehensive, protocol-aware security analysis for the protocols they support. This allows them to make better security decisions than products that focus purely on packet header information.

#### **7.4. Review Questions**

2. Describe briefly any 5 network security threats you know
3. What are the precautions to reduce the risk of being stung by a denial of service in computer Network?
4. Describe briefly the term cryptograph
5. Describe briefly firewall and its 3 major types
6. What are the major security requirements in network environment
7. What are the basic rules used to generate public and private keys in RSA algorithm
8. For RSA algorithm we have  $p = 5$ ,  $q = 11$ ,  $n = 55$  and  $(p-1)(q-1) = 40$ . Find the public and private key, resulting ciphertext and verify the decryption.
9. Describe with diagram the use of hybrid cryptograph algorithm that combines secret, public, and hash function for Mr. A to send information to B.
10. Compare the strength of secret, public, and hash function cryptograph algorithm.

# CHAPTER EIGHT

## ANALOG VS DIGITAL TRANSMISSION

### 8.1. Analog and Digital Data

Data can be analog or digital. Analog data refers to information that is continuous; digital data refers to information that has discrete states. For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous. On the other hand, a digital clock that reports the hours and the minutes will change suddenly from 11:57 to 11:58. (See figure 35)



(a) Digital watch



(b) Analog watch

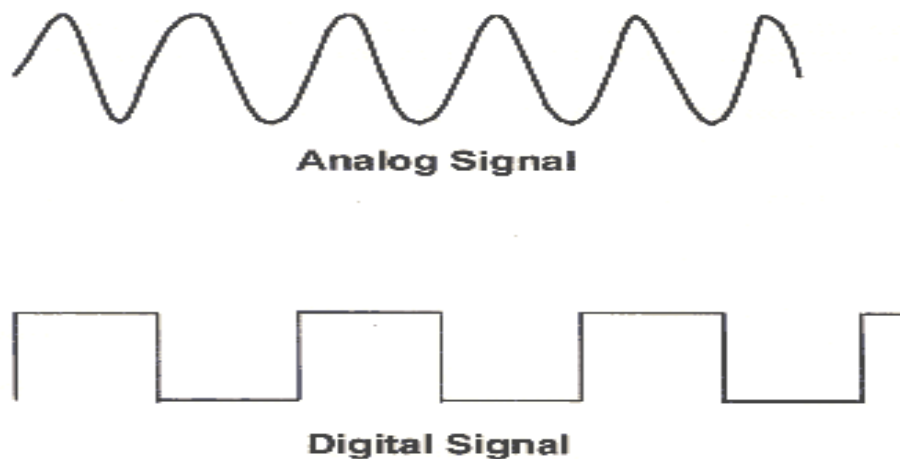
**Figure 35: Analog vs analog representation**

Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal.

Digital data take on discrete values. For example, data are stored in computer memory in the form of 0s and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

## 8.2. Analog and Digital Signals

Like the data they represent, signals can be either analog or digital. An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path. A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0. Figure 36 illustrates an analog signal and a digital signal. The curve representing the analog signal passes through an infinite number of points. The vertical lines of the digital signal, however, demonstrate the sudden jump that the signal makes from value to value.



**Figure 36: Analog vs Digital Signal**

Both analog and digital signals can take one of two forms: periodic or nonperiodic. A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A nonperiodic

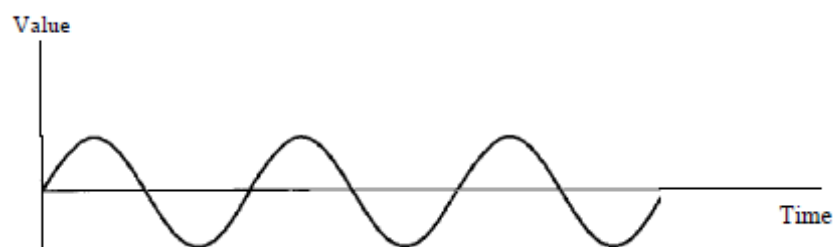
signal changes without exhibiting a pattern or cycle that repeats over time. Both analog and digital signals can be periodic or nonperiodic. In data communications, we frequently use periodic analog signals (because they need less bandwidth), and nonperiodic digital signals (because they can represent variation in data).

### 8.3. Periodic Analog Signals

Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves.

#### Sine Wave

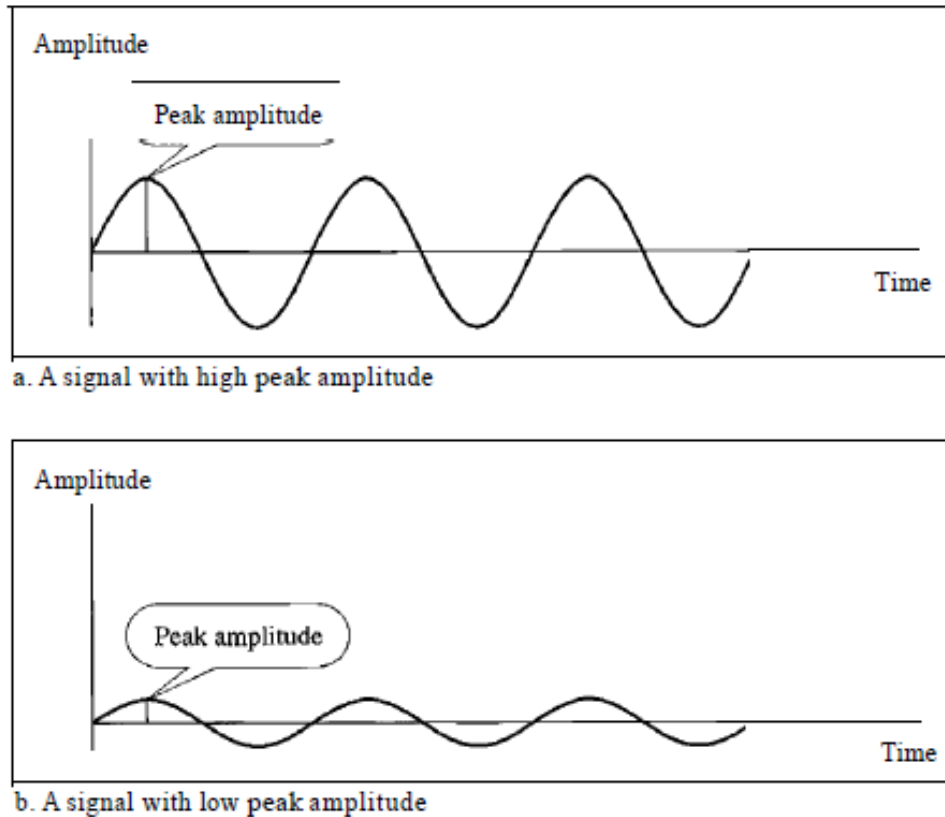
The sine wave is the most fundamental form of a periodic analog signal. When we visualize it as a simple oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow. Figure 37 shows a sine wave. Each cycle consists of a single arc above the time axis followed by a single arc below it.



**Figure 37: A sine wave**

A sine wave can be represented by three parameters: the peak amplitude, the frequency, and the phase. These three parameters fully describe a sine wave. The peak amplitude of a signal is the absolute value of its highest intensity, proportional to the energy it carries. For electric signals, peak amplitude is normally measured in volts. Figure 38

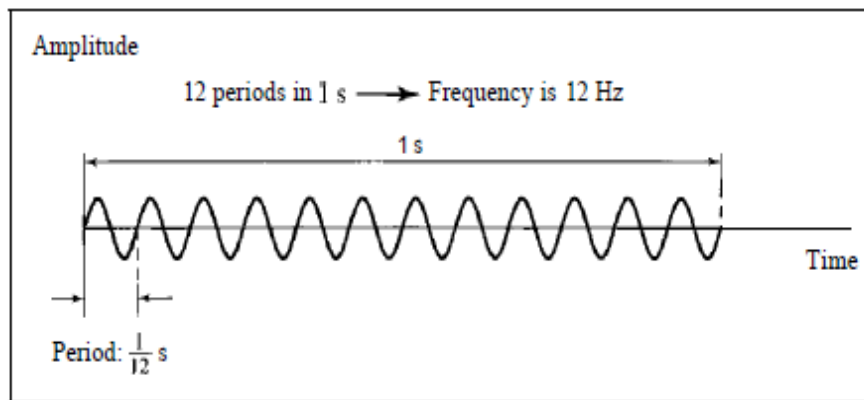
shows two signals and their peak amplitudes. This discrepancy is due to the fact that these are root mean square (rms) values. The signal is squared and then the average amplitude is calculated. The peak value is equal to  $2^{1/2}$  rms value.



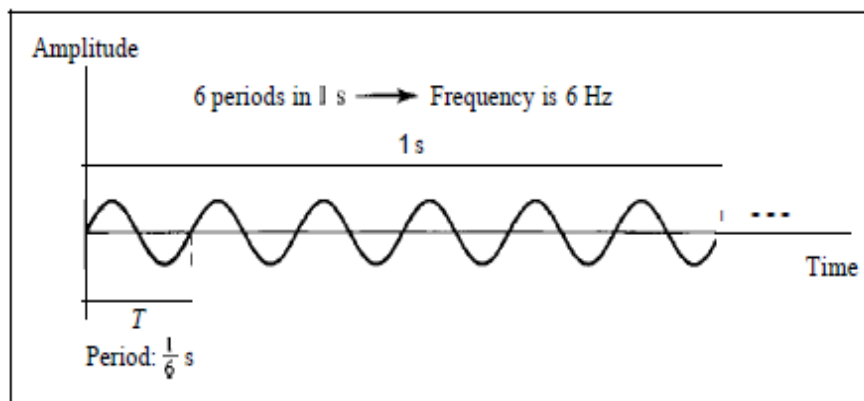
**Figure 38: Two signals with the same phase and frequency, but different amplitudes**

### ***Period and Frequency***

Period refers to the amount of time, in seconds; a signal needs to complete 1 cycle. Frequency refers to the number of periods in 1s. Note that period and frequency are just one characteristic defined in two ways. Period is the inverse of frequency, and frequency is the inverse of period, as the following formulas show  $F = 1/T$  and  $T = 1/f$ . *Period is formally expressed in seconds. Frequency is formally expressed in Hertz (Hz), which is cycle per second.*



a. A signal with a frequency of 12 Hz



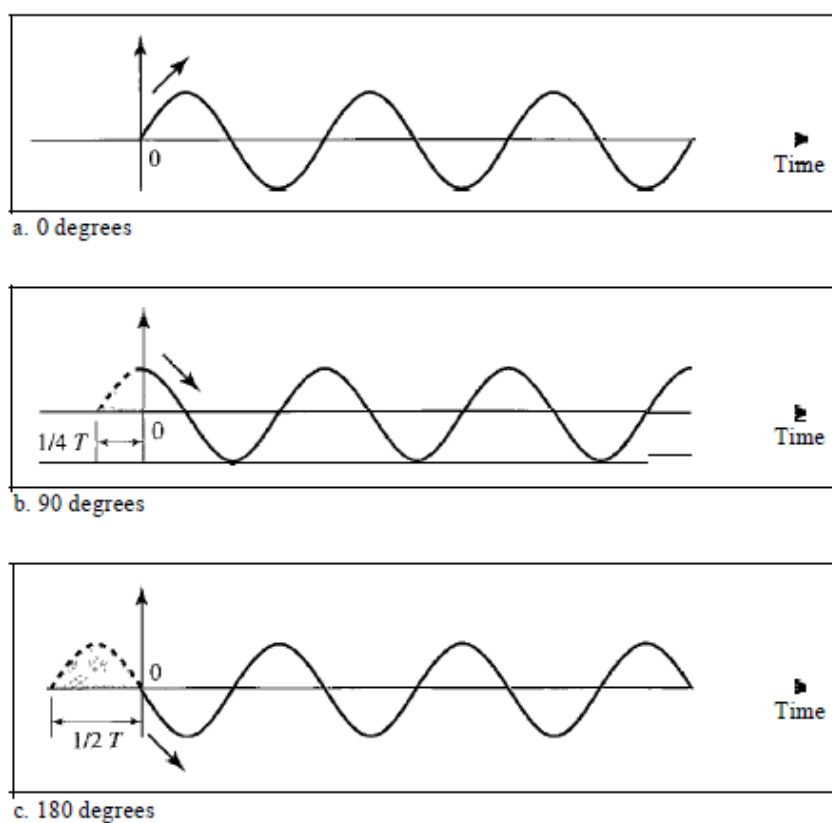
b. A signal with a frequency of 6 Hz

**Figure 39: 2 signals with the same phase and frequency, but different frequencies**

If a signal does not change at all, its frequency is zero. If a signal changes instantaneously, its frequency is infinite. What if a signal does not change at all? What if it maintains a constant voltage level for the entire time it is active? In such a case, its frequency is zero. Conceptually, this idea is a simple one. If a signal does not change at all, it never completes a cycle, so its frequency is aHz. But what if a signal changes instantaneously? What if it jumps from one level to another in no time? Then its frequency is infinite. In other words, when a signal changes instantaneously, its period is zero; since frequency is the inverse of period; in this case, the frequency is  $1/0$ , or infinite (unbounded).

## Phase

The term phase describes the position of the waveform relative to time 0. If we think of the wave as something that can be shifted backward or forward along the time axis, phase describes the amount of that shift. It indicates the status of the first cycle. Phase is measured in degrees or radians [ $360^\circ$  is  $2\pi$  rad;  $1^\circ$  is  $2\pi/360$  rad, and 1 rad is  $360/(2\pi)$ ]. A phase shift of  $360^\circ$  corresponds to a shift of a complete period; a phase shift of  $180^\circ$  corresponds to a shift of one-half of a period; and a phase shift of  $90^\circ$  corresponds to a shift of one-quarter of a period (see Figure 40).



**Figure 40: 3 sine waves with the same amplitude and frequency, but different phases**

Looking at Figure 40, we can say that: (1) A sine wave with a phase of  $0^\circ$  starts at time 0 with a zero amplitude. The amplitude is increasing. (2) A sine wave with a phase of  $90^\circ$

starts at time 0 with a peak amplitude. The amplitude is decreasing. (3) A sine wave with a phase of  $180^\circ$  starts at time 0 with a zero amplitude. The amplitude is decreasing.

Another way to look at the phase is in terms of shift or offset. We can say that

(1) A sine wave with a phase of  $0^\circ$  is not shifted. (2) A sine wave with a phase of  $90^\circ$  is shifted to the left by  $1/4$  cycle. However, note that the signal does not really exist before time 0. (3) A sine wave with a phase of  $180^\circ$  is shifted to the left by  $1/2$  cycle. However, note that the signal does not really exist before time 0.

**Example**

A sine wave is offset  $1/4$  cycle with respect to time 0. What is its phase in degrees and radians?

**Solution**

We know that 1 complete cycle is  $360^\circ$ . Therefore,  $1/4$  cycle is  $1/4 \times 360 = 90^\circ = 90 \times 2\pi$

$360\text{rad} = (2\pi/4)\text{rad} = 1.57\text{rad}$

## **Wavelength**

Wavelength is another characteristic of a signal traveling through a transmission medium. Wavelength binds the period or the frequency of a simple sine wave to the propagation speed of the medium. While the frequency of a signal is independent of the medium, the wavelength depends on both the frequency and the medium. Wavelength is a property of any type of signal. In data communications, we often use wavelength to describe the transmission of light in an optical fiber. The wavelength is the distance a simple signal can travel in one period. Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal. However, since period and frequency are related to each other, if we represent wavelength by  $\lambda$ ,

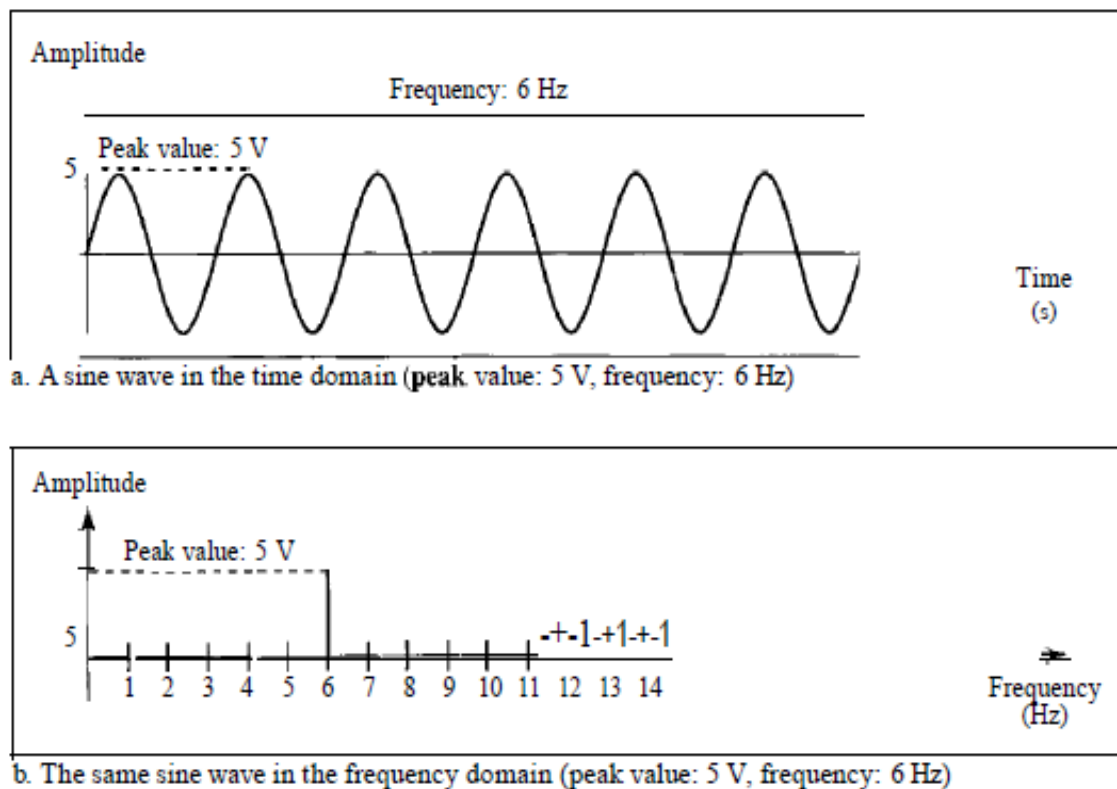


propagation speed by  $c$  (speed of light), and frequency by  $f$ , we get:

$$\lambda = c/f$$

## Time and Frequency Domains

A sine wave is comprehensively defined by its amplitude, frequency, and phase. We have been showing a sine wave by using what is called a time-domain plot. The time-domain plot shows changes in signal amplitude with respect to time (it is an amplitude-versus-time plot). Phase is not explicitly shown on a time-domain plot. To show the relationship between amplitude and frequency, we can use what is called a frequency-domain plot. A frequency-domain plot is concerned with only the peak value and the frequency. Changes of amplitude during one period are not shown. Figure 41 shows a signal in both the time and frequency domains.



**Figure 41: The time-domain and frequency-domain plots of a sine wave**

## **Composite Signals**

So far, we have focused on simple sine waves. Simple sine waves have many applications in daily life. We can send a single sine wave to carry electric energy from one place to another. For example, the power company sends a single sine wave with a frequency of 60 Hz to distribute electric energy to houses and businesses. As another example, we can use a single sine wave to send an alarm to a security center when a burglar opens a door or window in the house. In the first case, the sine wave is carrying energy; in the second, the sine wave is a signal of danger.

If we had only one single sine wave to convey a conversation over the phone, it would make no sense and carry no information. We would just hear a buzz. We send a composite signal to communicate data. A composite signal is made of many simple sine waves. French mathematician Jean-Baptiste Fourier showed that any composite signal is actually a combination of simple sine waves with different frequencies, amplitudes, and phases.

A composite signal can be periodic or nonperiodic. A periodic composite signal can be decomposed into a series of simple sine waves with discrete frequencies that have integer values (1, 2, 3, and so on). A nonperiodic composite signal can be decomposed into a combination of an infinite number of simple sine waves with continuous frequencies, frequencies that have real values. If the composite signal is periodic, the decomposition gives a series of signals with discrete frequencies; if the composite signal is nonperiodic, the decomposition gives a combination of sine waves with continuous frequencies.

### **Example**

A nonperiodic composite signal has a bandwidth of 200 kHz, with a middle frequency of 140 kHz and peak amplitude of 20

V. The two extreme frequencies have amplitude of 0. Draw the frequency domain of the signal.

**Solution**

Let  $f_1$  = lowest frequency, and  $f_2$  = highest frequency.

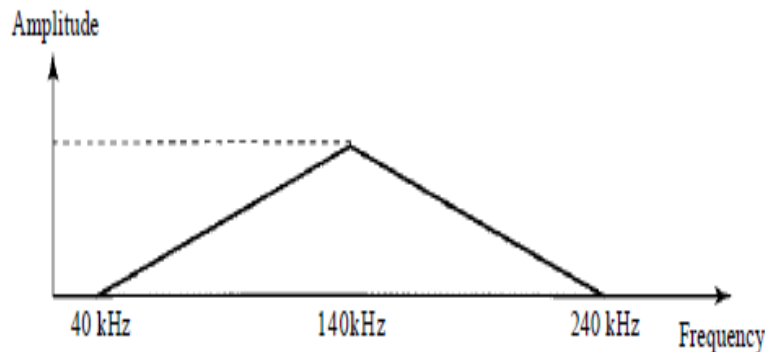
Therefore

$$f_1 - f_2 = 200 \text{ kHz} \text{ ---- eqn1}$$

$$(f_1 + f_2) = 140 \text{ kHz} \text{ ---- eqn2}$$

Solve for  $f_1$  and  $f_2$  from eqn1 and eqn2

Then the lowest frequency is 40 kHz and the highest is 240 kHz. Figure 42 shows the frequency domain and the bandwidth.

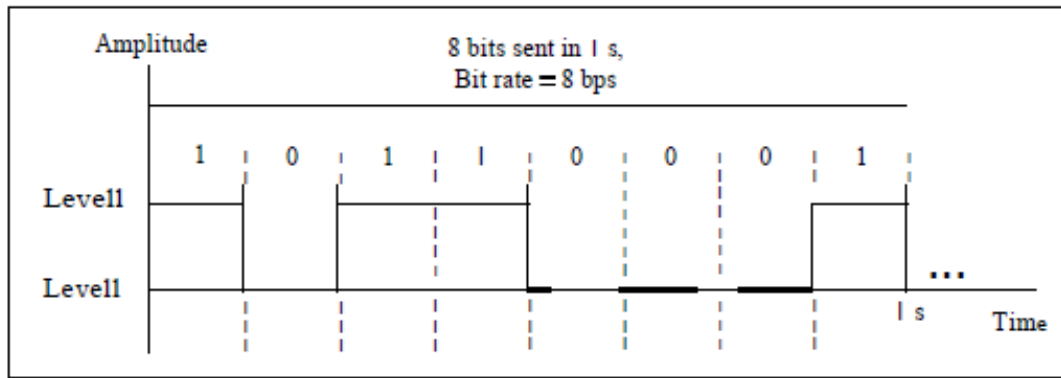


**Figure 42: solution for the above**

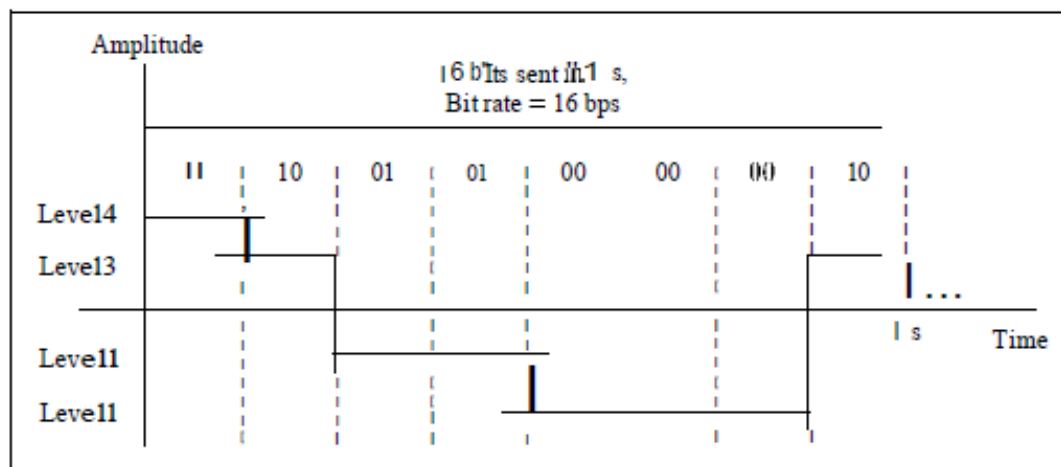
#### **8.4. Digital Signals**

In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level. Figure 43 shows two signals, one with two levels and the other with four. We send 1 bit per level in part (a) of the figure and 2 bits per level in part (b) of the figure 43. In general, if a signal has  $L$  levels, each level needs  $\log_2 L$  bits. For example if

a digital signal has sixteen levels. How many bits are needed per level? We calculate the number of bits from the formula  
 Number of bits per level =  $\log_2 16 = 4$ .



a. A digital signal with two levels



b. A digital signal with four levels

**Figure 43: Two digital signals: one with two signal levels and the other with four signal levels**

## 8.5. Review Questions

1. Define the relationship between period and frequency?
2. Explain how a composite signal can be decomposed into its individual frequencies?
3. Given the frequencies listed below, calculate the corresponding periods.
  - a. 24Hz
  - b. 8 MHz
  - c. 140 KHz

4. Given the following periods, calculate the corresponding frequencies.
  - a. 5 s
  - b. 14 micro seconds
  - c. 220 nano second
5. What is the phase shift for the for the following?
  - a. A sine wave with the maximum amplitude at time zero
  - b. A sine wave with maximum amplitude after  $1/4$  cycle
  - c. A sine wave with zero amplitude after  $3/4$  cycle and increasing
6. What is the bandwidth of a signal that can be decomposed into five sine waves with frequencies at 0, 25, 60, 120, and 240 Hz? All peak amplitudes are the same. Hence draw the bandwidth.

## CHAPTER NINE

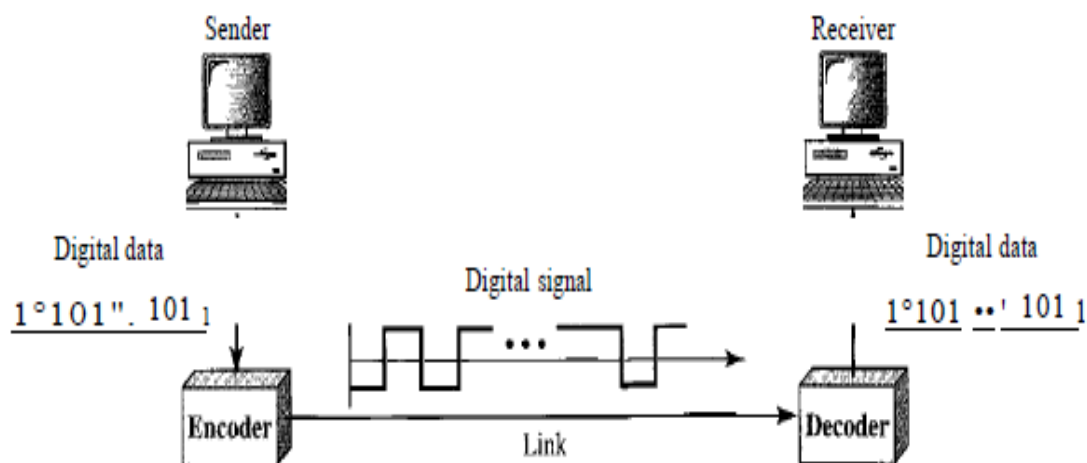
# DIGITAL DATA TO DIGITAL SIGNAL CONVERSION

### 10.1. Digital Signal Representation

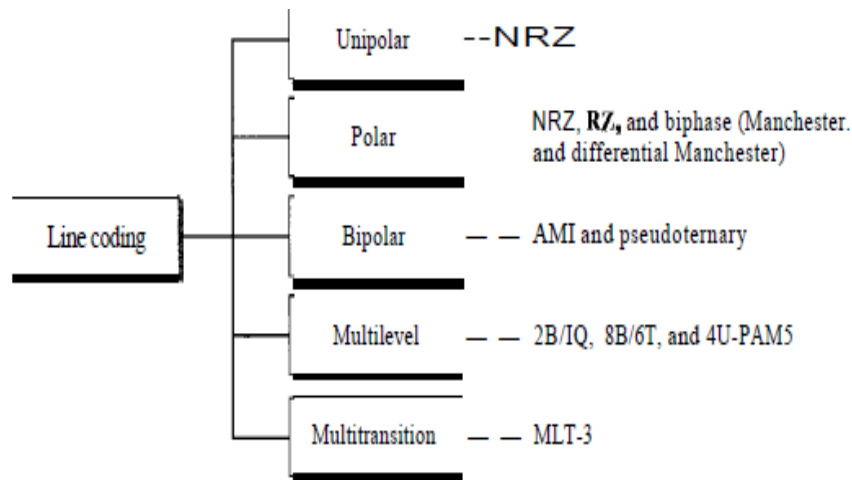
Signals that represent data can be digital or analog. In this chapter, we see how we can represent digital data by using digital signals. The conversion involves three techniques: line coding, block coding, and scrambling.

### 10.2. Line Coding

Line coding is the process of converting digital data to digital signals. We assume that data, in the form of text, numbers, graphical images, audio, or video, are stored in computer memory as sequences of bits. Line coding converts a sequence of bits to a digital signal. At the sender, digital data are encoded into a digital signal; at the receiver, the digital data are recreated by decoding the digital signal. Figure 44 shows the process. There are five types of line coding schemes available see figure 45.



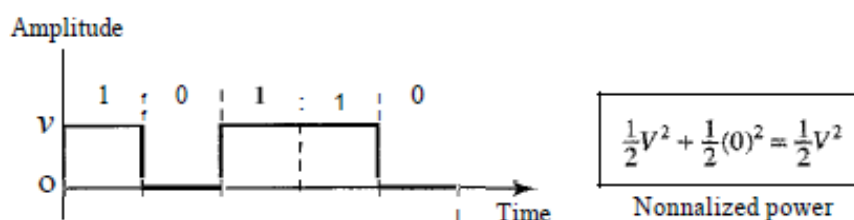
**Figure 44: Line coding and decoding**



**Figure 45: Types of Line Coding**

### 10.2.1. Unipolar Coding

In a unipolar scheme, all the signal levels are on one side of the time axis, either above or below. NRZ (Non-Return-to-Zero) traditionally, a unipolar scheme was designed as a non-return-to-zero (NRZ) scheme in which the positive voltage defines bit 1 and the zero voltage defines bit 0. It is called NRZ because the signal does not return to zero at the middle of the bit. Figure 47 show a unipolar NRZ scheme.



**Figure 46: Unipolar NRZ**

### 10.2.2. Polar Coding

In polar schemes, the voltages are on the both sides of the time axis. For example, the voltage level for 0 can be positive and the voltage level for 1 can be negative.

**Non-Return-to-Zero (NRZ)** In polar NRZ encoding, we use two levels of voltage amplitude. We can have two versions of polar NRZ: NRZ-L and NRZ-I, as shown in Figure 47, the figure

also shows the value of  $r$ , the average baud rate, and the bandwidth. In the first variation, NRZ-L (NRZ-Level), the level of the voltage determines the value of the bit. In the second variation, NRZ-I (NRZ-Invert), the change or lack of change in the level of the voltage determines the value of the bit. If there is no change, the bit is 0; if there is a change, the bit is 1.

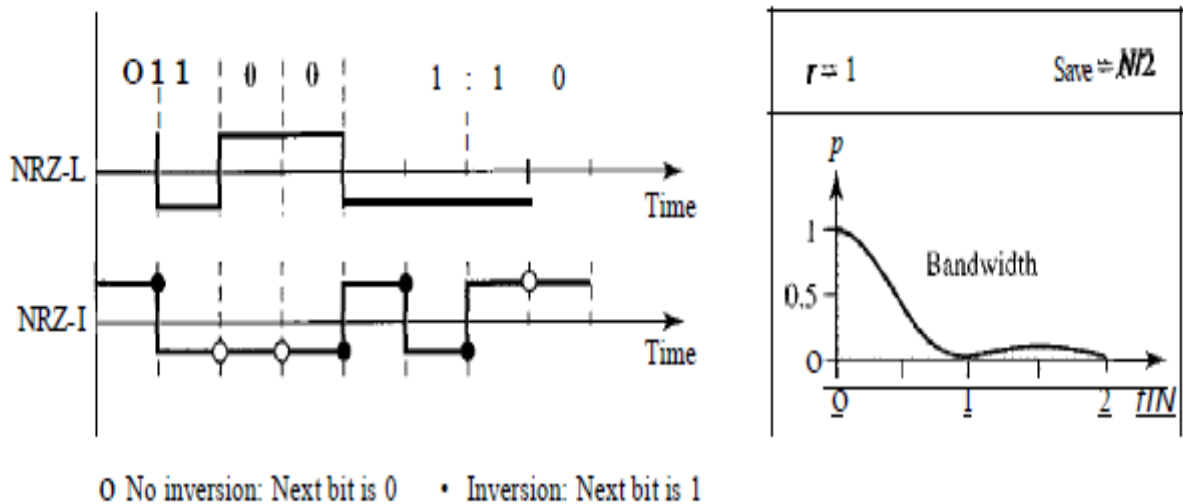
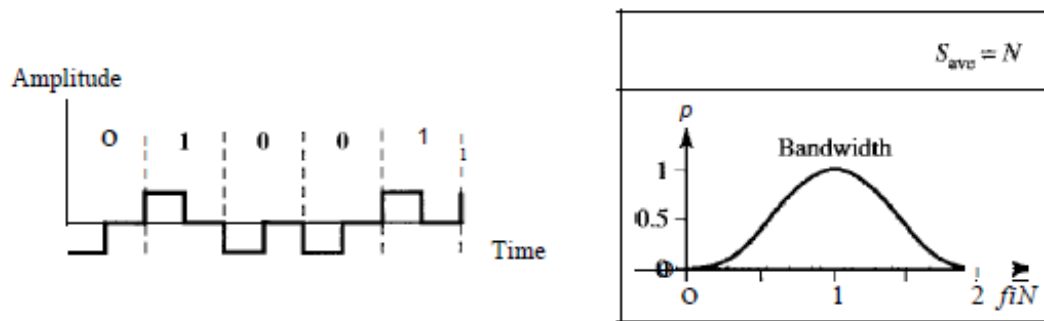


Figure 47: Polar Coding

**Return to Zero (RZ)** The main problem with NRZ encoding occurs when the sender and receiver clocks are not synchronized. The receiver does not know when one bit has ended and the next bit is starting. One solution is the return-to-zero (RZ) scheme, which uses three values: positive, negative, and zero. In RZ, the signal changes not between bits but during the bit. In Figure 48 we can see that the signal goes to 0 in the middle of each bit. It remains there until the beginning of the next bit. The main disadvantage of RZ encoding is that it requires two signal changes to encode a bit and therefore occupies greater bandwidth. The same problem we mentioned, a sudden change of polarity resulting in all 0s interpreted as 1s and all 1s interpreted as 0, still exist here, but there is no DC component problem. Another problem is the complexity: RZ uses three levels of voltage,



which is more complex to create and discern. As a result of all these deficiencies, the scheme is not used today. Instead, it has been replaced by the better-performing Manchester and differential Manchester schemes.



**Figure 48: Polar RZ type coding**

### **Manchester and Differential Manchester**

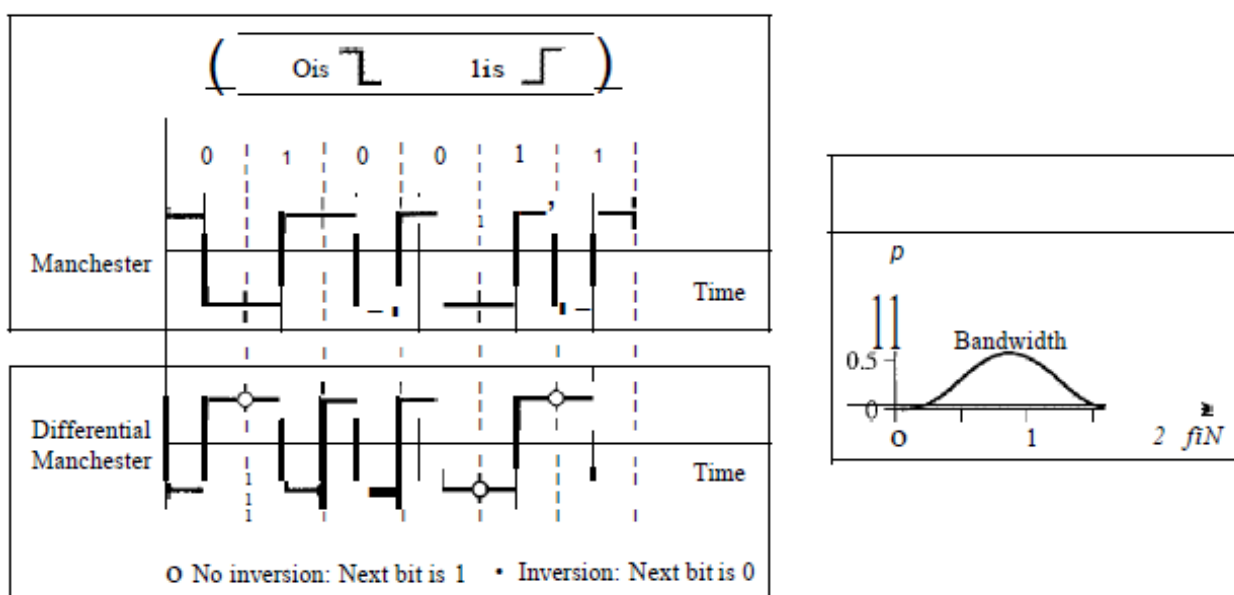
The awareness of RZ (transition at the middle of the bit) and the awareness of NRZ-L are combined into the Manchester scheme. In Manchester encoding, the period of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half. The transition at the middle of the bit provides synchronization. Differential Manchester, on the other hand, combines the ideas of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition; if the next bit is 1, there is none. Figure 49 shows both Manchester and differential Manchester encoding. In Manchester and differential Manchester encoding, the transition at the middle of the bit is used for synchronization.

The Manchester scheme overcomes several problems associated with NRZ-L, and differential Manchester overcomes several problems associated with NRZ-I. First, there is no baseline wandering. There is no DC component because each bit has a positive and negative voltage

contribution. The only drawback is the signal rate. The signal rate for

Manchester and differential Manchester is double that for NRZ. The reason is that there is always one transition at the middle of the bit and maybe one transition at the end of each bit. Figure 4.8 shows both Manchester and differential Manchester encoding schemes.

Manchester and differential Manchester schemes are also called biphase. The minimum bandwidth of Manchester and differential Manchester is 2 times that of NRZ.



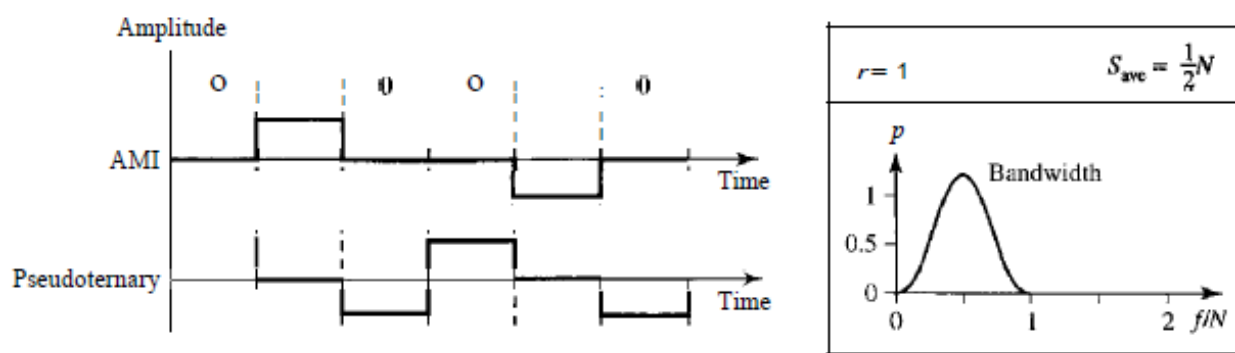
**Figure 49: *Manchester and differential Manchester Coding***

### 10.2.3. Bipolar Schemes

In bipolar encoding (sometimes called multilevel binary), there are three voltage levels: positive, negative, and zero. The voltage level for one data element is at zero, while the voltage level for the other element alternates between positive and negative. In bipolar encoding, we use three levels: positive, zero, and negative. AMI and Pseudoternary Figure 50 show two variations of bipolar encoding: AMI and

pseudoternary. A common bipolar encoding scheme is called bipolar alternate mark inversion (AMI). In the term alternate mark inversion, the word mark comes from telegraphy and means 1. So AMI means alternate 1 inversion. A neutral zero voltage represents binary 0. Binary 1s are represented by alternating positive and negative voltages. A variation of AMI encoding is called pseudoternary in which the 1 bit is encoded as a zero voltage and the 0 bit is encoded as alternating positive and negative voltages. The bipolar scheme was developed as an alternative to NRZ. The bipolar scheme has the same signal rate as NRZ, but there is no DC component. The NRZ scheme has most of its energy concentrated near zero frequency, which makes it unsuitable for transmission over channels with poor performance around this frequency. The concentration of the energy in bipolar encoding is around frequency  $N/2$ . Figure 50 shows the typical energy concentration for a bipolar scheme. One may ask why we do not have DC component in bipolar encoding. We can answer this question by using the Fourier transform, but we can also think about it naturally. If we have a long sequence of 1s, the voltage level alternates between positive and negative; it is not constant. Therefore, there is no DC component. For a long sequence of 0s, the voltage remains constant, but its amplitude is zero, which is the same as having no DC component. In other words, a sequence that creates a constant zero voltage does not have a DC component.

AMI is commonly used for long-distance communication, but it has a synchronization problem when a long sequence of 0s is present in the data. Scrambling technique can solve this problem

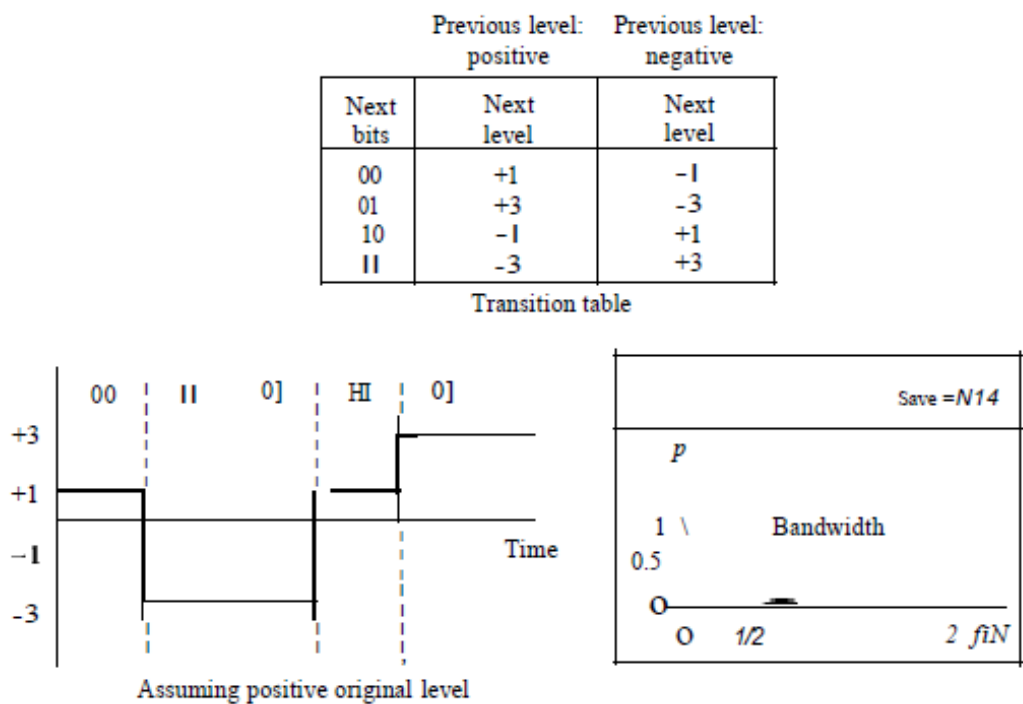


**Figure 50: Bipolar Scheme**

#### 10.2.4. Multilevel Schemes

The desire to increase the data speed or decrease the required bandwidth has resulted in the creation of many schemes. The goal is to increase the number of bits per baud by encoding a pattern of  $m$  data elements into a pattern of  $n$  signal elements. We only have two types of data elements (0s and 1s), which means that a group of  $m$  data elements can produce a combination of  $2^m$  data patterns. We can have different types of signal elements by allowing different signal levels. If we have  $L$  different levels, then we can produce  $Ln$  combinations of signal patterns. If  $2^m = Ln$ , then each data pattern is encoded into one signal pattern. If  $2^m < Ln$ , data patterns occupy only a subset of signal patterns. The subset can be carefully designed to prevent baseline wandering, to provide synchronization, and to detect errors that occurred during data transmission. Data encoding is not possible if  $2^m > Ln$  because some of the data patterns cannot be encoded. The code designers have classified these types of coding as  $mBnL$ , where  $m$  is the length of the binary pattern,  $B$  means binary data,  $n$  is the length of the signal pattern, and  $L$  is the number of levels in the signaling. A letter is often used in place of  $L$ :  $B$  (binary) for  $L = 2$ ,  $T$  (ternary) for  $L = 3$ , and  $Q$  (quaternary) for  $L = 4$ . The first two letters define the data pattern, and the second two define the signal pattern. In

*mBnL* schemes, a pattern of *m* data elements is encoded as a pattern of *n* signal elements in which  $2^m$  less than or equal to  $L^n$ . 2BIQ The first *mBnL* scheme we discuss, two binary, one quaternary (2BIQ), uses data patterns of size 2 and encodes the 2-bit patterns as one signal element belonging to a four-level signal. In this type of encoding  $m = 2$ ,  $n = 1$ , and  $L = 4$  (quaternary). Figure 51 shows an example of a 2B1Q signal. The average signal rate of 2BIQ is  $S = N/4$ . This means that using 2BIQ, we can send data 2 times faster than by using NRZ-L. However, 2B IQ uses four different signal levels, which means the receiver has to discern four different thresholds. The reduced bandwidth comes with a price. There are no redundant signal patterns in this scheme because  $2^2 = 4^1$ .



**Figure 51: Multilevel: 2B1Q scheme**

### 10.2.5. Multiline Transmission

NRZ-I and differential Manchester are classified as differential encoding but use two transition rules to encode binary data (no inversion, inversion). If we have a signal with

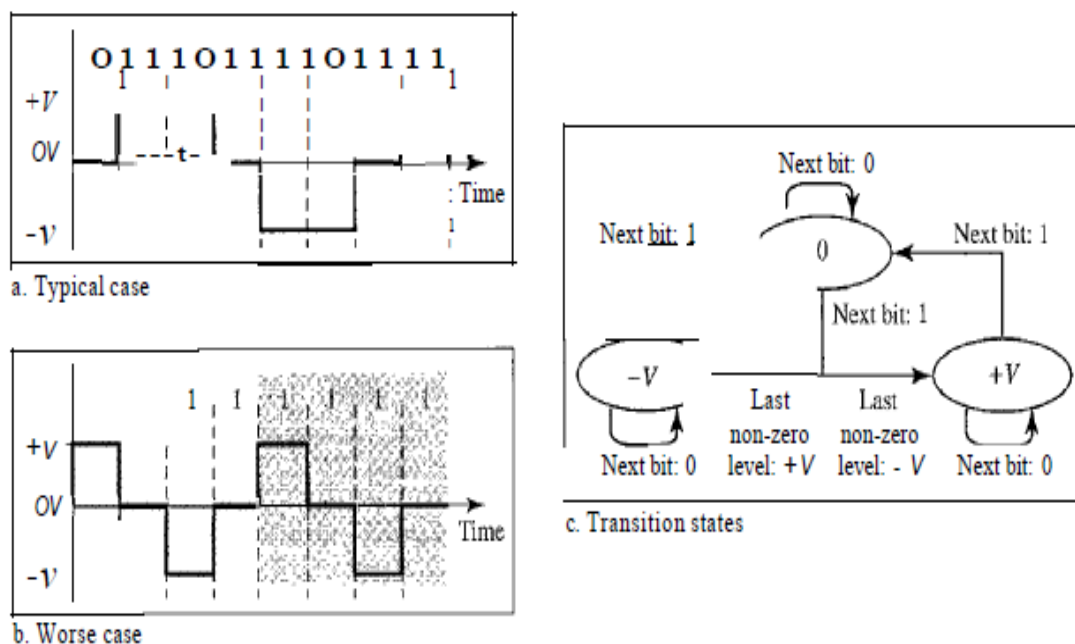
more than two levels, we can design a differential encoding scheme with more than two transition rules. MLT-3 is one of them. The multiline transmission, three level (MLT-3) scheme uses three levels ( $+V$ ,  $0$ , and  $-V$ ) and three transition rules to move between the levels.

- a. If the next bit is  $0$ , there is no transition.
- b. If the next bit is  $1$  and the current level is not  $0$ , the next level is  $0$ .
- c. If the next bit is  $1$  and the level is  $0$ , the next level is the opposite of the last nonzero level.

The behavior of MLT-3 can best be described by the state diagram shown in Figure 52. The three voltage levels ( $-V$ ,  $0$ , and  $+V$ ) are shown by three states (ovals). The transition from one state (level) to another is shown by the connecting lines. Figure 52 also shows two examples of an MLT-3 signal.

We might wonder why we need to use MLT-3, a scheme that maps one bit to one signal element. The signal rate is the same as that for NRZ-I, but with greater complexity (three levels and complex transition rules). It turns out that the shape of the signal in this scheme helps to reduce the required bandwidth. Let us look at the worst-case scenario, a sequence of  $1$ s. In this case, the signal element pattern  $+V0-V0$  is repeated every 4 bits.

A nonperiodic signal has changed to a periodic signal with the period equal to 4 times the bit duration. This worst-case situation can be simulated as an analog signal with a frequency one-fourth of the bit rate. In other words, the signal rate for MLT-3 is one-fourth the bit rate. This makes MLT-3 a suitable choice when we need to send 100 Mbps on a copper wire that cannot support more than 32 MHz (frequencies above this level create electromagnetic emissions).

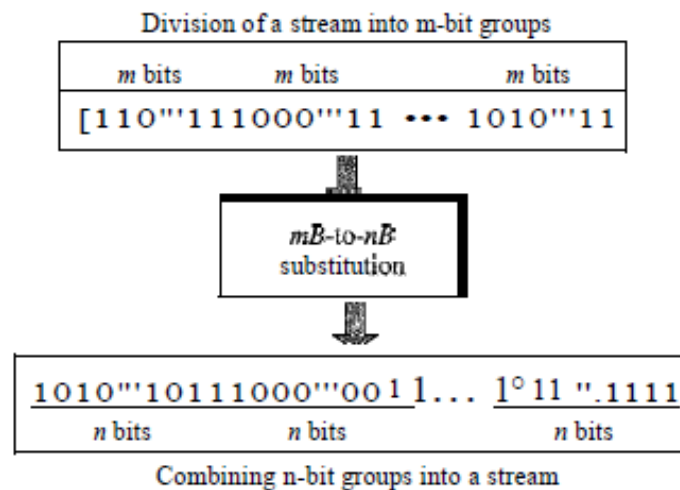


**Figure 52: 9.2.5. Multiline Transmission ML-3**

### 10.3. Block Coding

We need redundancy to ensure synchronization and to provide some kind of inherent error detecting. Block coding can give us this redundancy and improve the performance of line coding. In general, block coding changes a block of  $m$  bits into a block of  $n$  bits, where  $n$  is larger than  $m$ . Block coding is referred to as an  $mB/nB$  encoding technique. Block coding is normally referred to as  $mB/nB$  coding; it replaces each  $m$ -bit group with an  $n$ -bit group. The slash in block encoding (for example, 4B/5B) distinguishes block encoding from multilevel encoding (for example, 8B6T), which is written without a slash. Block coding normally involves three steps: division, substitution, and combination. In the division step, a sequence of bits is divided into groups of  $m$  bits. For example, in 4B/5B encoding, the original bit sequence is divided into 4-bit groups. The heart of block coding is the substitution step. In this step, we substitute an  $m$ -bit group for an  $n$ -bit group. For example, in 4B/5B encoding we substitute a 4-bit code for

a 5-bit group. Finally, the  $n$ -bit groups are combined together to form a stream. The new stream has more bits than the original bits. Figure 53 shows the procedure.



**Figure 53: Block coding**

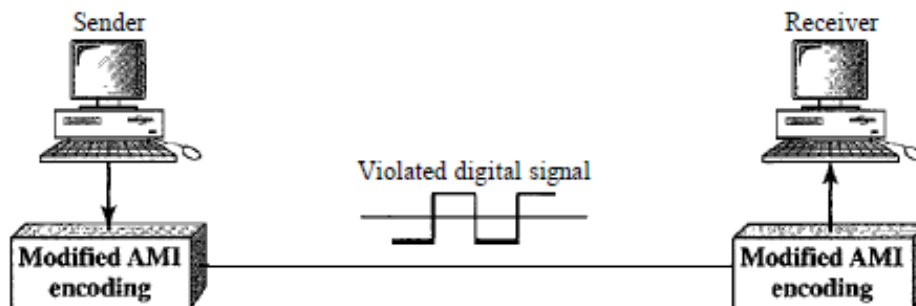
#### 10.4. Scrambling

Biphase schemes that are suitable for dedicated links between stations in a LAN are not suitable for long-distance communication because of their wide bandwidth requirement. The combination of block coding and NRZ line coding is not suitable for long-distance encoding either, because of the DC component. Bipolar AMI encoding, on the other hand, has a narrow bandwidth and does not create a DC component. However, a long sequence of 0s upsets the synchronization. If we can find a way to avoid a long sequence of 0s in the original stream; we can use bipolar AMI for long distances. We are looking for a technique that does not increase the number of bits and does provide synchronization.

We are looking for a solution that substitutes long zero-level pulses with a combination of other levels to provide synchronization. One solution is called scrambling. We modify part of the AMI rule to include scrambling, as shown in Figure



54. Note that scrambling, as opposed to block coding, is done at the same time as encoding. The system needs to insert the required pulses based on the defined scrambling rules. Two common scrambling techniques are B8ZS and HDB3.



**Figure 54: *AMI used with scrambling***

### 10.5. Review Questions

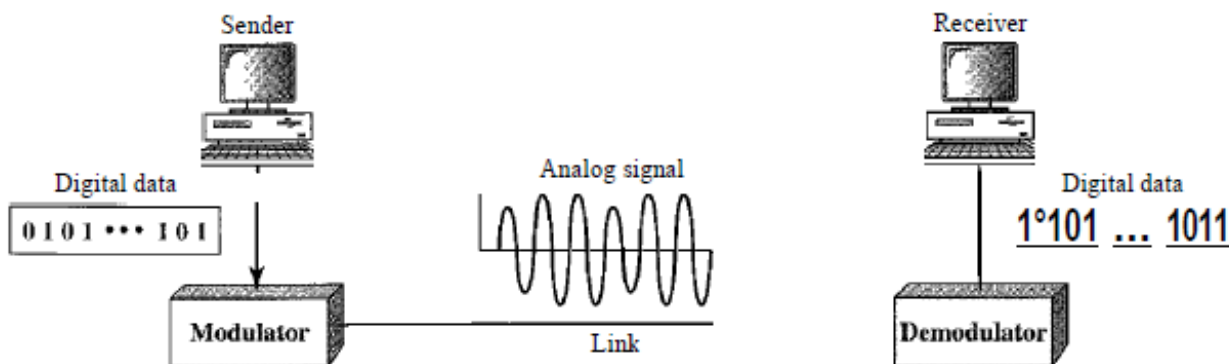
1. Highlights three techniques of digital-to-digital conversion.
2. Define the characteristics of a self-synchronizing signal.
3. Compare and contrast five line coding schemes discussed in this book.
4. Define block coding and give its purpose.
5. Define scrambling and give its purpose.
6. Give natural explanation on why we do not have DC component in bipolar encoding.

# CHAPTER TEN

## DIGITAL-TO-ANALOG CONVERSION USING MODULATION TECHNIQUES

### 10.1. DIGITAL-TO-ANALOG CONVERSION

Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal based on the information in digital data. Figure 55 shows the relationship between the digital information, the digital-to-analog modulating process, and the resultant analog signal.



**Figure 55: *Digital-to-analog conversion***

### 10.2. What is Modulation Techniques?

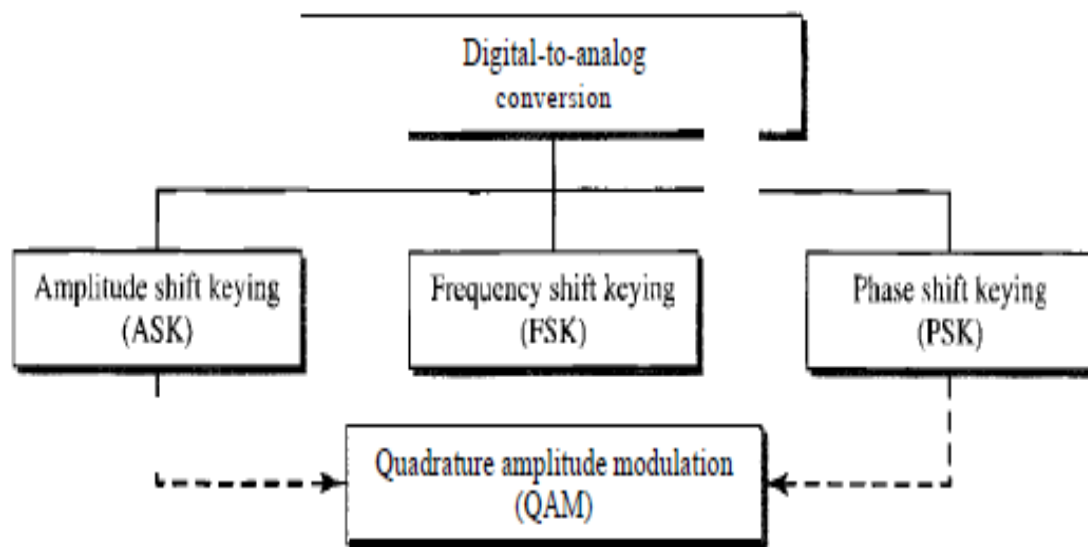
As discussed earlier, a sine wave is defined by three characteristics: amplitude, frequency, and phase. When we vary anyone of these characteristics, we create a different version of that wave. So, by changing one characteristic of a simple electric signal, we can use it to represent digital data. The techniques of varying the characteristics are known as modulation techniques.

Modulation Techniques are methods used to encode digital information in an analog world. Additionally, digital signals usually require an intermediate modulation step for transport

across wideband, analog-oriented networks. Modulation is the process where a Radio Frequency or Light Wave's amplitude, frequency, or phase is changed in order to transmit intelligence. Digital information changes the carrier signal by modifying one or more of its characteristics (amplitude, frequency, or phase). This kind of modification is called modulation (shift keying).

### 10.3. Types of Modulation

Any of the three characteristics can be altered in this way, giving us at least three types for modulating digital data into an analog signal: amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK). In addition, there is a fourth (and better) mechanism that combines changing both the amplitude and phase, called quadrature amplitude modulation (QAM). QAM is the most efficient of these options and is the mechanism commonly used today (see Figure 56).



**Figure 56: *Types of digital-to-analog conversion***

### 10.3.1. Amplitude Shift Keying

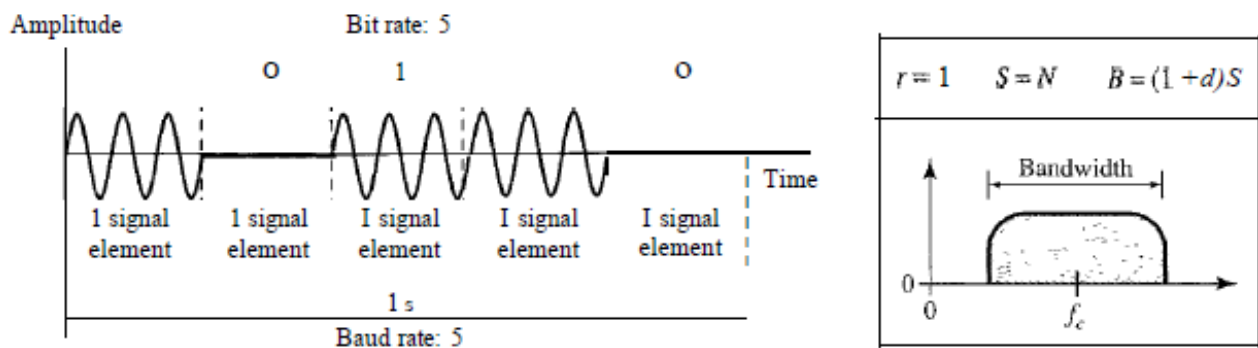
In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes. *Binary ASK (BASK)* although we can have several levels (kinds) of signal elements, each with a different amplitude, ASK is normally implemented using only two levels. This is referred to as binary amplitude shift keying or *on-off keying (OOK)*. The peak amplitude of one signal level is 0; the other is the same as the amplitude of the carrier frequency. Figure 57 gives conceptual views of binary ASK.

Bandwidth for ASK Figure 57 also shows the bandwidth for ASK. Although the carrier signal is only one simple sine wave, the process of modulation produces a nonperiodic composite signal. This signal, as was discussed earlier, has a continuous set of frequencies. As we expect, the bandwidth is proportional to the signal rate (baud rate). However, there is normally another factor involved, called  $d$ , which depends on the modulation and filtering process. The value of  $d$  is between 0 and 1. This means that the bandwidth can be expressed as shown, where  $S$  is the signal rate and the  $B$  is the bandwidth.

$$B = (1 + d) \times S$$

The formula shows that the required bandwidth has a minimum value of  $S$  and a maximum value of  $2S$ . The most important point here is the location of the bandwidth.

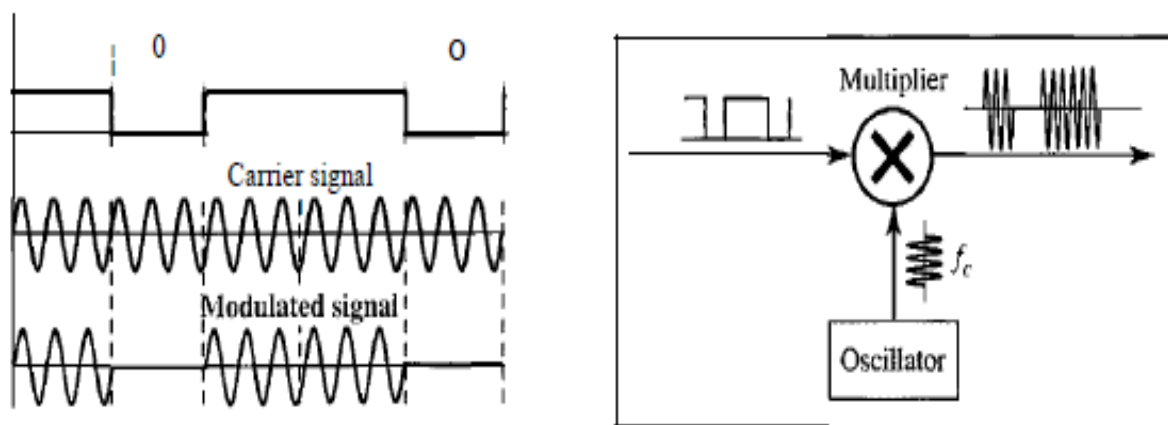
The middle of the bandwidth is where  $f_c$  the carrier frequency, is located. This means if we have a bandpass channel available, we can choose our  $f_c$  so that the modulated signal occupies that bandwidth. This is in fact the most important advantage of digital-to-analog conversion. We can shift the resulting bandwidth to match what is available.



**Figure 57: Binary amplitude shift keying**

### Implementation of ASK

The complete discussion of ASK implementation is beyond the scope of this book. However, the simple ideas behind the implementation may help us to better understand the concept itself. Figure 58 illustrate how we can simply implement binary ASK. If digital data are presented as a unipolar NRZ, digital signal with a high voltage of 1V and a low voltage of 0 V, the implementation can be achieved by multiplying the NRZ digital signal by the carrier signal coming from an oscillator. When the amplitude of the NRZ signal is 1, the amplitude of the carrier frequency is held; when the amplitude of the NRZ signal is 0, the amplitude of the carrier frequency is zero.



**Figure 58: Implementation of binary ASK**

## Multilevel ASK

The above discussion uses only two amplitude levels. We can have multilevel ASK in which there are more than two levels. We can use 4, 8, 16, or more different amplitudes for the signal and modulate the data using 2, 3, 4, or more bits at a time. In these cases,  $r=2$ ,  $r=3$ ,  $r=4$ , and so on. Although this is not implemented with pure ASK, it is implemented with QAM.

### 10.3.2 Frequency Shift Keying

In frequency shift keying, the frequency of the carrier signal is varied to represent data. The frequency of the modulated signal is constant for the duration of one signal element, but changes for the next signal element if the data element changes. Both peak amplitude and phase remain constant for all signal elements.

#### Binary FSK (BFSK)

One way to think about binary FSK (or BFSK) is to consider two carrier frequencies. In Figure 59, we have selected two carrier frequencies,  $f_1$  and  $f_2$ . We use the first carrier if the data element is 0; we use the second if the data element is 1. However, note that this is an unrealistic example used only for demonstration purposes. Normally the carrier frequencies are very high, and the difference between them is very small.

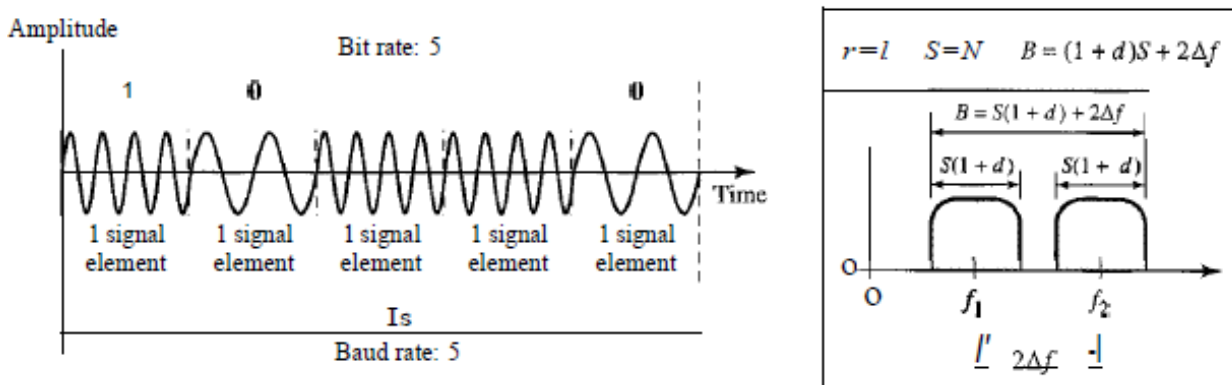


Figure 59: Binary frequency shift keying

As Figure 59 shows, the middle of one bandwidth is  $f_1$  and the middle of the other is  $f_2$ . Both  $f_1$  and  $f_2$  are  $\Delta f$  apart from the midpoint between the two bands. The difference between the two frequencies is  $2\Delta f$

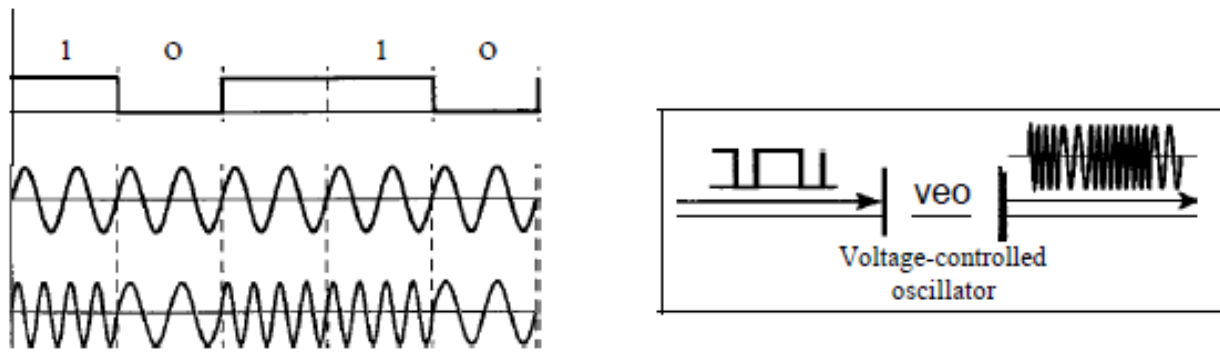
Bandwidth for BFSK Figure 59 also shows the bandwidth of FSK. Again the carrier signals are only simple sine waves, but the modulation creates a nonperiodic composite signal with continuous frequencies. We can think of FSK as two ASK signals, each with its own carrier frequency. If the difference between the two frequencies is  $2\Delta f$ , then the required bandwidth is

$$B = (1 + d)S + 2\Delta f$$

What should be the minimum value of  $2\Delta f$  In Figure 59, we have chosen a value greater than  $(1 + d)S$ . It can be shown that the minimum value should be at least  $S$  for the proper operation of modulation and demodulation.

## Implementation

There are two implementations of BFSK: noncoherent and coherent. In noncoherent BFSK, there may be discontinuity in the phase when one signal element ends and the next begins. In coherent BFSK, the phase continues through the boundary of two signal elements. Noncoherent BFSK can be implemented by treating BFSK as two ASK modulations and using two carrier frequencies. Coherent BFSK can be implemented by using one *voltage-controlled oscillator* (VCO) that changes its frequency according to the input voltage. Figure 60 shows the simplified idea behind the second implementation. The input to the oscillator is the unipolar NRZ signal. When the amplitude of NRZ is zero, the oscillator keeps its regular frequency; when the amplitude is positive, the frequency is increased.



**Figure 60: Implementation of BPSK**

### ***Multilevel FSK***

Multilevel modulation (MFSK) is not uncommon with the FSK method. We can use more than two frequencies. For example, we can use four different frequencies  $f_1$ ,  $f_2$ ,  $f_3$ , and  $f_4$  to send 2 bits at a time. To send 3 bits at a time, we can use eight frequencies. And so on. However, we need to remember that the frequencies need to be  $2\Delta f$  apart. For the proper operation of the modulator and demodulator, it can be shown that the minimum value of  $2\Delta f$  to be  $S$ . We can show that the bandwidth with  $d=0$  is

$$B = (1 + d) \times S + (L - 1) 2\Delta f$$

$$B = L \times S$$

### **10.3.3. Phase Shift Keying**

In phase shift keying, the phase of the carrier is varied to represent two or more different signal elements. Both peak amplitude and frequency remain constant as the phase changes. Today, PSK is more common than ASK or FSK. However, we will see that QAM, which combines ASK and PSK, is the dominant method of digital-to-analog modulation.

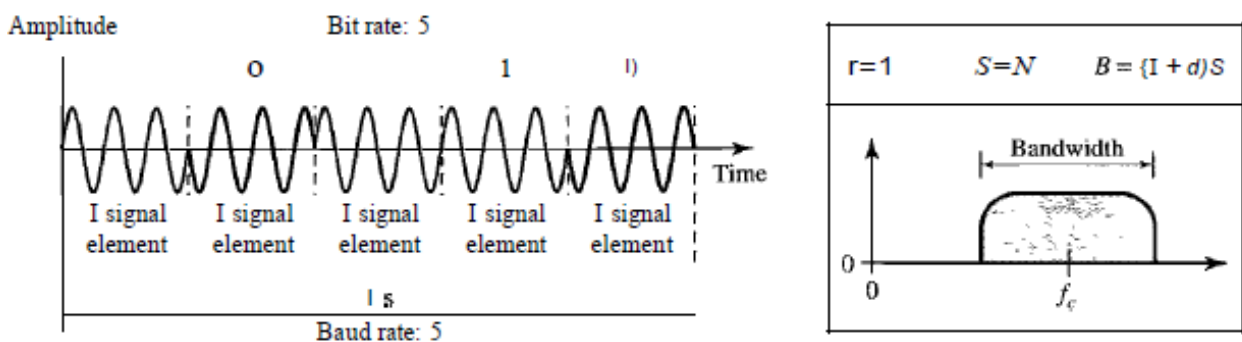
### ***Binary PSK (BPSK)***



The simplest PSK is binary PSK, in which we have only two signal elements, one with a phase of  $0^\circ$ , and the other with a phase of  $180^\circ$ . Figure 5.9 gives a conceptual view of PSK. Binary PSK is as simple as binary ASK with one big advantage—it is less susceptible to noise. In ASK, the criterion for bit detection is the amplitude of the signal; in PSK, it is the phase. Noise can change the amplitude easier than it can change the phase. In other words, PSK is less susceptible to noise than ASK. PSK is superior to FSK because we do not need two carrier signals.

**Bandwidth** Figure 60 also shows the bandwidth for BPSK. The bandwidth is the same as that for binary ASK, but less than that for BFSK. No bandwidth is wasted for separating two carrier signals.

**Implementation** The implementation of BPSK is as simple as that for ASK. The reason is that the signal element with phase  $180^\circ$  can be seen as the complement of the signal element with phase  $0^\circ$ . This gives us a clue on how to implement BPSK. We use the same idea we used for ASK but with a polar NRZ signal instead of a unipolar NRZ signal.



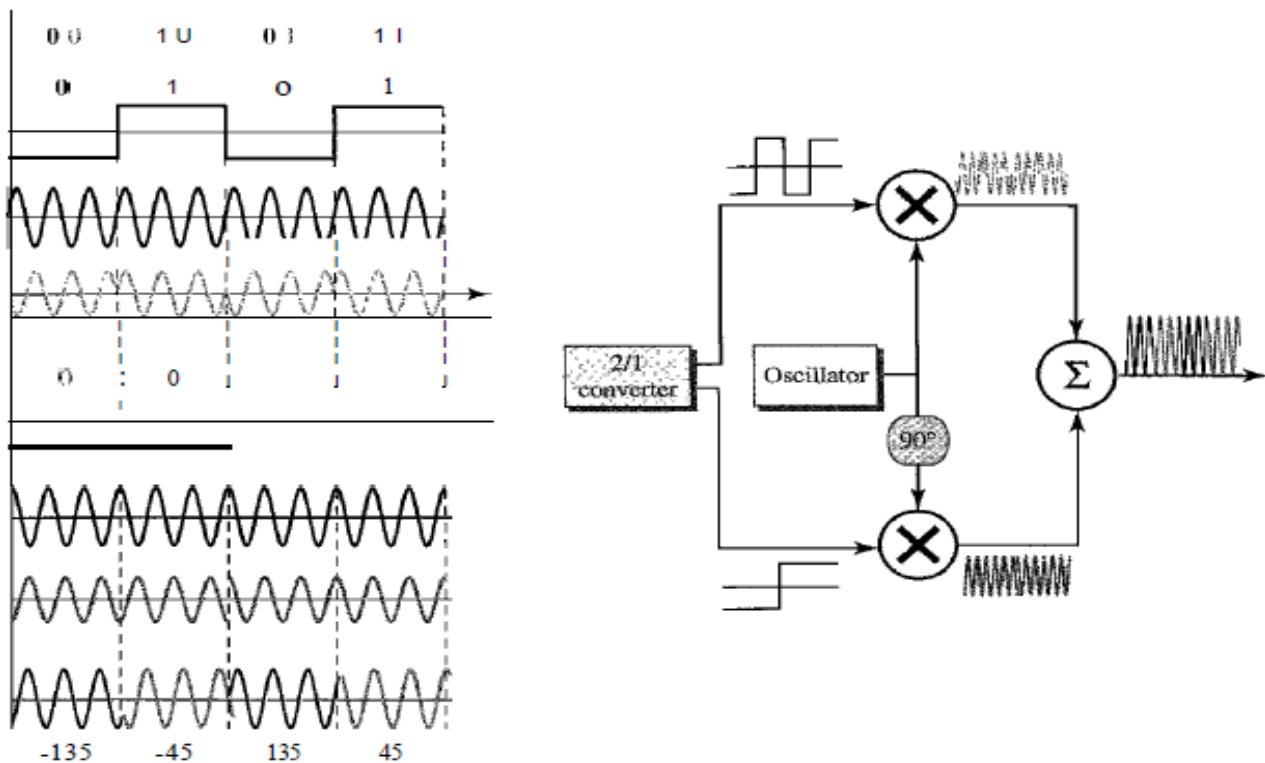
**Figure 61: *Binary phase shift keying***

#### **10.3.4. Quadrature PSK (QPSK)**

The simplicity of BPSK enticed designers to use 2 bits at a time in each signal element, thereby decreasing the baud rate

and eventually the required bandwidth. The scheme is called quadrature PSK or QPSK because it uses two separate BPSK modulations; one is in-phase, the other quadrature (out-of-phase). The incoming bits are first passed through a serial-to-parallel conversion that sends one bit to one modulator and the next bit to the other modulator. If the duration of each bit in the incoming signal is  $T$ , the duration of each bit sent to the corresponding BPSK signal is  $2T$ . This means that the bit to each BPSK signal has one-half the frequency of the original signal. Figure 62 shows the idea.

The two composite signals created by each multiplier are sine waves with the same frequency, but different phases. When they are added, the result is another sine wave, with one of four possible phases:  $45^\circ$ ,  $-45^\circ$ ,  $135^\circ$ , and  $-135^\circ$ . There are four kinds of signal elements in the output signal ( $L = 4$ ), so we can send 2 bits per signal element ( $r=2$ ).



**Figure 62: QPSK and its implementation:**

## 10.4. Constellation Diagram

A constellation diagram can help us define the amplitude and phase of a signal element, particularly when we are using two carriers (one in-phase and one quadrature), the diagram is useful when we are dealing with multilevel ASK, PSK, or QAM. In a constellation diagram, a signal element type is represented as a dot. The bit or combination of bits it can carry is often written next to it.

The diagram has two axes. The horizontal  $X$  axis is related to the in-phase carrier; the vertical  $Y$  axis is related to the quadrature carrier. For each point on the diagram, four pieces of information can be deduced. The projection of the point on the  $X$  axis defines the peak amplitude of the in-phase component; the projection of the point on the  $Y$  axis defines the peak amplitude of the quadrature component. The length of the line (vector) that connects the point to the origin is the peak amplitude of the signal element (combination of the  $X$  and  $Y$  components); the angle the line makes with the  $X$  axis is the phase of the signal element. All the information we need, can easily be found on a constellation diagram. Figure 63 shows a constellation diagram.

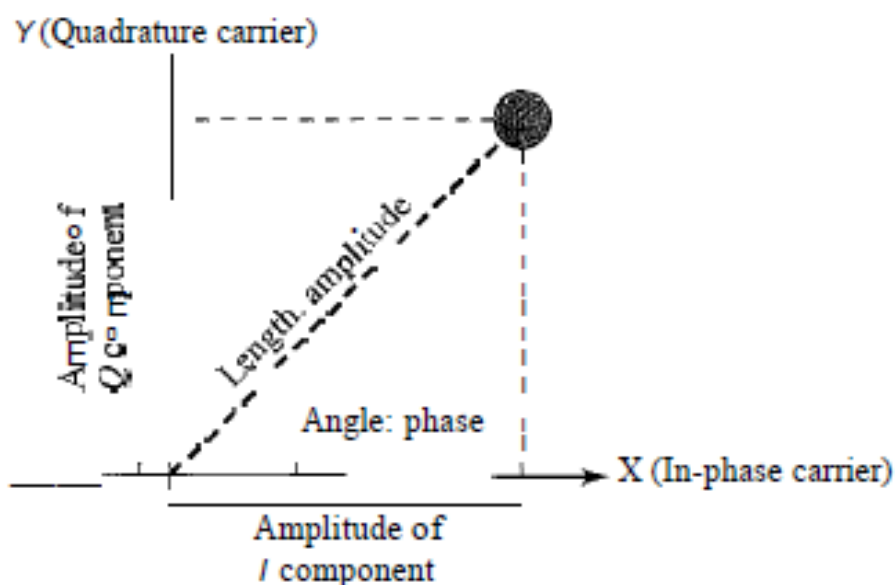


Figure 63: *Concept of a constellation diagram*

## **10.5. Review Questions**

- 1. Define analog transmission.**
- 2. Define carrier signal and its role in analog transmission.**
- 3. Describe digital-to-analog conversion.**
- 4. Which characteristics of an analog signal are changed to represent the digital signal in each of the following digital-to-analog conversion?**
  - a. ASK**
  - b. FSK**
  - c. PSK**
  - d. QAM**
- 5. Which of the four digital-to-analog conversion techniques (ASK, FSK, PSK or QAM) is the most susceptible to noise? Juxtapose your answer.**
- 6. Define constellation diagram and its role in analog transmission.**
- 7. What are the two components of a signal when the signal is represented on a constellation diagram? Which component is shown on the horizontal axis? Which is shown on the vertical axis?**

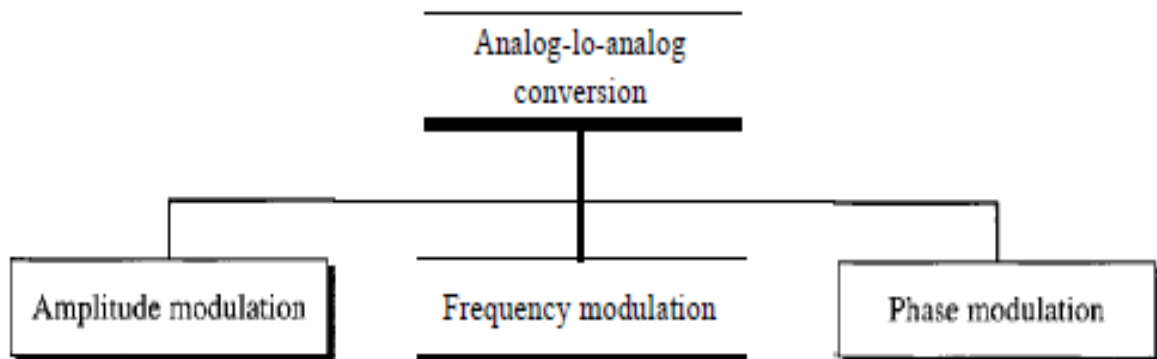
# CHAPTER ELEVEN

## MULTIPLEXING

### 11.1. Definition of Multiplexing

Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. As data and telecommunications use increases, so does traffic. We can accommodate this increase by continuing to add individual links each time a new channel is needed; or we can install higher-bandwidth links and use each to carry multiple signals. In a multiplexed system,  $n$  lines share the bandwidth of one link. Figure 6.1 shows the basic format of a multiplexed system. The lines on the left direct their transmission streams to a multiplexer (MUX), which combines them into a single stream (many-to-one). At the receiving end, that stream is fed into a demultiplexer (DEMUX), which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines. In the figure, the word link refers to the physical path. The word channel refers to the portion of a link that carries a transmission between a given pair of lines. One link can have many ( $n$ ) channels. Multiplexing is the transmission of multiple data communication sessions over a common wire or medium. Multiplexing reduces the number of wires or cable required to connect multiple sessions. A session is considered to be data communication between two devices: computer to computer, terminal to computer, etc. There are three basic multiplexing techniques: frequency-

division multiplexing, wavelength-division multiplexing, and time-division multiplexing. The first two are techniques designed for analog signals, the third, for digital signals (see Figure 6.2).



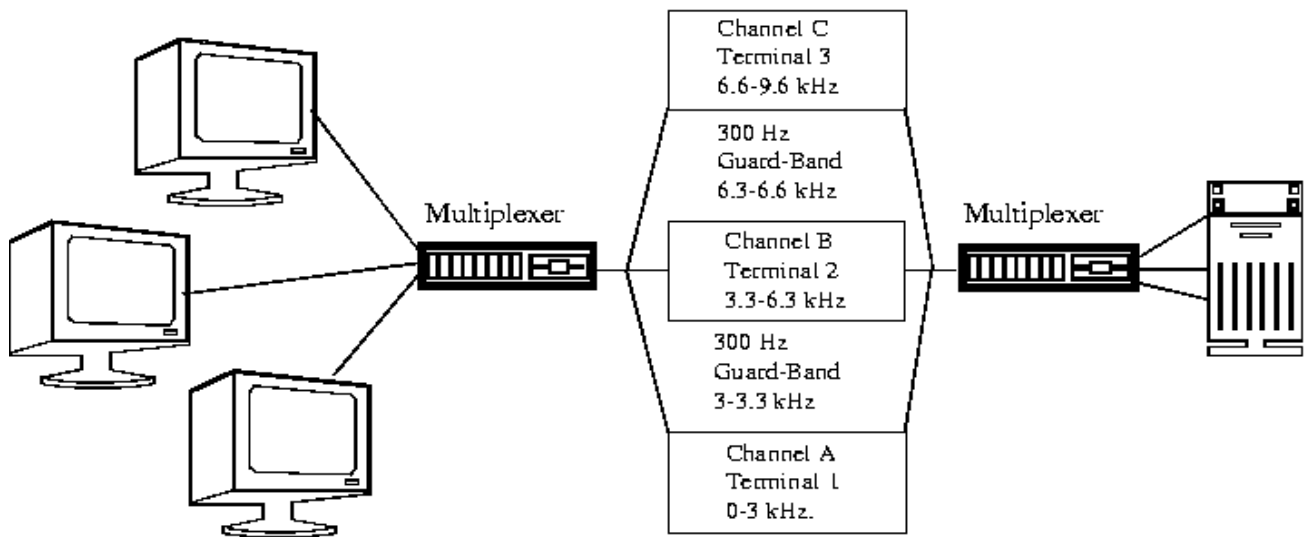
**Figure 64: *Categories of multiplexing***

## **11.2. Types of Multiplexing Techniques**

### **11.2.1. Frequency Division Multiplexing**

Frequency Division Multiplexing (FDM) is an analog technique where each communications channel is assigned a carrier frequency. To separate the channels, a guard-band would be used. This is to ensure that the channels do not interfere with each other. For example, if we had our 3 terminals each requiring a bandwidth of 3 kHz and a 300 Hz guard-band, Terminal 1 would be assigned the lowest frequency channel 0-3 kHz, Terminal 2 would be assigned the next frequency channel 3.3kHz-6.3kHz and Terminal 3 would be assigned the final frequency channel 6.6kHz-9.6 kHz.

The frequencies are stacked on top of each other and many frequencies can be sent at once. The downside is that the overall line bandwidth increases. Individual terminal requirement were 3 kHz bandwidth each, in the above example: the bandwidth to transmit all 3 terminals is now 9.6 kHz.



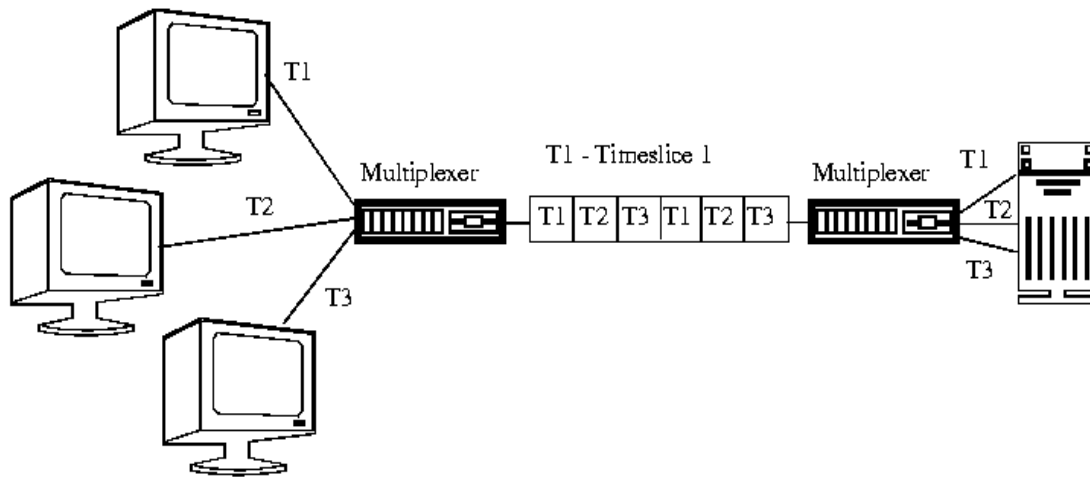
**Figure 65: Frequency Division Multiplexing**

FDM does not require all channels to terminate at a single location. Channels can be extracted using a multi-drop technique; terminals can be stationed at different locations within a building or a city. FDM is an analog and slightly historical multiplexing technique. It is prone to noise problems and has been overtaken by Time Division Multiplexing which is better suited for digital data.

### 11.2.2. Time Division Multiplexing

Time Division Multiplexing is a technique where a short time sample of each channel is inserted into the multiplexed data stream. Each channel is sampled in turn and then the sequence is repeated. The sample period has to be fast enough to sample each channel according to the Nyquist Theory ( $2 \times$  highest frequency) and to be able to sample all the other channels within that same time period. It can be thought of as a very fast mechanical switch, selecting each channel for a very short time then going on to the next channel. Each channel has a time slice assigned to it whether the terminal is being used or not. Again, to the send and receiving stations, it appears as if there is a single line connecting them. All lines

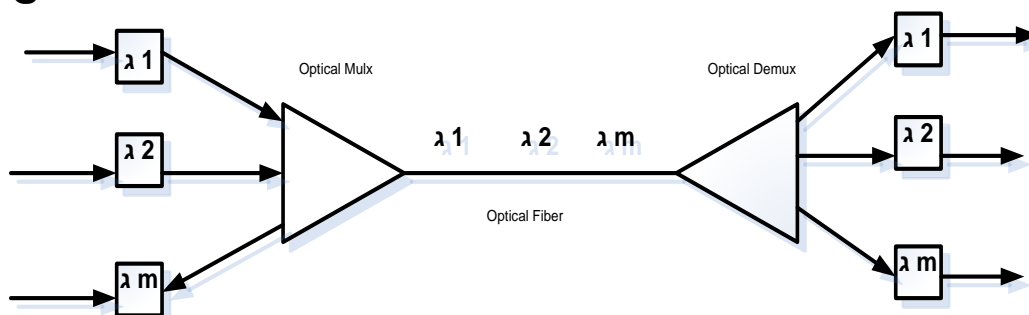
originate in one location and end in one location. TDM is more efficient, easier to operate, less complex and less expensive than FDM.



**Figure 66: Time Division Multiplexing**

### 11.2.3. Wavelength Division Multiplexing

This technique is used in optical fiber. It is useful to increase the information carried by single optical fiber. WDM can be viewed as an optical domain version of FDM in which multiple information signals modulate optical signals at different optical wavelengths (colors). The resulting signals are combined and transmitted simultaneously over the same optical fiber as in the diagram below.



**Figure 67: Wavelength Division Multiplexing**

Various optical devices such as prisms and diffraction grating can be used to combine and split color signals. For instance, early WDM systems combine 16 wavelengths at 2.5Gbps to provide an aggregate signal of 16 x 2.5Gbps. WDM systems



with 32 wavelengths at 10gbps have a total bit rate of 320Gbps and are widely deployed. Systems that carry 160 wavelengths at 10Gbps are also available and achieved at amazing bit rate of 1.6 terabit/second. The attraction of WDM is that a huge increase in available bandwidth is obtained with less investment associated with deploying additional optical fiber. The additional bandwidth can be used to carry more traffic and can also provide the additional protection bandwidth refined by self-healing network topologies.

### **11.3. Review Question**

1. Explain briefly the term multiplexing
2. With the aid of diagram describe briefly;
  - i. Wavelength Division multiplexing (WDM)
  - ii. Time Division Multiplexing (TDM)
  - iii. Frequency Division Multiplexing (FDM)
3. Suppose that a frequency band  $W$  Hz wide into  $M$  channels of equal bandwidth.
  - a) What bit rate is achievable in each channel? Assume all channels have the same SNR.
  - b) What bit rate is available to each  $M$  user if the entire frequency band is used as a single channel and TDM is applied?
  - c) How does the comparison of (a) and (b) change if we suppose that FDM require a guard band between adjacent channels? Assume the guard band is 10% of channel bandwidth
4. Suppose Ray Power FM 100.5, has a large band of available bandwidth, say 1GHz, which is to be used by central office to transmit and receive from large number of users. Describe how the following approach can be use to organizing the system:
  - a) A single TDM

- b) A hybrid TDM/FDM system in which the frequency band is divided into multiple channel and time division multiplexing is used within each channel
- 5. Compare the operation of multiplexer, an add-drop multiplexer, a switch, and a digital cross-connect.

# **CHAPTER TWELVE**

## **NETWORK IMPLEMENTATION DEVICES**

### **12.1. Network Implementation Devices**

The equipment's and tools use to connect two or more system together is refers to as network implementation devices. Some of the devices are described below.

#### **12.1.1. Network Interface Card and Driver**

A network interface card (NIC) is a circuit board or card that is installed in a computer so that it can be connected to a network. It provides the computer with a dedicated, full-time connection to a network. Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology Network Interface Card Drivers are the software interface between the Network Card Hardware/Firmware and the Network Operating System Data Link layer. The Network Card device driver is a device driver loaded in config.sys. The Network Card consists of Firmware and Hardware. The Firmware is the program stored on the network card's ROM (BIOS) and configuration information stored in E2ROM. There are basically 3 types of Network Card Drivers: NDIS; ODI; and Packet drivers.

1. **NDIS** stands for Network Driver Interface Specification. NDIS drivers are used by Microsoft based Network Operating Systems such as Microsoft LAN Manager, Windows NT, Windows for WorkGroups and IBM's OS/2.

2. **ODI** stands for Open Datalink Interface. ODI drivers are used by Novell's Network Operating System and Apple.
3. **Packet drivers** use software interrupts to interface to the network card. Many non-commercial programs (shareware and freeware) use packet driver interfaces.

### 12.1.2. Repeaters

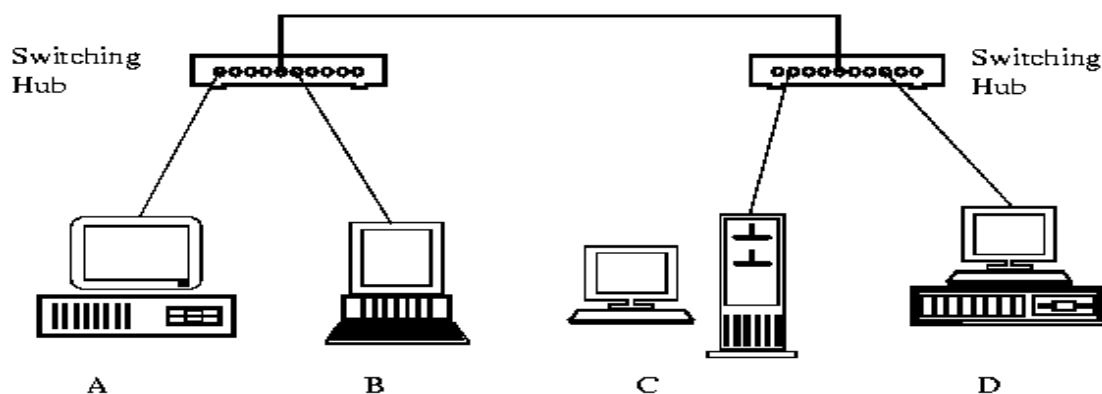
Repeaters are physical hardware devices that have a primary function to regenerate the electrical signal by: Reshaping the waveform; amplifying the waveform; and Retiming the signal

### 12.1.3. Hubs

Hubs are also called Multiport Repeaters or Concentrators. They are physical hardware devices. Some Hubs are basic hubs with minimum intelligence no microprocessors. Intelligent Hubs can perform basic diagnostics and test the nodes to see if they are operating correctly. If they are not, the Smart Hubs or Intelligent Hubs will remove the node from the network. Some Smart Hubs can be polled and managed remotely.

### 12.1.4. Switching Hubs

Switching hubs are hubs that will directly switch ports to each other. They are similar to full duplex hubs except that they allow dedicated 10Mbps channels between ports.



**Figure 68: Switching Hub Operation**

If A wanted to communicate with B, a dedicated 10 Mbps connection would be established between the two. If C wanted to communicate with D, another dedicated 10 Mbps connection would be established.

### **12.1.5. Bridges**

Bridges are both hardware and software devices. They can be standalone devices - separate boxes specifically designed for bridging applications, or they can be dedicated PCs with 2 NICs and bridging software. Most servers' software will automatically act as a bridge when a second NIC card is installed.

#### **Purpose of a Bridge**

The purposes of a Bridge are:

- i. Isolates networks by MAC addresses
- ii. Manages network traffic by filtering packets
- iii. Translate from one protocol to another

#### **Bridge Methodologies**

There are 3 primary bridging methodologies used by bridges for connecting local area networks:

- i. Transparent bridges
- ii. Spanning Tree Protocol
- iii. Source Routing

#### **Why using Bridge**

There are four basic reasons to use a bridge:

- i. Security: Stops networks from forwarding sensitive data
- ii. Bandwidth: Reduce traffic by segmentation
- iii. Reliability: If 1 segment goes down, it does not take down the complete LAN

- iv. **Translation:** Translate different Data Link protocols such as Token Ring to Ethernet

### **12.1.6. Routers**

Routers are hardware and software devices. They can be cards that plug into a collapsed backbone, stand-alone devices (rack mount or desktop) or software that would run on a file server with 2 NICs.

The purpose of a router is to connect nodes across an internetwork regardless of the Physical Layer and Data Link Layer protocol used. Routers are hardware and topology independent. Routers are not aware of the type of medium or frame used (Ethernet, Token Ring, FDDI, X.25, etc.). Routers are aware of the Network Layer protocol used: Novell's IPX, Unix's IP, XNS, Apples DDP, etc.

## **12.2. Cabling and Network Setup**

### **12.2.1. RJ45 Cabling**

**Materials required**

1. Ethernet Cable - bulk Category (Cat) 5, 5e, 6, 6a or higher ethernet cable
2. Wire Cutters - to cut and strip the ethernet cable if necessary
3. For Patch Cables:
  - a. 8P8C Modular Connector Plugs ("RJ45")
  - b. Modular Connector Crimper ("RJ45")
4. For Fixed Wiring:
  - a. 8P8C Modular Connector Jacks ("RJ45")
  - b. 110 Punch Down Tool
5. Recommended:
6. Wire Stripper
7. Cable Tester

### 12.2.2. Ethernet Cable Structure

Ethernet cable Cat 5 is required for basic 10/100 functionality, you will want Cat 5e for gigabit (1000BaseT) operation and Cat 6 or higher gives you a measure of future proofing. Bulk Ethernet cable comes in many types; there are 2 basic categories, solid and braided stranded cable. Figure 69 shows the internal structure of a cable.

- i. Stranded Ethernet cable tends to work better in patch applications for desktop use. It is more flexible and resilient than solid ethernet cable and easier to work with, but really meant for shorter lengths.
- ii. Solid Ethernet cable is meant for longer runs in a fixed position.



**Figure 69: Internal Cable Structure and Color Coding**

Inside the Ethernet cable, there are 8 color coded wires. These wires are twisted into 4 pairs of wires; each pair has a common color theme. One wire in the pair being a solid or primarily solid colored wire and the other being a primarily

white wire with a colored stripe (Sometimes Ethernet cables won't have any color on the striped wire, the only way to tell which is which is to check which wire it is twisted around). Examples of the naming schemes used are: Orange (alternatively Orange/White) for the solid colored wire and White/Orange for the striped cable. The twists are extremely important. They are there to counteract noise and interference.

It is important to wire according to a standard to get proper performance from the Ethernet cable. The TIA/EIA-568-A specifies two wiring standards for an 8-position modular connector such as RJ45. The two wiring standards, T568A and T568B vary only in the arrangement of the colored pairs.

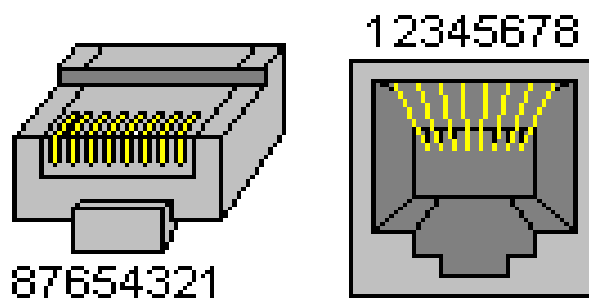
### **12.2.3. Modular Connector Plugs and Jacks**

The 8P8C modular connectors for Ethernet are often called RJ45 due to their physical resemblance. The plug is an 8-position modular connector that looks like a large phone plug. There are a couple variations available. The primary variation you need to pay attention to is whether the connector is intended for braided or solid wire. For braided/stranded wires, the connector has sharp pointed contacts that actually pierce the wire. For solid wires, the connector has fingers which cut through the insulation and make contact with the wire by grasping it from both sides.

Modular connector jacks come in a variety styles intended for several different mounting options. The choice is one of requirements and preference. Jacks are designed to work only with solid Ethernet cable. Most jacks come labeled with color coded wiring diagrams for T568A, T568B or both. Make sure you end up with the correct one. Figure 70 shows a wiring diagram and pin out:



Where is pin #1?



**Figure 70: Modular Connector Plug and Jack Pin Out**







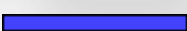



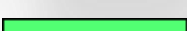


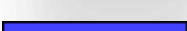

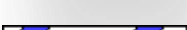
#### 12.2.4. Ethernet Cable Pin Outs

There are two basic Ethernet cable pin outs. A straight through Ethernet cable, which is used to connect to a hub or switch, and a crossover Ethernet cable used to operate in a peer-to-peer fashion without a hub/switch. Generally all fixed wiring should be run as straight through. Some Ethernet interfaces can cross and un-cross a cable automatically as needed, a handy feature.

**Table 1: Straight-Through Ethernet Cable Pin Out for T568A**

RJ45 Pin #	Wire Color (T568A)	Wire Diagram (T568A)	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	White/Green		Transmit+	BI_DA+
2	Green		Transmit-	BI_DA-
3	White/Orange		Receive+	BI_DB+
4	Blue		Unused	BI_DC+
5	White/Blue		Unused	BI_DC-
6	Orange		Receive-	BI_DB-
7	White/Brown		Unused	BI_DD+
8	Brown		Unused	BI_DD-

**Table 2: Crossover Cable Wiring Diagram (T568B)**

RJ45 Pin #	Wire Color T568B	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

**+Note:** The crossover Ethernet cable layout is suitable for 1000Base-T operation, all 4 pairs are crossed.

### 12.2.5. Wiring Ethernet Patch Cables

#### Basic Theory

By looking at a T-568A UTP Ethernet straight-thru cable and an Ethernet crossover cable with a T-568B end, we see that the TX (transmitter) pins are connected to the corresponding RX (receiver) pins, plus to plus and minus to minus. You can also see that both the blue and brown wire pairs on pins 4, 5, 7, and 8 are not used in either standard. What you may not realize is that, these same pins 4, 5, 7, and 8 are not used or required in 100BASE-TX as well. So why bother using these wires, well for one thing it's simply easier to make a connection with all the wires grouped together. Otherwise you'll be spending time trying to fit those tiny little wires into each of the corresponding holes in the RJ-45 connector.

## **T-568A Straight-Through Ethernet Cable**

The T-568A standard is supposed to be used in new network installations. Most off-the-shelf Ethernet cables are still of the T-568B standard; however, it makes absolutely no functional difference in which you choose. If you require a cable to connect two Ethernet devices directly together without a hub or when you connect two hubs together, you will need to use a Crossover cable instead.

## **RJ-45 Crossover Ethernet Cable**

A good way of remembering how to wire a Crossover Ethernet cable is to wire one end using the T-568A standard and the other end using the T-568B standard. Another way of remembering the color coding is to simply switch the Green set of wires in place with the Orange set of wires. Specifically, switch the solid Green (G) with the solid Orange, and switch the green/white with the orange/white.

## **Procedures for Cabling**

1. Strip off about 2 inches of the Ethernet cable sheath.
2. Untwist the pairs, “don't untwist them beyond what you have exposed” the more untwisted cable you have the worse the problems you can run into.
3. Align the colored wires according to the wiring diagrams for either straightthrough or crossover.
4. Trim all the wires to the same length, about 1/2" to 3/4" left exposed from the sheath.
5. Insert the wires into the RJ45 plug “make sure each wire is fully inserted to the front of the RJ45 plug and in the correct order”. The sheath of the ethernet cable should extend into the plug by about 1/2" and will be held in place by the crimp.
6. Crimp the RJ45 plug with the crimper tool.

7. Verify the wires ended up the right order and that the wires extend to the front of the RJ45 plug and make good contact with the metal contacts in the RJ45 plug.
8. Cut the ethernet cable to length, @make sure it is more than long enough for your needs”
9. Repeat the above steps for the second RJ45 plug.

#### **12.2.6. Using Cable Tester**

If an Ethernet cable tester is available, use it to verify the proper connectivity of the cable. That should be it, if your ethernet cable doesn't turn out, look closely at each end and see if you can find the problem. Often a wire ended up in the wrong place or one of the wires is making no contact or poor contact. Also double check the color coding to verify it is correct. If you see a mistake or problem, cut the end off and start again. Ethernet cable tester is invaluable at identifying and highlighting these issues. When sizing ethernet cables remember that an end to end connection should not extend more than 100m (~328ft). Try to minimize the ethernet cable length, the longer the cable becomes, the more it may affect performance. This is usually noticeable as a gradual decrease in speed and increase in latency.

### **12.3. Network Card Configuration**

#### **Network Interface Cards configuration**

There are 3 configuration types of Network Interface Cards (NIC): jumper configurable; software configurable; and Plug n Play (PnP)

1. **Jumper configurable:** Cards have physical jumpers that you use to select the IRQ, I/O address, and upper memory block and transceiver type (10BaseT, 10Base2 or 10Base5). Older cards will also allow selecting DMA channel - this was used with XT and 286 PCs.

2. **Software configurable:** NICs have a proprietary software program that sets the NIC's "internal jumpers". They are usually menu driven and have an auto configuration mode, where the program will attempt to determine the most suitable configuration. These programs are not foolproof; you still require a thorough knowledge of the PC's architecture.
3. **Plug n Play:** NICs will attempt to auto-configure themselves during the bootup sequence immediately after installation. They also come with a proprietary software program in case that anything goes wrong and you have to manually configure them.

#### **12.4. Review Questions**

1. Enumerate and give function of any five network implementation device.
2. Explain three configuration types of Network Interface Cards.
3. Discuss the important of Ethernet cable tester.
4. Describe the Procedures for making network patch cable with Rj45.
5. Compare T-568A and T-568B
6. Enlist materials required for making network patch cable for a LAN.

# **CHAPTER THIRTEEN**

## **NETWORK SET-UP & CONFIGURATION (PHYSICAL HOME LAN)**

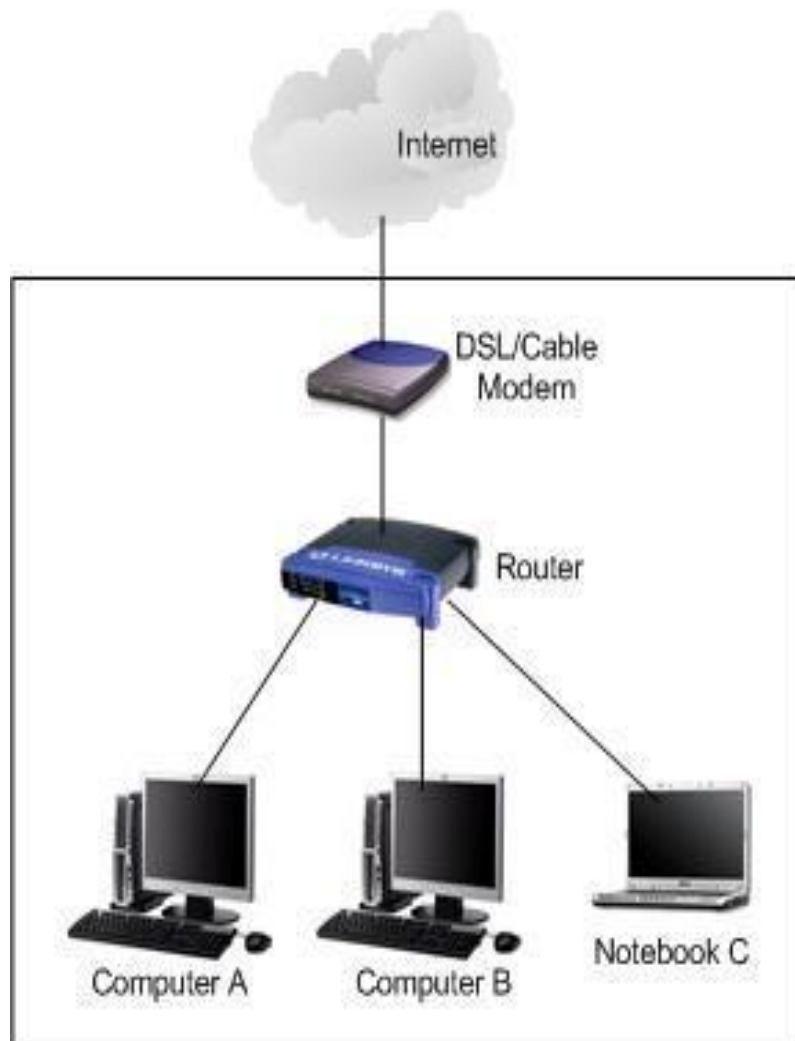
### **13.1. Building Home Network**

Before pushing forward, we made the following assumptions

- i. There is availability of DSL/Cable connection.
- ii. Internet connection can be share with other computers.

The most common home network is Ethernet; it's a very popular LAN (Local Area Network) technology due to its inexpensive setup cost and reasonably fast speed. The other types of network are Token Ring, LocalTalk, and FDDI, but they are not important here. The speed (data transfer rate) of an Ethernet can be 10Mbps (Ethernet), 100Mbps (Fast Ethernet) and 1000Mbps (Gigabit Ethernet). Mbps is called Megabits per seconds. From our opinion, 100Mbps speed might be sufficient for the network set up here.

There is one rule here, make sure all your network devices (router, network card, switch, hub, network cable) are able to support the network with particular speed (10Mbps, 100Mbps, 1000Mbps) which you plan to set up. If you plan to set up a Gigabit Ethernet, although you have 100Mbps' network card, but your router can only support 100Mbps, then the network speed would be 100Mbps. See figure 71 for a usual network topology.



**Figure 71: Usual network topology**

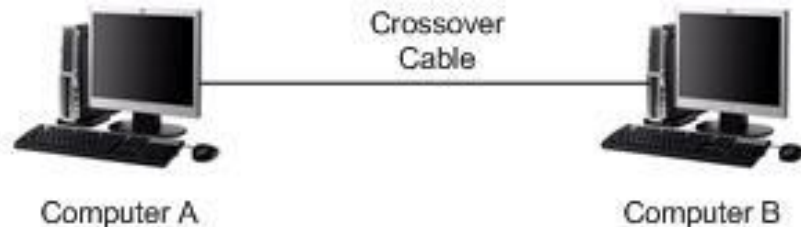
### **13.2. Direct Connection of Two Computers**

In this section we give the procedure for connectivity of two computers sometimes for file or printer sharing?

The two major network device required are: crossover cable and network cards. This is wired connection approach' it's effective and simple way if you want to connect the computers temporary. If the network card on computers supports auto MDI/MDIX feature, you could use crossover or straight through network cable to connect both computers. If not, crossover cable is needed.

## Procedure

1. Plug in network card each to computer and then connect the network cable to both computers' network card. See figure 72.



**Figure 72: Direct connection of two computers**

## Network configuration

We assumed that network card on both computer are installed and working properly, for the network configuration, we create a simple network by assigning following IP address and subnet mask settings to each computer's network card, so that both computers know how to talk to each other:

### **Computer A:**

IP Address: 10.1.1.1

Subnet mask: 255.255.255.0

Gateway: [leave-it-blank]

DNS Servers: [leave-it-blank]

### **Computer B:**

IP Address: 10.1.1.2

Subnet mask: 255.255.255.0

Gateway: [leave-it-blank]

DNS Servers: [leave-it-blank]

As these 2 computers are directly connected, no gateway and DNS servers are required to be configured. After assigning IP address, try to ping the other computer from command prompt, you should be able to ping each other and then sharing printers or files as you wish.

## **13.3. Configuring of IP Address and Other Network Information in On Windows 7**

IP address must be configured on computer in order to communicate with other computers, because this IP address



is the standard address understood by computers and other networking devices in networking world. We can configure IP address, subnet mask, gateway and DNS servers manually on computer, we can also configure computer to obtain IP address and other network information from DHCP server (most of the time is configured on router).

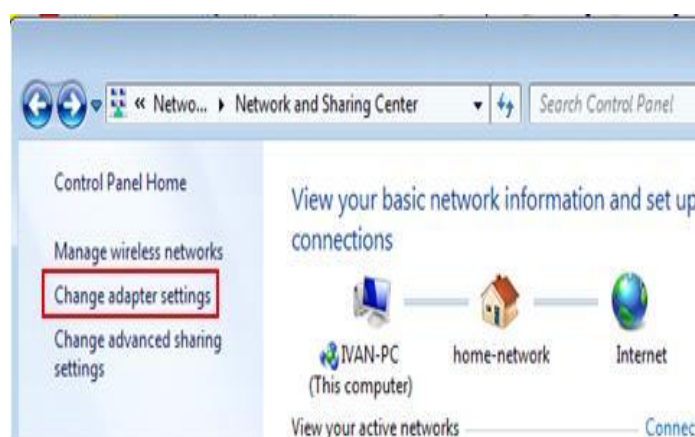
### Procedure

1. Go to Start and click on Control Panel.
2. Click View network status and tasks in Control Panel window. See figure 73.



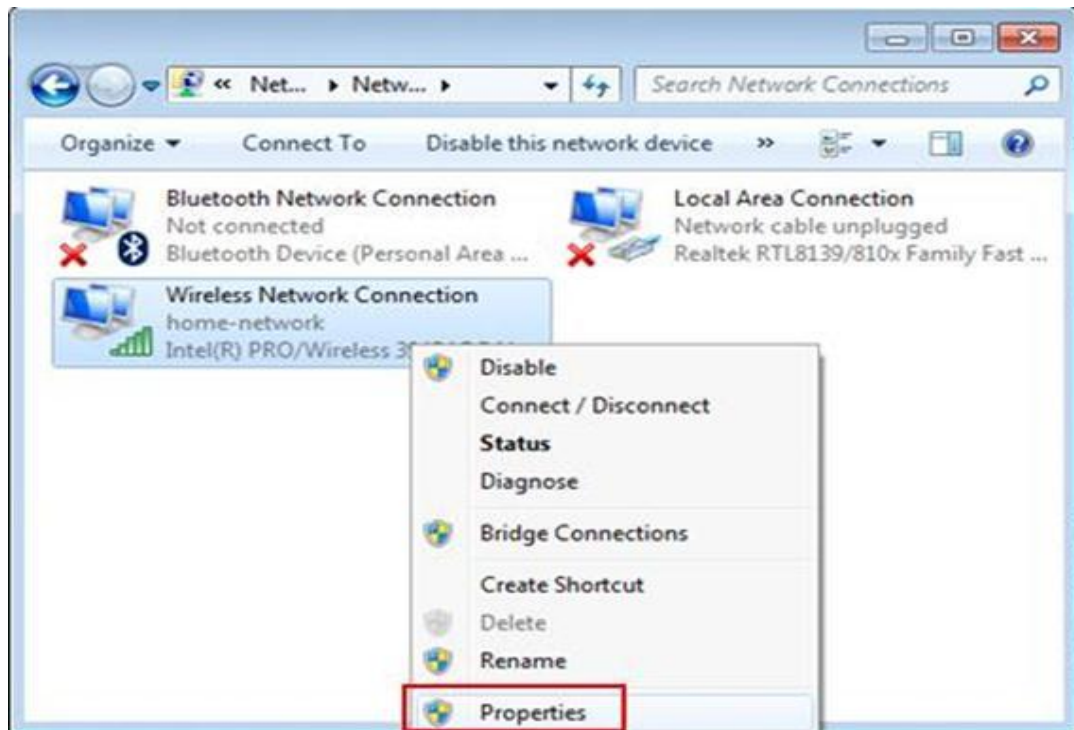
**Figure 73: Control Panel Window**

3. Network and Sharing Center window will appear, and then click change adapter settings. See figure 74.



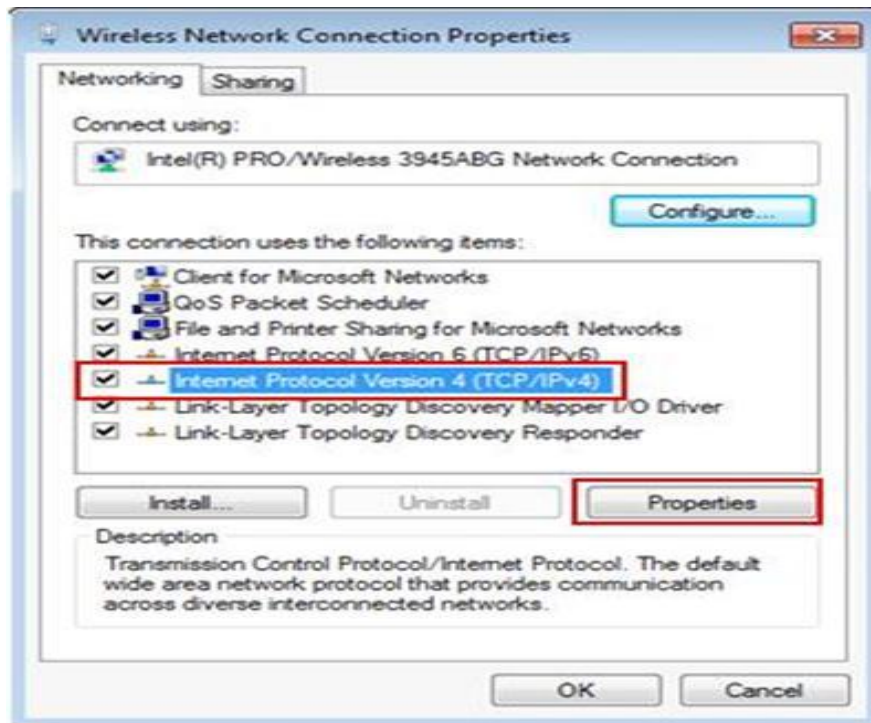
**Figure 74: Network and Sharing Center window**

4. Network Connections window will appear. Here you can right click on the network adapter (can be wireless adapter or wired Ethernet adapter) that you wish to configure and click Properties. See figure 75.



**Figure 75: Network Connections window**

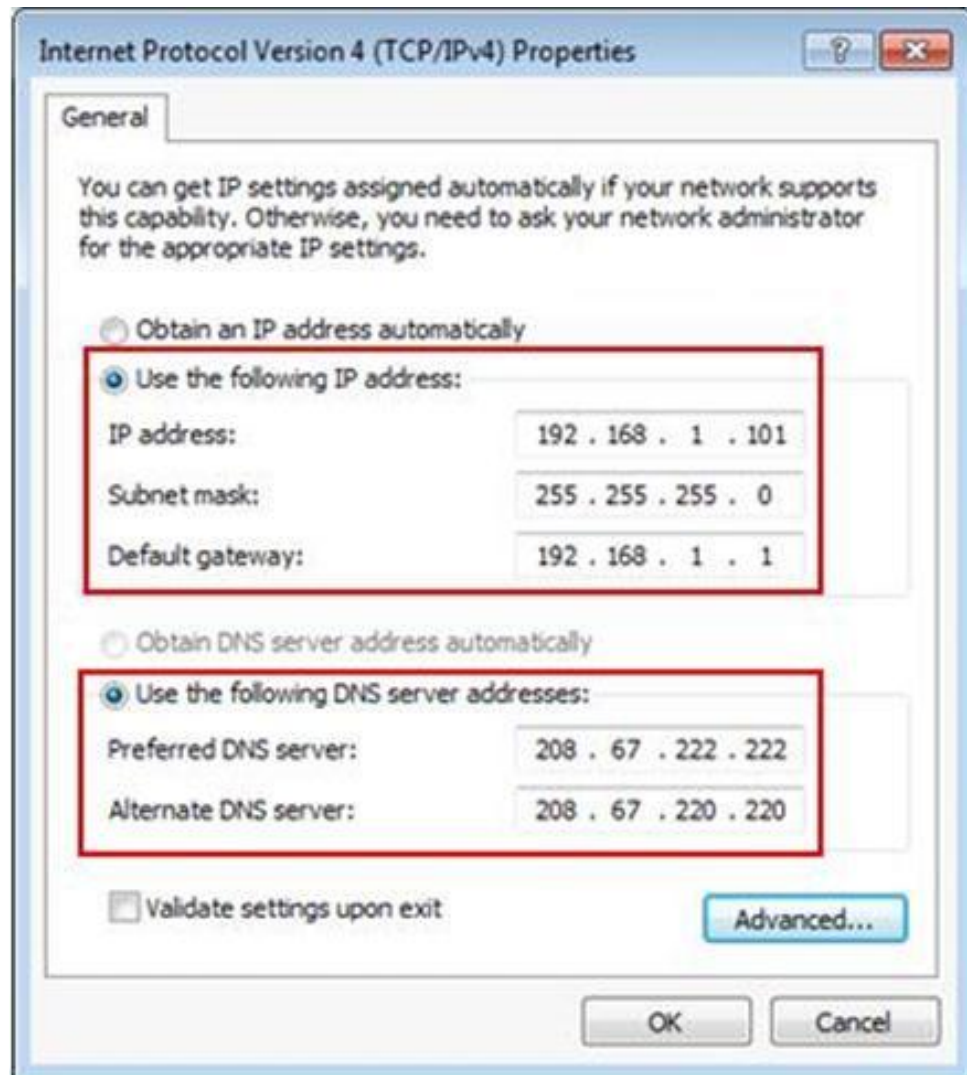
5. In the Network Connection Properties window, tick on Internet Protocol Version 4 (TCP/IPv4) and click Properties. See figure 76.



**Figure 76: Network Connection Properties window**

## **6. Assigning IP Address**

- a) After clicking properties, TCP/IPv4 window appear. (See figure 77) For manual IP Assigning we can now key in the IP address, Subnet mask, Default gateway and DNS servers. IP address of your computer must be unique. None of the 2 computers in the same network can share same IP address, because it will cause IP address conflict.



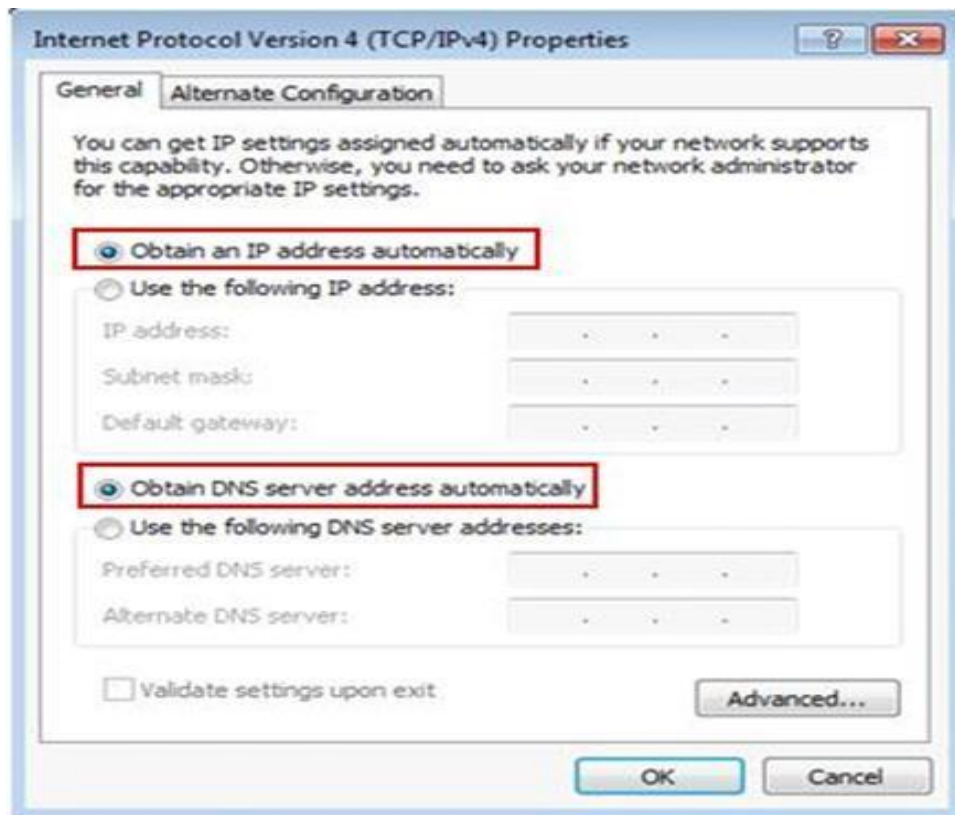
**Figure 77: TCP/IPv4 window**

***Note: Default gateway is a router that can route the traffic to the other network or Internet. DNS server is an application server that can translate URL to IP address. Check with your ISP on what DNS servers you should use. If not, you can try this free Opendns or Google DNSservers.***

**b) IP Assigned by DHCP server**

If you have DHCP server setup on your router or you have dedicated DHCP server, your computer can be assigned IP address and other network information automatically by selecting Obtain an IP address

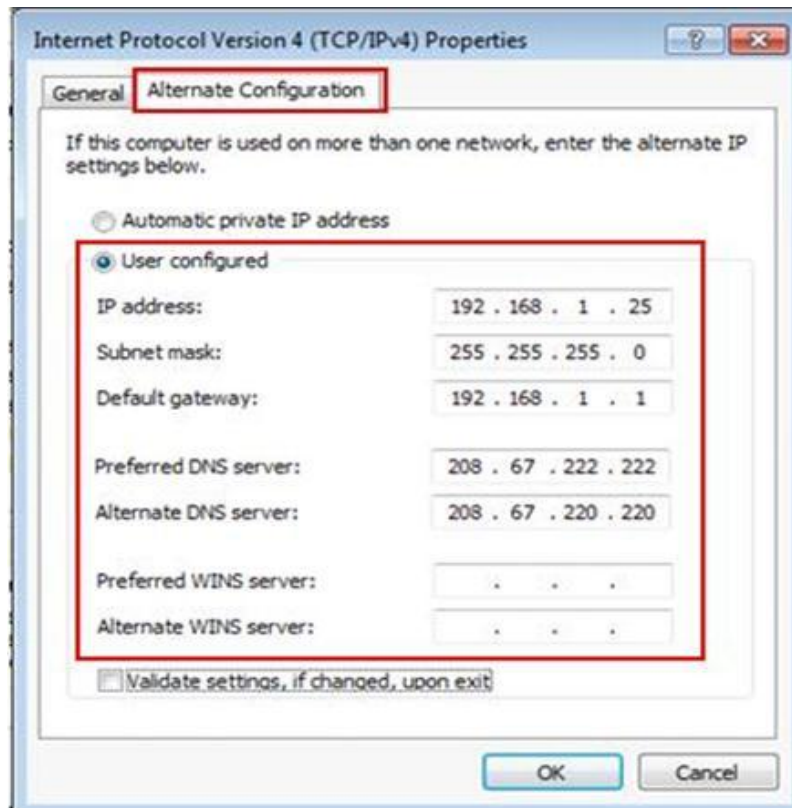
automatically and Obtain DNS server address automatically. See figure 78.



**Figure 78: IP Assigned by DHCP server**

*Note: If you have a laptop, and you use static IP at home and the IP assigned by DHCP server at the office, you can make use of alternate configuration to set IP and network information for these 2 different networks. Set Obtain an IP address and DNS automatically on General Tab as in the figure 79 so that the laptop will be assigned IP addresses automatically at the office. After that, click Alternate Configuration tab, select User configured option and key in your home network's static IP and other network information. By setting this, when there is no IP information assigned due to no DHCP server at home, this alternate configuration will be applied automatically, so that you don't have to spend time on configuring IP manually every time at home.*





**Figure 79: Using alternate configuration**

### **13.4. Physical Network Setup**

We will use D-Link's DI-604 broadband router as an example see figure 80. We can use other type of router according to your needs. Make available some straight network cable as well. Connect the WAN port on router to your cable/DSL modem using straight cable, then connect computers' network card to router's LAN ports using straight cable also. You can connect up to 4 computers to this router. Power on the router after finish connecting, you should be able to see the WAN and LAN lights on the router. Also you need to ensure that your DSL/Cable modem is configured in bridge mode, so that it can work well after connecting to router. Here is how to configure DSL/Cable modem in bridge mode. This is very common setup after you have subscribed new DSL broadband service, you just need to configure the modem as a bridge, and after that configure PPPoE dialer in

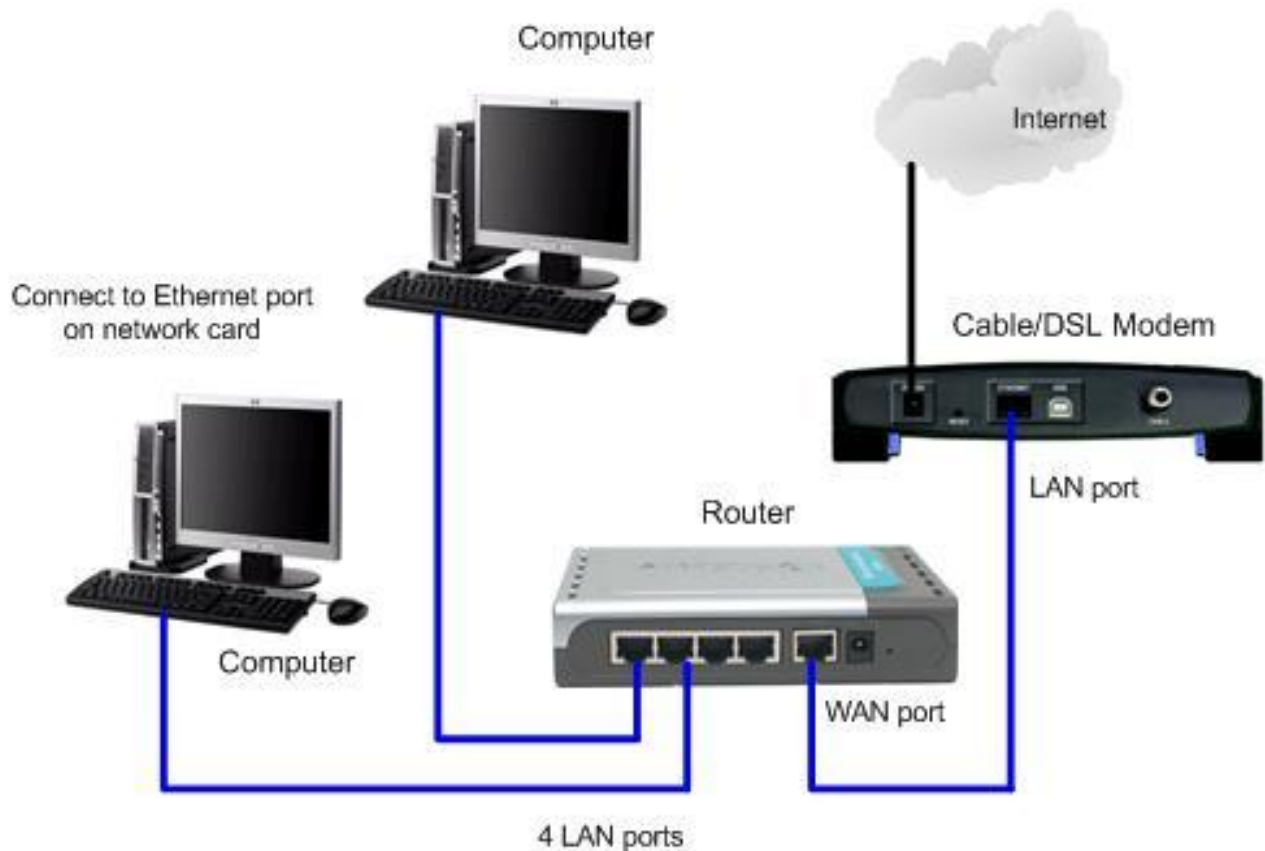
Microsoft Windows by providing username/password or other network information for accessing Internet.

If you plan to connect the modem to router and set up a home network, you must set bridge mode on modem too.

#### Procedure

1. Connect DSL modem's LAN port to computer's network card by using straight through network cable.
2. Read the modem manual, find out the default modem IP address, after that you need to set computer with the IP address in same network with modem, so you can access and configure it. As an example, if the modem IP is 192.168.1.1, I set computer IP as 192.168.1.10 (you can set 192.168.1.X, X= number between 2 and 254), netmask as 255.255.255.0 and gateway as 192.168.1.1.
3. Open a web browser and key in **http://DSL-modem-default-IP**(example: **http://192.168.1.1**) into the address bar, after that hit Enter key.
4. The modem logon screen will appear, type in default username and password you found in modem manual. You will then log on to the modem management page.
5. Go to the correct configuration page by referring to modem manual, and then set the operation mode to Bridge mode. Here is an example:
6. The other important info for modem to work well is Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI), you need to set these numbers correctly. If you get the modem from ISP, most likely it's been pre-configured correctly.
7. Ok, at this stage you have done the modem configuration, you can then proceed to configure PPPoE dialer on connected computer. If you need help, here is PPPoE dialer setup in Windows 7, Vista and XP. If this modem is connected to router (wireless or

wired), you can then proceed to configure that wireless router or Ethernet wired route.



**Figure 80: Physical Network Setup with D-Link's DI-604 broadband router**

### 13.5. IP Logical Network Design

This is one of the task which we need to do is do after we have set up a network (wired or wireless) at home. This is the process to decide the IP addresses, netmask for computers, router and other network devices. Since each IP address assigned to your computer must be unique, you can't simply assign an IP address to your computer.

Here are 3 recommended IP ranges we can used in our network. These 3 blocks of private IP address space are reserved by Internet Assigned Numbers Authority (IANA) for private network, such as home network. The three (3) Private



IP address space: 10.0.0.0 - 10.255.255.255; 172.16.0.0 - 172.31.255.255; and 192.168.0.0 - 192.168.255.255. We can use the private IP address space in our network without worrying of conflict with the IP addresses in Internet.

After deciding the IP addresses to be used, the next is to decide what netmask to be used. Netmask will decide how many IP addresses available to be used in our network. Let use 255.255.255.0 for having 254 addresses to be assigned. There is a network address and broadcast address which can't be used for IP assigning. Network address is used to represent that particular created network, whereas broadcast address is used to talk to all computers in that particular network. Below are some examples for assigning IP addresses in on network.

#### Example 1: 5 computers and a router on network

Let us assign 10.0.0.1 to the router, 10.0.0.2 – 10.0.0.6 to other 5 computers. We use netmask 255.255.255.0 for this network, so that we can assign IP addresses 10.0.0.1 - 10.0.0.254 in the network. Network address is 10.0.0.0, broadcast address is 10.0.0.255.

#### Example 2: 8 computers, 2 notebooks and a router on network

Let us assign 172.16.10.1 to the router, 172.16.10.2 – 172.16.10.9 to other 8 computers and 172.16.10.10 – 172.16.10.11 to other 2 notebooks. We will use netmask 255.255.255.0 for this network, so that we can assign IP addresses 172.16.10.1 – 172.16.10.254 in the network.

Network address is 172.16.10.0, broadcast address is 172.16.10.255.

**Example 3: 8 computers, a router and a network printer on network**

Let us assign 192.168.1.1 to the router, 192.168.1.2 to the network printer and 192.168.1.3 –192.168.1.10 to other 8 computers. we use netmask 255.255.255.0 for this network, so that we can assign IP addresses 192.168.1.1 – 192.168.1.254 in the network. Network address is 192.168.1.0, broadcast address is 192.168.1.255.

### **13.6. Review Questions**

1. Describe the procedure to connect two computer systems with only network card and cross over cable.
2. Under what condition can we use straight through network cable for connecting two computer systems.
3. Describe procedure for Configuring of IP Address on window 7
4. Describe how you can setup IP Logical Network Design for (1) 10 computers, 2 notebooks and a router on network; (2) 12 computers, a router and a network printer on network. Private IP addresses space: 10.0.0.0 - 10.255.255.255.
5. Why is it important to configure modem in bridge mode when setting up network? Hence describe the procedure to configure modem in bridge mode.

# CHAPTER FOURTEEN

## NETWORKING TROUBLESHOOTING

### 14.1. Networking Troubleshooting Steps

When problems occurred in our network, there are one or more step the troubleshooter must follow. Some of these steps are:

**Check the Cords & Power:** The first thing you should always do is check to make sure everything is plugged in: your computer, router, device, etc. Many laptops have a button to turn off the wireless connection; the icon looks like a signal tower. When in doubt, read the manual.

**Ping Yourself:** You want to test that your machine is working properly. To do this, you want to ping yourself. You use the loop-back address (127.0.0.1) to do this. Pinging the loop-back address tests to make sure software on your computer is working properly. Typically, if something is not working at this stage, you may just need to restart your computer.

**Ping Your Router (AKA: the Default Gateway):** The next step would be to ping your router. You can find your router's IP address with ipconfig as well (it should be on the bottom of the unit and listed in the manual too). Remember that ipconfig lists your router as the "Default Gateway." It is very likely to be 192.168.1.1 or a similar number. This is done to test if your router is responding. If it is not, and you have already checked to make sure it is on, then it may need to be turned off and turned on. Every once in a while it may need a refresh.

If the problem continues, contact your ISP for assistance to see if they can help.

**Ping Yourself with Your IP Address:** We want to test to make sure everything is working correctly between your router and your computer. To do this, ping your IP address. It is listed in the ipconfig command at the same time the router IP number is. If this works, you can be confident that a problem is outside your network.

**Ping and Tracert outside Your Network:** From here, you want to test something outside your network. In a medium or larger network setting, a server on another branch of the network will do. For a home network, the Internet is often your only option. Since chances are the problem is that one or more websites are (or seem) down, this is a logical thing to check. You can use a few different tools. First try the ping command because it is the fastest. It will only tell you if the site is working or not. For more detailed information, use tracert and pathping. They can give a better idea of what is going on. For instance, if you can reach your router, but no further, the node that connects you to the Internet may be down: an ISP issue. If you can reach only a couple (one or two) steps past your router, then it still is probably an ISP issue. Your Internet is down.

## **14.2. Ways to check if a website is down**

Some of the ways to check if a website is down are.

**Ping:** A ping basically sends a Hello to a server waiting for a response. If the response takes too long a timeout will occur. Ping is measured in ms, if it is incredibly high something is wrong with either your computer, the route in between or the destination. The command is similar in Windows and Linux,

just enter ping destination, with destination being an IP or domain name, and wait for the response.

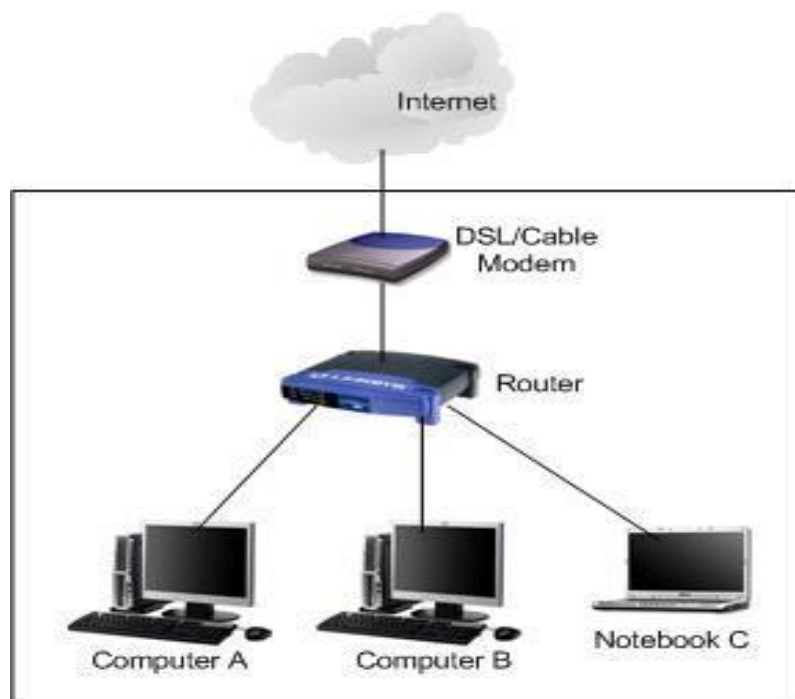
**Traceroute:** You can compare Tracerouter with a list of all the roads that you travel until you reach your destination. Only that the roads are the servers in this case that your data is send through to reach their destination. If everything is fine the destination server should appear at the end, if it is not you could get timeouts for instance. Tracert is the command that you can use in Windows to trace the route between your computer and the destination. Use the command “tracert IP” or “tracert domain” to achieve this. Traceroute is the equivalent in Linux.

**Domain Name System (DNS):** DNS errors most of the time occur when a website is freshly registered or moving to another server. It usually takes some time to update the DNS records to point at the new server. DNS is providing information much like your phone book is. Domain names are for us puny humans who have troubles remembering those server IP addresses (64.233.161.18 for Google for instance). Problems occur when the Nameservers who translate the human entered domain names into IP addresses have still the old IP in their records while the website is already up and running on the new IP. You can use the online script DNS Report to receive a detailed report. Green results are fine, red ones point to failures and yellow ones are warnings.

**Proxies:** Proxy's can be used to establish connections to websites even if the direct route from your computer to theirs is somehow blocked. You can compare that to visiting a friend and using his computer to connect to a server that you cannot connect to. If it works it is somehow related to your computer or connection.

### 14.3 Troubleshoot Network Problem With “ping” Command

Ping is a program used to check whether a host is up and active in network. It is commonly used to troubleshoot network problem. Figure 81 is typical home wired network design, let's explore how to use this ping tool to troubleshoot network problem and find the root cause.

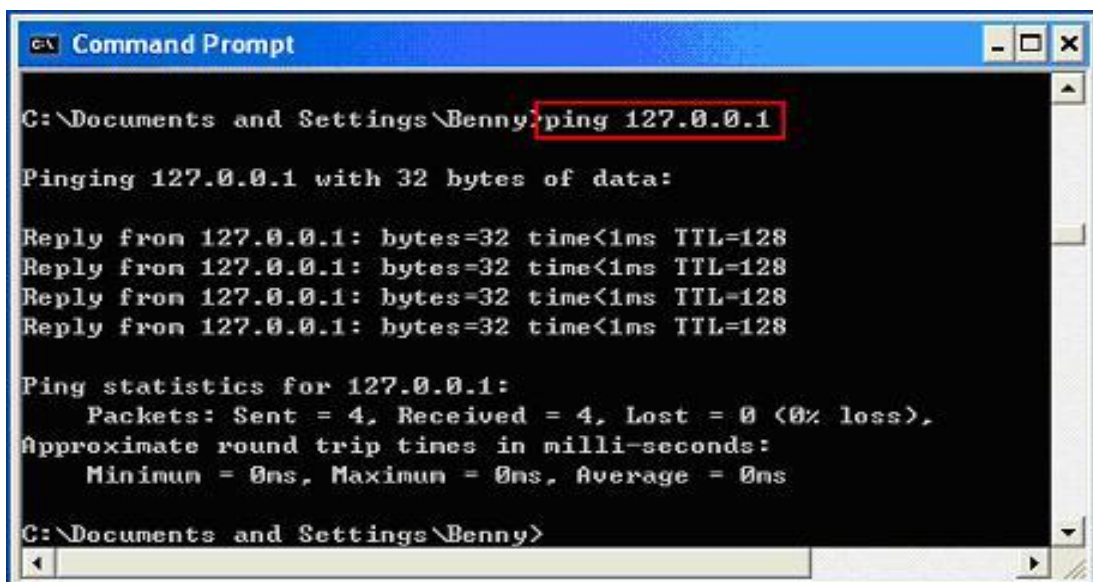


**Figure 81: A typical home wired network**

- i. First thing you need to do is to make sure there is light on network card with cable connected. Sometimes network down is due to disconnected network cable or loose cable connection. If you notice no light on your network card after connecting with network cable, make sure the network cable is working and router that connected by this computer is up and active. If you see the light, then proceed to step 2.

**Note:** You need to make sure the network cable is connected to router's LAN port

2. Go to Start and click on Run.
3. Run window will appear. Type in cmd on Run window and click OK.
4. Key in ping 127.0.0.1 in Command Prompt window. This is network card loopback address. If you receive Reply from 127.0.0.1, it works. If you receive Request timed out, it means network card doesn't work properly. Unplug and re-seat the network card, connect with network cable then ping loopback address again. If still fails, check the network card driver status in Windows 7, Vista or XP to troubleshoot network card and make sure the card works well. If still fails, most probably the network card cannot be used anymore. Try again by using other network cards. However if you just cannot install network card driver correctly on this computer but it works on other computer, then maybe there is problem on Microsoft Windows OS or its TCP/IP function.



```
C:\Documents and Settings\Benny>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Benny>
```

5. Ok, now you can proceed to ping your computer IP address. If you are not sure about computer IP, use ipconfig to find out. If you fail to ping this IP or no IP is configured on computer, check network configuration such as IP address (assigned manually or automatically?), subnet mask, gateway on network card to make sure it's configured correctly.
6. If you are able to ping loopback address and your computer IP, proceed to ping router LAN IP address. If you receive Request timed out, make sure router is up and configured properly with correct IP, subnet mask, DHCP and other network settings.

*Note: Ensure that your DSL/Cable modem is configured in bridge mode (not routing mode), so that it can work well after connecting to router. Even if router is up and it's configured properly, you need to check and ensure the computer is connected to correct and working router LAN port too, sometimes it might be connected to faulty port or incorrect port (such as uplink port). If you have enabled firewall on router, make sure firewall is configured correctly without dropping legitimate network packets.*

7. If you can ping the router IP, then you should be able to ping the other computers or notebook in your network. If you still fail to ping the router IP or other computers, then you can take a look on this wired home network setup tutorial in order to get more helps.
8. If you have successfully done above steps and all are working properly, but you still fail to connect to Internet, then check your DSL, cable or wireless modem and router to make sure all cables are connected correctly. Reboot your DSL, cable or



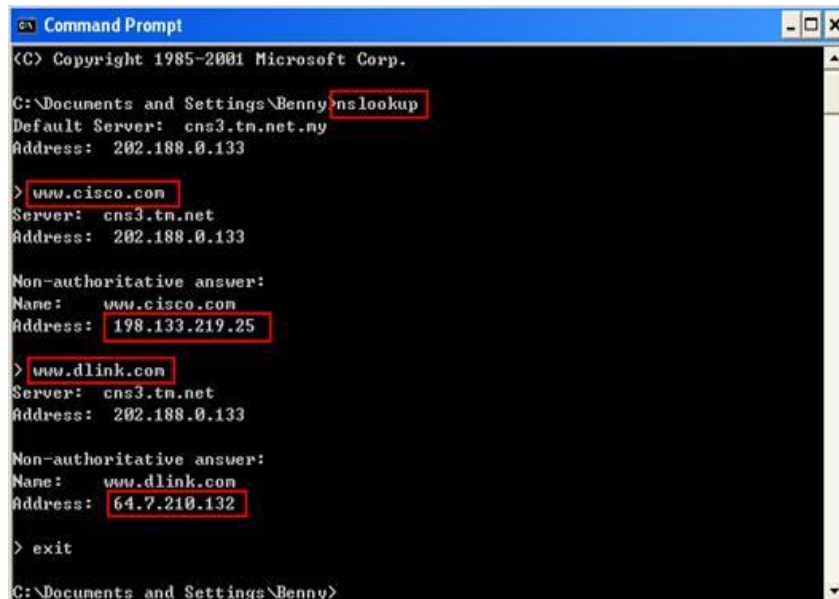
wireless modem and router and try internet access after that.

If still no Internet connection after that, connect computer to modem directly with network cable and test Internet connection. If this works, then I think the problem is on wired router configuration. If this fails too, contact your ISP for getting more helps to troubleshoot this network problem. This might due to some problems at your ISP side sometimes or the modem is broken.

#### **14.4. nslookup**

Sometimes you might find out your computer is connected to network, but just cannot browse Internet websites. So what to do next? Just use nslookup to try resolving the domain name problem. If you wish to know what the IP address is resolved from domain name, you can use **nslookup** command to find out. This command is also useful to check whether the DNS servers configured in Microsoft Windows work well. If the configured DNS server doesn't work well, the webpage will not be displayed on your web browser since the domain names will not be translated to IP addresses successfully.

Type in **nslookup** in command prompt window, you will enter interactive mode with > symbol. It also shows the DNS server (202.188.0.133) is being used to serve the system used in this case (different DNS IP address will be displayed in your command prompt). You can then enter the domain name which you want to check its IP address. For example, enter **www.cisco.com** and press **Enter** key, it will be resolved to 198.133.219.25. In another example, **www.dlink.com** will be resolved to 64.7.210.132. If the domain name can be resolved successfully, that means the configured DNS server works well on your computer. See figure 82.



```
C:\Documents and Settings\Benny>nslookup
Default Server: cns3.tn.net
Address: 202.188.0.133

> www.cisco.com
Server: cns3.tn.net
Address: 202.188.0.133

Non-authoritative answer:
Name: www.cisco.com
Address: 198.133.219.25

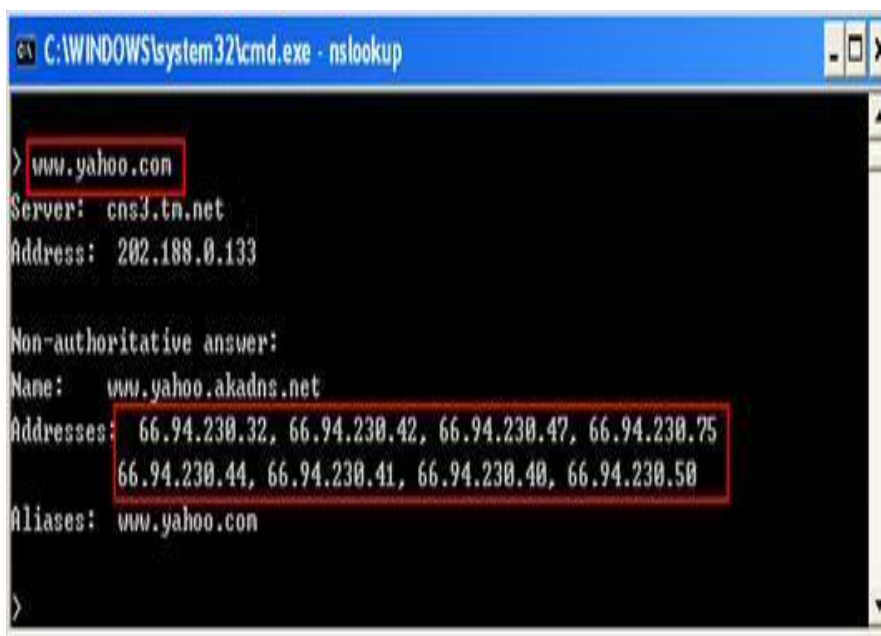
> www.dlink.com
Server: cns3.tn.net
Address: 202.188.0.133

Non-authoritative answer:
Name: www.dlink.com
Address: 64.7.210.132

> exit
C:\Documents and Settings\Benny>
```

**Figure 82: Command Prompt window for nslookup**

Don't feel surprise if sees multiple IP addresses share same domain name. Those domain names are usually popular domain names, such as [www.yahoo.com](http://www.yahoo.com), [www.aol.com](http://www.aol.com), [www.microsoft.com](http://www.microsoft.com), [www.ebay.com](http://www.ebay.com), etc. Usually the main reason of having multiple IP addresses is to load balance the user access to those popular websites.



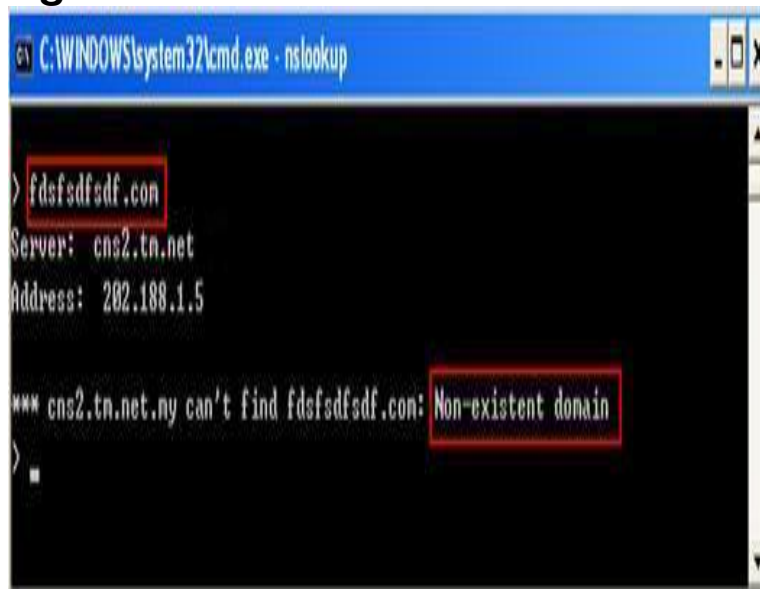
```
C:\WINDOWS\system32\cmd.exe - nslookup

> www.yahoo.com
Server: cns3.tn.net
Address: 202.188.0.133

Non-authoritative answer:
Name: www.yahoo.akadns.net
Addresses: 66.94.230.32, 66.94.230.42, 66.94.230.47, 66.94.230.75
           66.94.230.44, 66.94.230.41, 66.94.230.40, 66.94.230.50
Aliases: www.yahoo.com

>
```

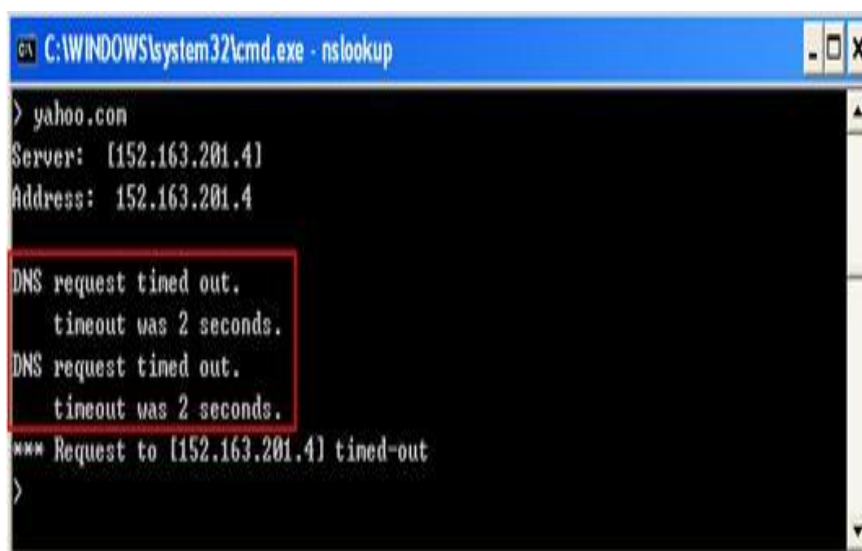
If you enter invalid domain name, the **Non-existent domain** message will be shown.

A screenshot of a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe - nslookup". The user has entered "fdsfsdfsdf.com" at the prompt. The output shows "Server: cns2.tn.net" and "Address: 202.188.1.5". Below that, it says "\*\*\* cns2.tn.net.ny can't find fdsfsdfsdf.com: Non-existent domain". The text "Non-existent domain" is highlighted with a red box.

```
C:\WINDOWS\system32\cmd.exe - nslookup
> fdsfsdfsdf.com
Server: cns2.tn.net
Address: 202.188.1.5

*** cns2.tn.net.ny can't find fdsfsdfsdf.com: Non-existent domain
>
```

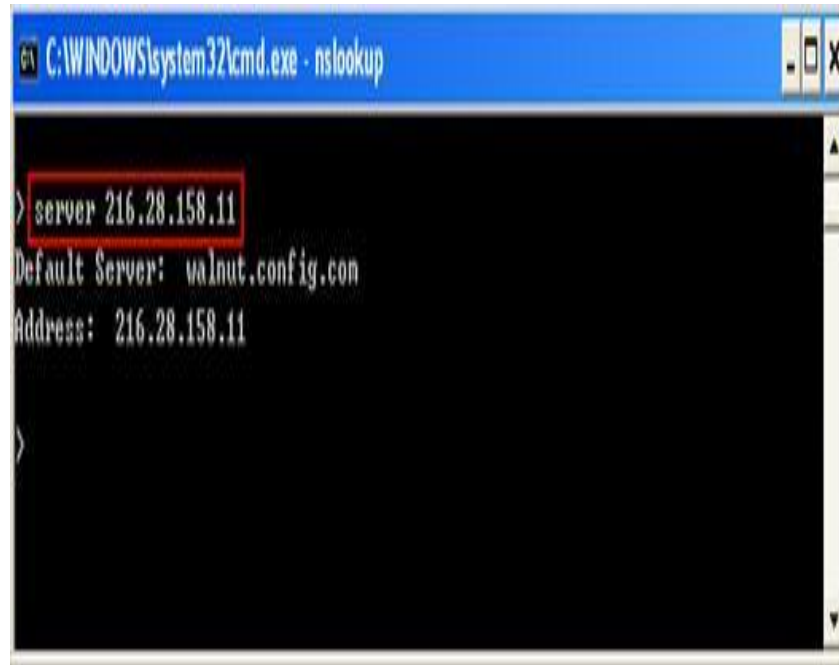
If you receive **DNS request timed out** messages which are shown as below, that means the domain name is failed to be resolved at the time being. The DNS server might be down or not valid, in this case you should try to resolve the domain name by configuring other DNS servers on your computer. If you are not sure which DNS servers to configure, feel free to use these free DNS servers from OpenDNS or Google to resolve domain names.

A screenshot of a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe - nslookup". The user has entered "yahoo.com" at the prompt. The output shows "Server: [152.163.201.4]" and "Address: 152.163.201.4". Below that, it says "DNS request timed out. timeout was 2 seconds." twice, and then "\*\*\* Request to [152.163.201.4] timed-out". The first two lines of the error message are highlighted with a red box.

```
C:\WINDOWS\system32\cmd.exe - nslookup
> yahoo.com
Server: [152.163.201.4]
Address: 152.163.201.4

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to [152.163.201.4] timed-out
>
```

If you wish to check address translation by other DNS servers, such as your secondary DNS server, just enter this command **server new-DNS-server-IP**. I changed to DNS server 216.28.158.11.



```
C:\WINDOWS\system32\cmd.exe - nslookup
> server 216.28.158.11
Default Server: walnut.config.com
Address: 216.28.158.11
>
```

#### 14.5. Review Questions

1. What are Steps towards Networking Troubleshooting
2. Describe Troubleshooting with Ping Commands
3. Describe the procedure for Troubleshoot Network Problem With “ping” Command.
4. On which condition can we require the use of nslookup command in network problem troubleshooting?

## **Bibliography**

- Alberto Leon-Garcial and Indra Widjaja. Communication Networks, Fundamental Concepts and Key Architecture. Second Edition, McGraw-Hill Publishing Company, New dehlhi 2004
- Bertsekas, D. and R. Gallager, Data Networks, Prentice-Hall, Englewood Cliffs, 1992
- Clack, M. P., Network and Telecommunication: Design and Operation, John Willey and Sons, New York, 1997.
- Jain, B. N. and A.K. Agrawala. Open System Interconnection: Its architecture and Protocol. McGraw-Hill. New York 1993
- William Buchanan, Distributed Systems and Networks, McGraw-Hill Publishing Company, 2000.
- Yekini and Lawal 2010, Introduction to ICT and data Processing, Hasfem Publication Nigeria.
- Yekini et al, 2007. Fundamental of Computing, Hasfem Publication Nigeria.
- Bello, O and Adebari, F. A. (2012) "Data communication and Networking", Tony Terry Prints, Lagos, Nigeria.