NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF SCIENCE AND TECHNOLOGY

COURSE CODE: CIT 305

COURSE TITLE: NETWORKING AND COMMUNICATION TECHNOLOGY

COURSE GUIDE

CIT 305: NETWORKING AND COMMUNICATION TECHNOLOGY

Course Developer	Dr A. S. Sodiya Dept. of computer Science University of Agriculture, Abeokuta
Course Co-ordinator	Afolorunso, A. A. National Open University of Nigeria Lagos.

NATIONALOPENUNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Annex
245 Samuel AdesujoAdemulegun Street
Central Business District
Opposite Arewa Suites
Abuja

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

National Open University of Nigeria 2009

First Printed 2009

ISBN

Printed by ……………..
For
National Open University of Nigeria

TABLE OF CONTENTS PAGE

Introduction

CIT 305 – Networking and Communication Technology is a three [3] credit unit course of fifteen units. It teaches the various forms of Networking, Network Design, Communication technology used by people to accomplish different organizational or individual task.

It also gives an insight into various forms of computer networking ranging from the LAN to the WAN and even go as far as looking into the wireless networks that are in use in today's technology. The course also explain the Enterprise Network, which forms a branchcomputer networking technology.

This course is divided into five modules. The first module deals with the introduction to networking concept, data links, physical media used in networking and the network protocol.

The second module deals with the network design, building internetworks using TCP/IP and Routers, Telecommunication Circuits and Features of Best Security in Computer networks.

The third module deals with Enterprise Network, Network Standards and Background of Advanced WAN and LAN

The fourth module deals with Communication Technology, Signal Transmission analysis, Multiplexers, Modulation Concepts, Transmission impairment.

The fifth module deals with various network technologies which includes ISDN, DSL, SONET and it also deals with packet switching.

This Course Guide gives you a brief overview of the course content, course duration, and course materials.

What you will learn in this course

The main purpose of this course is to provide the necessary tools for designing and managing Information Systems. It makes available the steps and tools that will enable you to make proper and accurate decision on Database designs and operations whenever the need arises. Thus, we intend to achieve through the following:

Course Aims

I. Introduce the concepts associated with Information systems development;
II. Provide necessary tools for analyzing, designing, developing a Database of any size;
III. Provide you with the necessary foundation in Database programming
IV. Introduction of Web services and their architectural frameworks; and
V. Provide you with the necessary foundation on the use of XML

Course Objectives

Certain objectives have been set out to ensure that the course achieves its aims. Apart from the course objectives, every unit of this course has set objectives. In the course of the study, you will need to confirm, at the end of each unit, if you have met the objectives set at the beginning of each unit. By the end of this course you should be able to:

- Explain the fundamental of Networking
- Explain the term "Data links"
- Explain Network Protocols
- Understand the Building of Internetworks using TCP/IP and Routers
- Explain the Network Standards (IEEE 802 Standards)
- Know the fundamentals of Enterprise Network
- What is involved in Signal Transmission and Impairment
- Explain Digital Technologies
- Understand the concept behind Packet Switching

Working Through This Course

In order to have a thorough understanding of the course units, you will need to read and understand the contents, practise the steps by designing an Information system of your own, and be committed to learning and implementing your knowledge.

This course is designed to cover approximately seventeen weeks, and it will require your devoted attention. You should do the exercises in the Tutor-Marked Assignments and submit to your tutors.

Course Materials

These include:
1. Course Guide
2. Study Units
3. Recommended Texts
4. A file for your assignments and for records to monitor your progress.

Study Units

There are Twenty three study units in this course:

MODULE ONE	**NETWORKING**
UNIT 1:	Introduction to Networking
UNIT 2:	Constructing data links
UNIT 3:	Deploying Physical Media/Network Media
UNIT 4:	Network Protocols

MODULE TWO	**NETWORK DESIGN**
UNIT 1	Harnessing WiFi for user mobility
UNIT 2	Building Internetworks using TCP/IP and Routers
UNIT 3	Utilizing Telecommunication Circuits

UNIT 4	Implementing Security best practices
MODULE THREE	**ENTERPRISE NETWORK**
UNIT 1	Creating Enterprise Network
UNIT 2	Planning and Selection of Enterprise Network
UNIT 3	Network Standards (IEEE 802 Standards)
UNIT 4	Applications of data communication and networks
UNIT 5	Background of Advanced WAN and LAN Classes
MODULE FOUR	**COMMUNICATION TECHNOLOGY**
UNIT 1	Signal Transmission Analysis
UNIT 2	Modem and Modulation Concept
UNIT 3	Multiplexers
UNIT 4	Digital Technologies
UNIT 5	Transmission Impairment
MODULE FIVE	**NETWORK TECHNOLOGIES**
UNIT 1	ISDN
UNIT 2	DSL
UNIT 3	SONET
UNIT 4	Packet Switching
UNIT 5	Internet and TCP/IP

Make use of the course materials, do the exercises to enhance your learning.

Textbooks and References

- Prasad, K. V. (2009). “Principles of Digital Communication Systems and Computer Networks”, Dreamtech Press.
- "How does the Internet Work?".http://tldp.org/HOWTO/Unix-and-Internet-Fundamentals-HOWTO/internet.html. Retrieved June 15, 2009.
- JohnaTill Johnson. "Net was born of economic necessity, not fear". http://www.networkworld.com/columnists/2004/0607johnson.html. Retrieved June 15, 2009.URL is sufficient attribution
- Leonard Kleinrock (2005). *The history of the Internet*. http://www.lk.cs.ucla.edu/personal_history.html. Retrieved 2009-05-28.
- Hafner, Katie (1998). *Where Wizards Stay Up Late: The Origins Of The Internet.*
- McGraw Hill - All in One CompTIA A+ Certification Exam Guide - Sixth Edition 2007 (Mike Meyers)
- http://www.apan.net/meetings/busan03/cs-history.htm. Retrieved December 25, 2005.David Roessner, Barry Bozeman, Irwin Feller, Christopher Hill, Nils Newman (1997). *The Role of NSF's Support of Engineering in Enabling Technological Innovation*. http://www.sri.com/policy/csted/reports/techin/inter2.html. Retrieved 2009-05-28.
- "RFC 675 - Specification of internet transmission control program". Tools.ietf.org. http://tools.ietf.org/html/rfc675. Retrieved 2009-05-28.
- Tanenbaum, Andrew S. (1996). *Computer Networks*. Prentice Hall. ISBN 0-13-394248-1.
- Hauben, Ronda (2004). "The Internet: On its International Origins and Collaborative Vision". *Amateur Computerist* **12** (2). http://www.ais.org/~jrh/acn/ACn12-2.a03.txt. Retrieved 2009-05-29.
- J. R. Barry, E. A.Lee, D. G.Messerschmidt, Digital Communication, Kluwer Academic Publishers, 2004.

Assignments File

These are of two types: the self-assessment exercises and the Tutor-Marked Assignments. The self-assessment exercises will enable you monitor your performance by yourself, while the Tutor-Marked Assignment is a supervised assignment. The assignments take a certain percentage of your total score in this course. The Tutor-Marked Assignments will be assessed by your tutor within a specified period. The examination at the end of this course will aim at determining the level of mastery of the subject matter. This course includes twelve Tutor-Marked Assignments and each must be done and submitted accordingly. Your best scores however, will be recorded for you. Be sure to send these assignments to your tutor before the deadline to avoid loss of marks.

Presentation Schedule

The *Presentation Schedule* included in your course materials gives you the important dates for the completion of tutor marked assignments and attending tutorials. Remember, you are required to submit all your assignments by the due date. You should guard against lagging behind in your work.

Assessment

There are two aspects to the assessment of the course. First are the tutor marked assignments; second, is a written examination.

In tackling the assignments, you are expected to apply information and knowledge acquired during this course. The assignments must be submitted to your tutor for formal assessment in accordance with the deadlines stated in the Assignment File. The work you submit to your tutor for assessment will count for 30% of your total course mark.

At the end of the course, you will need to sit for a final three-hour examination. This will also count for 70% of your total course mark.

Tutor Marked Assignments (TMAS)

There are twelve tutor marked assignments in this course. You need to submit all the assignments. The total marks for the best four (4) assignments will be 30% of your total course mark.

Assignment questions for the units in this course are contained in the Assignment File. You should be able to complete your assignments from the information and materials contained in your set textbooks, reading and study units. However, you may wish to use other references to broaden your viewpoint and provide a deeper understanding of the subject.

When you have completed each assignment, send it together with form to your tutor. Make sure that each assignment reaches your tutor on or before the deadline given. If, however, you cannot complete your work on time, contact your tutor before the assignment is done to discuss the possibility of an extension.

Examination and Grading

The final examination for the course will carry 70% percentage of the total marks available for this course. The examination will cover every aspect of the course, so you are advised to revise all your corrected assignments before the examination.

This course endows you with the status of a teacher and that of a learner. This means that you teach yourself and that you learn, as your learning capabilities would allow. It also means that you are in a better position to determine and to ascertain the what, the how, and the when of your language learning. No teacher imposes any method of leaming on you.

The course units are similarly designed with the introduction following the table of contents, then a set of objectives and then the dialogue and so on.

The objectives guide you as you go through the units to ascertain your knowledge of the required terms and expressions.

Course Marking Scheme

This table shows how the actual course marking is broken down.

Assessment	**Marks**
Assignment 1- 4	Four assignments, best three marks of the four

	count at 30% of course marks
Final Examination	70% of overall course marks
Total	100% of course marks

Table 1: Course Marking Scheme

Course Overview

Unit	Title of Work	Weeks Activity	Assessment (End of Unit)
	Course Guide	Week 1	
	Module 1		
1	Introduction to Networking	Week 1	Assignment 1
2	Data links	Week 2	Assignment 2
3	Deploying Physical Media	Week 3	Assignment 3
4	Network Protocols	Week 4 - 5	Assignment 4
	Module 2		
1	Harnessing WiFi for user mobility		
2	Building Internetworks using TCP/IP and Routers		
3	Network Standards (IEEE 802 Standards)	Week 8	Assignment 7
4	Implementing Security best practices	Week 9	Assignment 8
	Module 3		
1	Creating Enterprise Network	Week 11	Assignment 10
2	Planning and Selection of Enterprise Network		
3	Advanced WAN and LAN Classes	Week 12	Assignment 11
	Module 4		
1	Modem and Modulation Concepts	Week 14	Assignment 13
2	Multiplexers	Week 15	Assignment 14
3	Digital Technologies	Week 15	
	Revision	Week 16	
	Examination	Week 17	
Total		15 weeks	

How to get the best from this course

In distance learning the study units replace the university lecturer. This is one of the great advantages of distance learning; you can read and work through specially designed study materials at your own pace, and at a time and place that suit you best. Think of it as reading the lecture instead of listening to a lecturer. In the same way that a lecturer might set you some reading to do, the study units tell you when to read your set books or other material. Just as a lecturer might give you an in-class exercise, your study units provide exercises for you to do at appropriate points.

Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit and how a particular unit is integrated with the other units and the course as a whole. Next is a set of learning objectives. These objectives enable you know what you should be able to do by the time you have completed the unit. You should use these objectives to guide your study. When you have finished the units you must go back and check whether you have achieved the objectives. If you make a habit of doing this you will significantly improve your chances of passing the course.

Remember that your tutor's job is to assist you. When you need help, don't hesitate to call and ask your tutor to provide it.

1. Read this *Course Guide* thoroughly.

2. Organize a study schedule. Refer to the 'Course Overview' for more details. Note the time you are expected to spend on each unit and how the assignments relate to the units. Whatever method you chose to use, you should decide on it and write in your own dates for working on each unit.

3. Once you have created your own study schedule, do everything you can to stick to it. The major reason that students fail is that they lag behind in their course work.

4. Turn to *Unit 1* and read the introduction and the objectives for the unit.

5. Assemble the study materials. Information about what you need for a unit is given in the 'Overview' at the beginning of each unit. You will almost always need both the study unit you are working on and one of your set of books on your desk at the same time.

6. Work through the unit. The content of the unit itself has been arranged to provide a sequence for you to follow. As you work through the unit you will be instructed to read sections from your set books or other articles. Use the unit to guide your reading.

7. Review the objectives for each study unit to confirm that you have achieved them. If you feel unsure about any of the objectives, review the study material or consult your tutor.

8. When you are confident that you have achieved a unit's objectives, you can then start on the next unit. Proceed unit by unit through the course and try to pace your study so that you keep yourself on schedule.

9. When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment is returned, pay particular attention to your tutor's comments, both on the tutor-marked assignment form and also written on the assignment. Consult your tutor as soon as possible if you have any questions or problems.

10. After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in this *Course Guide*).

Tutors and Tutorials

There are 15 hours of tutorials provided in support of this course. You will be notified of the dates, times and location of these tutorials, together with the name and phone number of your tutor, as soon as you are allocated a tutorial group.

Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulties you might encounter and provide assistance to you during the course. You must mail or submit your tutor-marked assignments to your tutor well before the due date (at least two working days are required). They will be marked by your tutor and returned to you as soon as possible.

Do not hesitate to contact your tutor by telephone, or e-mail if you need help. The following might be circumstances in which you would find help necessary. Contact your tutor if:

- you do not understand any part of the study units or the assigned readings,
- you have difficulty with the self-tests or exercises,
- you have a question or problem with an assignment, with your tutor's comments on an assignment or with the grading of an assignment.

You should try your best to attend the tutorials. This is the only chance to have face to face contact with your tutor and to ask questions which are answered instantly. You can raise any problem encountered in the course of your study. To gain the maximum benefit from course tutorials, prepare a question list before attending them. You will learn a lot from participating in discussions actively.

Summary

Information Systems introduces you to the concepts associated with Information systems development which is critical in understanding the various computer technology and data communications technology.The content of the course material was planned and written to ensure that you acquire the proper knowledge and skills for the appropriate situations. Real-life situations have been created to enable you identify with and create some of your own. The essence is to help you in acquiring the necessary knowledge and competence by equipping you with the necessary tools to accomplish this.
We hope that by the end of this course you would have acquired the required knowledge to view Information Systems in a new way.

I wish you success with the course and hope that you will find it both interesting and useful.

Course Code	CIT 305
Course Title	Networking and Communication Technology
Course Developer	Dr A. S. Sodiya Dept. of Computer Science University of Agriculture, Abeokuta
Course Co-ordinator	Afolorunso, A. A. National Open University of Nigeria Lagos.

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Annex
245 Samuel AdesujoAdemulegun Street
Central Business District
Opposite Arewa Suites
Abuja

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

National Open University of Nigeria 2011

First Printed 2011

ISBN

Printed by ……………..
For
National Open University of Nigeria

MODULE FIVE NETWORK TECHNOLOGIES

MODULE 1 NETWORKING

UNIT 1: INTRODUCTION TO NETWORKING

Table of Contents

1.0 INTRODUCTION

Having read through the course guide, you will have a general understanding of what this unit is about and how it fits into the course as a whole. This unit will describe the general concept of Networking, types and its application areas.

2.0 OBJECTIVES

By the end this unit, you should be able to:

- Explain the term Networking system
- Identify the various types of Networking.
- Have good knowledge of the history of Networking
- Describe the areas of work of Networking

3.0 MAIN CONTENT

3.1 OVERVIEW

The concept of a network is pretty simple. A couple of computers have some cable strung between them, and send data back and forth using electrical signaling over the cable. More or less the same as telephones do or, in a very rough sense, like two kids speaking into tin cans connected by a string.

But how does the data actually get from computer A to computer B? How does computer A find the physical location of computer B on the network? If they communicate with electrical signaling, so the data is traveling "at the speed of light", why does it take so long to send a big file across the network?

The internet is not one single being, it is a massive interconnection of hosts such as your computer, and another halfway across the world. We understand that our ISPs provide internet access to our host, but it may not necessarily provide service to the server that you are communicating with. In this case, how does information make its way from your host to the other host and vice versa?

The answer lies in the interconnection of many ISPs themselves. ISPs can be categorised into Tier 1,2 and 3 ISPs. Tier 1 ISPs are major internet service providers that usually sell access to smaller Tier 2 ISPs. Tier 2 ISPs may service entire countries or cities, but not the rest of the world. Tier 3 ISPs are also customers of Tier 2 ISPs, and usually service end users such as yourself. ISPs **peer** with each other to allow data from your host to reach the other host. From this, we understand that data passes through multiple ISPs in order to be delivered from one location to another.

3.2 DEFINITION OF NETWORKING

A computer network, often simply referred to as a network, is a collection of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources.

A network can as well be define as a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

3.3 HISTORY OF COMPUTER NETWORKS

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

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

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

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

1965 Thomas Merrill and Lawrence G. Roberts created the first wide area network (WAN).

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

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

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

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

3.4 PURPOSE OF COMPUTER NETWORKS

Computer networks can be used for a variety of purposes:

Facilitating communications. Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.

Sharing hardware. In a networked environment, each computer on a network may access and use hardware resources on the network, such as printing a document on a shared network printer.

Sharing files, data, and information. In a network environment, authorized user may access data and information stored on other computers on the network. The capability of providing access to data and information on shared storage devices is an important feature of many networks.

Sharing software. Users connected to a network may run application programs on remote computers.

3.5 NETWORK CLASSIFICATION

The following list presents categories used for classifying networks.

3.5.1 CONNECTION METHOD

Computer networks can be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as optical fiber, Ethernet, wireless LAN, HomePNA, power line communication or G.hn.

Ethernet as it is defined by IEEE 802 utilizes various standards and mediums that enable communication between devices. Frequently deployed devices include hubs, switches, bridges, or routers. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium. ITU-T G.hn technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network.

3.5.2 WIRED TECHNOLOGIES

Twisted pair wire is the most widely used medium for telecommunication. Twisted-pair cabling consist of copper wires that are twisted into pairs. Ordinary telephone wires consist of two insulated copper wires twisted into pairs. Computer networking cabling consist of 4 pairs of copper cabling that can be utilized for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 100 million bits per second. Twisted pair cabling comes in two forms which are Unshielded Twisted Pair (UTP) and Shielded twisted-pair (STP) which are rated in categories which are manufactured in different increments for various scenarios.

Coaxial cable is widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminum wire wrapped with insulating layer typically of a flexible material with a high dielectric constant, all of which are surrounded by a conductive layer. The layers of insulation help minimize interference and distortion. Transmission speed range from 200 million to more than 500 million bits per second.

Optical fiber cable consists of one or more filaments of glass fiber wrapped in protective layers. It transmits light which can travel over extended distances. Fiber-optic cables are not affected by electromagnetic radiation. Transmission speed may reach trillions of bits per second. The transmission speed of fiber optics is hundreds of times faster than for coaxial cables and thousands of times faster than a twisted-pair wire.[citation needed]

3.5.3 Wireless technologies

Terrestrial microwave – Terrestrial microwaves use Earth-based transmitter and receiver. The equipment looks similar to satellite dishes. Terrestrial microwaves use low-gigahertz range, which limits all communications to line-of-sight. Path between relay stations spaced approx, 30 miles apart. Microwave antennas are usually placed on top of buildings, towers, hills, and mountain peaks.

Communications satellites – The satellites use microwave radio as their telecommunications medium which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically 22,000 miles (for geosynchronous satellites) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.

Cellular and PCS systems – Use several radio communications technologies. The systems are divided to different geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.

Wireless LANs – Wireless local area network use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. An example of open-standards wireless radio-wave technology is IEEE.

Infrared communication, which can transmit signals between devices within small distances not more than 10 meters peer to peer or (face to face) without anybody in the line of transmitting.

3.6 TYPES OF NETWORKS BASED ON PHYSICAL SCOPE

Common types of computer networks may be identified by their scale.

3.6.1 LOCAL AREA NETWORK

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G.hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines).Typical library network, in a branching tree topology and controlled access to resourcesAll interconnected devices must understand the network layer (layer 3), because they are handling multiple subnets (the different colors). Those inside the library, which have only 10/100 Mbit/s Ethernet connections to the user device and a Gigabit Ethernet connection to the central router, could be called "layer 3 switches" because they only have Ethernet interfaces and must understand IP. It would be more correct to call them access routers, where the router at the top is a distribution router that connects to the Internet and academic networks' customer access routers.The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at speeds up to 10 Gbit/s. This is the data transfer rate. IEEE has projects investigating the standardization of 40 and 100 Gbit/s.

3.6.2 PERSONAL AREA NETWORK

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters. A wired PAN is usually constructed with USB and Firewire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

3.6.3 HOME AREA NETWORK

A home area network (HAN) is a residential LAN which is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a CATV or Digital Subscriber Line (DSL) provider. It can also be referred to as an office area network (OAN).

3.6.4 WIDE AREA NETWORK

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

3.6.5 CAMPUS NETWORK

A campus network is a computer network made up of an interconnection of local area networks (LAN's) within a limited geographical area. The networking equipments (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned (by the campus tenant / owner: an enterprise, university, government etc.).

In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including; academic departments, the university library and student residence halls.

3.6.6 METROPOLITAN AREA NETWORK

A Metropolitan area network is a large computer network that usually spans a city or a large campus.

Sample EPN made of Frame relay WAN connections and dialup remote access.

Sample VPN used to interconnect 3 offices and remote users

3.6.7 ENTERPRISE PRIVATE NETWORK

An enterprise private network is a network build by an enterprise to interconnect various company sites, e.g., production sites, head offices, remote offices, shops, in order to share computer resources.

3.6.8 VIRTUAL PRIVATE NETWORK

A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

3.6.9 INTERNETWORK

An internetwork is the connection of two or more private computer networks via a common routing technology (OSI Layer 3) using routers. The Internet is an aggregation of many internetworks, hence its name was shortened to Internet.

3.6.10 BACKBONE NETWORK

A Backbone network (BBN) A backbone network or network backbone is part of a computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnetworks.A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than the networks connected to it.

A large corporation that has many locations may have a backbone network that ties all of the locations together, for example, if a server cluster needs to be accessed by different departments of a company that are located at different geographical locations. The pieces of the network connections (for example: ethernet, wireless) that bring these departments together is often mentioned as network backbone. Network congestion is often taken into consideration while designing backbones.

Backbone networks should not be confused with the Internet backbone.

3.6.11 GLOBAL AREA NETWORK

A global area network (GAN) is a network used for supporting mobile communications across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off the user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial wireless LANs.

3.6.12 INTERNET

The Internet is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the United States Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW).

Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP addresses) administered by the Internet Assigned Numbers Authority and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

3.6.13 INTRANETS AND EXTRANETS

Intranets and extranets are parts or extensions of a computer network, usually a local area network.

An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications, that is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

An extranet is a network that is limited in scope to a single organization or entity and also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities—a company's customers may be given access to some part of its intranet—while at the same time the customers may not be considered trusted from a security standpoint. Technically, an extranet may also be categorized as a CAN, MAN, WAN, or other type of network, although an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

3.6.14 OVERLAY NETWORK

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay are connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network.

A sample overlay network: IP over SONET over Optical

For example, many peer-to-peer networks are overlay networks because they are organized as nodes of a virtual system of links run on top of the Internet. The Internet was initially built as an overlay on the telephone network .[8]

Overlay networks have been around since the invention of networking when computer systems were connected over telephone lines using modem, before any data network existed.

Nowadays the Internet is the basis for many overlaid networks that can be constructed to permit routing of messages to destinations specified by an IP address. For example, distributed hash tables can be used to route messages to a node having a specific logical address, whose IP address is known in advance.

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposals such as IntServ, DiffServ, and IP Multicast have not seen wide acceptance largely because they require modification of all routers in the network.[citation needed] On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination.

3.7 INTRODUCTION TO TELECOMMUNICATION CIRCUIT

A **telecommunication circuit** is any line, conductor, or other conduit by which information is transmitted. A **dedicated circuit**, **private circuit**, or **leased line** is a line that is dedicated to only one use. Originally, this was analog, and was often used by radio stations as a studio/transmitter link (STL) or remote pickup unit (RPU) for their audio, sometimes as a backup to other means. Later lines were digital, and used for private corporatedata networks.

A **telecommunication circuit** may be defined as follows:

- The complete path between two terminals over which one-way or two-way communications may be provided. See communications protocol.
- An electronic path between two or more points, capable of providing a number of channels.

- A number of conductors connected together for the purpose of carrying an electric current.
- An electronic closed-loop path among two or more points used for signaltransfer.
- A number of electrical components, such as resistors, inductances, capacitors, transistors, and power sources connected together in one or more closed loops.

4.0 CONCLUSION

In this unit you have been introduced to the fundamentalsof Networking. You have also learnt the different types of Networking and its classification. It is the basis for understanding the course.

5.0 SUMMARY

In this unit, you have learnt

Introduction to Networking which encompasses the definition, defined as a collection of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources.

6.0 TUTOR MARKED ASSIGNMENT.

a. Write short note on

- InterNetwork
- Backbone Network
- Intranet

b. State and Explain all the types of Networks based on their physical scope

7.0 FURTHER READING AND OTHER RESOURCES

- "How does the Internet Work?". http://tldp.org/HOWTO/Unix-and-Internet-Fundamentals-HOWTO/internet.html. Retrieved June 15, 2009.
- Johna Till Johnson. "Net was born of economic necessity, not fear". http://www.networkworld.com/columnists/2004/0607johnson.html. Retrieved June 15, 2009.URL is sufficient attribution
- Leonard Kleinrock (2005). *The history of the Internet*. http://www.lk.cs.ucla.edu/personal_history.html. Retrieved 2009-05-28.
- Hafner, Katie (1998). *Where Wizards Stay Up Late: The Origins Of The Internet*.

MODULE ONE

UNIT 2: DATA LINKS

Table of Contents

1.0 INTRODUCTION

In telecommunication, a **data link** is the means of connecting one location to another for the purpose of transmitting and receiving digital information. It can also refer to a set of electronics assembly, consisting of a transmitter and a receiver [two data terminal equipments (DTEs)] and the interconnecting data telecommunication circuit. These are governed by a link protocol enabling digital data to be transferred from a data source to a data sink.

2.0 OBJECTIVES

By the end this unit, you should be able to:

- Explain the term “Data Link”
- Identify the various type of Data Link
- Have good knowledge of the relevance of Data Link to Networking

3.0 MAIN CONTENT

3.1 OVERVIEW

The Data Link layer defines the rules for accessing and using the Physical layer. The Data Link Layer provides the physical transmission of the data and handles error notification, network topology and flow control. This means that the Data link layer will ensure that messages are delivered to the proper device on a LAN using hardware addresses and will translate messages from the Network layer into bits for the physical layer to transmit.

The Data layer formats the message into pieces, each called a data frame, and adds a customized header containing the hardware destination and source address.

3.2 CATEGORIES OF DATA LINKS

There are at least three categories of basic data-link configurations that can be conceived of and used:

- Simplex communications, most commonly meaning all communications in one direction only.
- Half-duplex communications, meaning communications in both directions, but not both ways simultaneously.
- Duplex communications, communications in both directions simultaneously

3.3 TYPES OF DATA LINKS

a. Industrial Ethernet

Industrial Ethernet is used to provide data link solutions for the Industrial Communications and Automation Industry. Traditional Office Grade Ethernet cannot meet the reliability demanded by Industrial Applications. A brief Loss of Service in an Office Environment may not be such a big issue, but in an industrial environment it may represent significant loss on your capital investment. Industrial Ethernet is specifically designed to operate in harsh environments such as Factory floor Automation, Process Control, HVAC, Medical, Manufacturing. Typically Industrial Automation devices include, Rugged Case, Din Rail Attachment, Wide Temperature Specification, Broad Power Source Input, these features give us a reliable Ethernet connection in demanding environments.

b. Radio Modems

Radio Modems are radio frequency transceivers for serial data communications. They connect to serial ports RS232, RS422/485 and transmit to and receive signals from other matching radio(point to point) or radios(multidrop) network. Wireless Radio Modems are designed to be transparent to the systems they operate within. All communication appears to your system as if communicating across directly connected cables, no special preparation of your data is needed. MaxStream units provides you true plug-and-communicate wireless capability operating in the internationally recognised 2.4Ghz License Free Band.

c. Ethernet to RS232 RS485 Serial Device Servers

An Ethernet to RS232 or RS485 Device Server allows you network enable virtually any serial RS232/422/485 port device. They provide the ability to remotely monitor, control or diagnose your equipment over your LAN or even WAN (Internet/Web) Link. Allowing you to maintain the existing investment you have made in Serial interface plant and machine equipment.

d. Wireless RS232 link

When creating an RS-232 wireless Link, you can replace conventional expensive RS232 serial cable runs, allowing for an easy to use, invisible connection. Handy Wave Bluetooth is the cable replacement solution for RS-232. Simply plug one unit into your RS-232 device and the other into your PC for an instant wireless link with minimal setup and also gives the added flexibility and mobility not available with traditional wired RS232 links.

e. GSM and GPRS

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves. GPRS modem is a GSM modem with additionally supports the GPRS technology for data transmission. GPRS stands for General Packet Radio Service. It is a packet-switched technology that is an extension of GSM. (GSM is a circuit-switched technology.) A key advantage of GPRS over GSM is that GPRS has a higher data transmission speed. This Technology is ideal for M2M(machine to machine communications) applications such as Meter Reading, Remote Maintenance, Traffic Control Systems, Vending Machines And Building Management Systems HVAC

f. Power Over Ethernet (PoE)

Power Over Ethernet or PoE technology describes any system to transmit electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. The standard is IEEE 802.3af which calls for 48 Volts DC over two pairs of a four-pair cable at a maximum current of 350 mA for a maximum load power of 16Watts.

g. Outdoor Ethernet Switches

Outdoor Ethernet Switches What is an Outdoor Ethernet Switch, An Outdoor Ethernet Switch, is specifically designed for the toughest industrial environments, an outdoor switch is constructed of a rugged weather tight aluminum case and the designed usually carries an IP rating which provide a waterproof, and dust-tight connection. An Outdoor Ethernet Switch can be easily adopted in almost all kinds of Industrial applications and provides the most reliable solutions for your network in outdoor environments, typical applications includes: Railway, Moving Vehicles, Factory Automation, Marine(DNV Approval).

4.0 CONCLUSION

In this unit, you have been introduced to what is referred to as Data Link. You have also learnt the different types of Data Link in use and as well as the relevance of the Data Link to Networking which is the main reason you are taking this course.

5.0 SUMMARY

What you have learned in this unit concerns

- The general knowledge about Data Link
- The types of Data Link in use

6.0 TUTOR MARKED ASSIGNMENT

- What do you understand by the term “Data Link”
- How relevant is Data Link to Networking of Computers

7.0 FURTHER READING AND OTHER RESOURCES

- McGraw Hill - All in One CompTIA A+ Certification Exam Guide - Sixth Edition 2007 (Mike Meyers)
- http://www.apan.net/meetings/busan03/cs-history.htm. Retrieved December 25, 2005.
- "APRICOT webpage". Apricot.net. 2009-05-04. http://www.apricot.net/. Retrieved 2009-05-28.
- "A brief history of the Internet in China". *China celebrates 10 years of being connected to the Internet.* http://www.pcworld.idg.com.au/index.php/id;854351844;pp;2;fp;2;fpid;1. Retrieved December 25, 2005.

MODULE ONE

UNIT 3 DEPLOYING PHYSICAL MEDIA

Table of Contents

1.0 INTRODUCTION

This unit will introduce you to Physical Media and also teach you how to deploy the physical media

2.0 OBJECTIVES

By the end of this unit, you should be able to:

- Explain the term “Physical Media”
- Identify the various type of Physical Media
- Identify which physical media is good for each of the network types

3.0 MAIN CONTENT

3.1 INTRODUCTION TO PHYSICAL MEDIA

In the OSI Reference Model, any physical means for transmitting data is referred to as the physical media. The bottom of the OSI model’s physical layer provides an interface to such media. Specifications for the physical media themselves are not part of the OSI model.

3.2 TYPES OF PHYSICAL MEDIA

a. Twistedpair - Wire twisted to avoid crosstalk interference. It may be shielded or unshielded.

- UTP-Unshielded Twisted Pair. Normally UTP contains 8 wires or 4 pair. 100 meter maximum length. 4-100 Mbps speed.
- STP-Shielded twisted pair. 100 meter maximum length. 16-155 Mbps speed. Lower electrical interference than UTP.

b. Coaxial - Two conductors separated by insulation such as TV 75 ohm cable. Maximum length of 185 to 500 meters.

Thinnet - Thinnet uses a British Naval Connector (BNC) on each end. Thinnet is part of the RG-58 family of cable*. Maximum cable length is 185 meters. Transmission speed is 10Mbps. Thinnet cable should have 50 ohms impedance and its terminator has 50 ohms impedance. A T or barrel connector will have no impedance. Maximum thinnet nodes are 30 on a segment. One end of each cable is grounded.

Thicknet - Half inch rigid cable. Maximum cable length is 500 meters. Transmission speed is 10Mbps. Expensive and is not commonly used. (RG-11 or RG-8). A vampire tap or piercing tap is used with a transceiver attached to connect computers to the cable. 100 connections may be made. The computer has an attachment unit interface (AUI) on its network card which is a 15 pin DB-15 connector. The computer is connected to the transceiver at the cable from its AUI on its network card using a drop cable. Maximum thicknet nodes are 100 on a segment. One end of each cable is grounded.

The RG value for cable types refers to its size. Coax cable types:

- RG-58 /U - 50 ohm, with a solid copper wire core for thin ethernet.
- RG-58 A/U* - 50 ohm, with a stranded wire core.
- RG-58 C/U* - Military version of RG-58 A/U.
- RG-59 - 75 ohm, for broadband transmission such as cable TV.
- RG-62 - 93 ohm, primarily used for ArcNet.
- RG-6 - Used for satellite cable (if you want to run a cable to a satellite!).
- RG-8 - 50 ohm thick ethernet.
- RG-11 - 75 ohm thick ethernet.

c. Fiber-optic - Data is transmitted using light rather than electrons. Usually there are two fibers, one for each direction. Cable length of 2 Kilometers. Speed from 100Mbps to 2Gbps. This is the most expensive and most difficult to install, but is not subject to interference. Two types of cables are:

- Single mode cables for use with lasers has greater bandwidth and costs more. Injection laser diodes (ILD) work with single mode cable.

- Multimode cables for use with Light Emitting Diode (LED) drivers. All signals appear to arrive at the same time. P intrinsic N diodes or photodiodes are used to convert light to electric signals when using multimode.

Table 3.1: Types of fiber cable

Fiber thickness (microns)	Cladding thickness (microns)	Mode
8.3	125	single
62.5	125	multi
50	125	multi
100	140	multi

3.2 Physical Media Comparisons

Table 3.2 shows the features of different types of physical media

Table 3.2: Comparing Physical Media

Media	Distance(meters)	Speed	Approx Cost/station
UTP	100	4-100Mbps	$90
STP	100	16-155Mbps	$125
Thinnet	185	10Mbps	$25
Thicknet	500	10Mbps	$50
Fiber	2000	100Mbps-2Gbps	$250 (multimode)

4.0 CONCLUSION

This unit has taken you through understanding the physical media and its various types. In this unit we also compare the media using the distance they can cover effectively, their effective speed of transferring data as our basis of comparison.

5.0 SUMMARY

In this unit you have learnt

- The explanation of the term “Physical Media”
- The various types of Physical Media

6.0 TUTOR MARKED ASSIGNMENT

- Discuss the various types of physical media as regard the distance they can cover.
- With the aid of diagram, explain the OSI model

7.0 FURTHER READINGS

- David Roessner, Barry Bozeman, Irwin Feller, Christopher Hill, Nils Newman (1997). *The Role of NSF's Support of Engineering in Enabling Technological Innovation*. http://www.sri.com/policy/csted/reports/techin/inter2.html. Retrieved 2009-05-28.
- "RFC 675 - Specification of internet transmission control program". Tools.ietf.org. http://tools.ietf.org/html/rfc675. Retrieved 2009-05-28.
- Tanenbaum, Andrew S. (1996). *Computer Networks*. Prentice Hall. ISBN 0-13-394248-1.
- Hauben, Ronda (2004). "The Internet: On its International Origins and Collaborative Vision". *Amateur Computerist* **12** (2). http://www.ais.org/~jrh/acn/ACn12-2.a03.txt. Retrieved 2009-05-29.

MODULE ONE

UNIT 4 NETWORK PROTOCOLS

Table of Content

1.0 INTRODUCTION

Having read through this unit, you will have a general understanding of what is referred to as Network Protocol and what it is all about.

2.0 OBJECTIVES

At the end of this unit, you should have learnt
Introduction to Network Protocols

- Network Protocol Overview
- Definition of Network Protocol
- Types of Network Protocols
- Comparing the Network Protocols

3.0 MAIN CONTENT

3.1 INTRODUCTION TO NETWORK PROTOCOLS

Packets can be transmitted across networks or over telephone lines. In fact, network protocols and several communications protocols use packet switching to establish a connection and route information. The format of a packet depends on the protocol that creates the packet the network computer must have a network protocol driver loaded. This program may be referred to as the transport protocol, or just as the protocol. It operates between the adapter and the initial layer of network software to package and unpackage data for the LAN.

3.2 NETWORK PROTOCOL OVERVIEW

The OSI model, and any other network communication model, provides only a conceptual framework for communication between computers, but the model itself does not provide specific methods of communication. Actual communication is defined by various communication protocols. In the context of data communication, a protocol is a formal set of rules, conventions and data structure that governs how computers and other network devices exchange information over a network. In other words, a protocol is a standard procedure and format that two data communication devices must understand, accept and use to be able to talk to each other.

In modern protocol design, protocols are "layered" according to the OSI 7 layer model or a similar layered model. Layering is a design principle which divides the protocol design into a number of smaller parts, each part accomplishing a particular sub-task and interacting with the other parts of the protocol only in a small number of well-defined ways. Layering allows the parts of a protocol to be designed and tested without a combinatorial explosion of cases, keeping each design relatively simple. Layering also permits familiar protocols to be adapted to unusual circumstances.

The header and/or trailer at each layer reflect the structure of the protocol. Detailed rules and procedures of a protocol or protocol group are often defined by a lengthy document. For example, IETF uses RFCs (Request for Comments) to define protocols and updates to the protocols.

A wide variety of communication protocols exists. These protocols were defined by many different standard organizations throughout the world and by technology vendors over years of technology evolution and development. One of the most popular protocol suites is TCP/IP, which is the heart of Internetworking communications. The IP, the Internet Protocol, is responsible for exchanging information between routers so that the routers can select the proper path for network traffic, while TCP is responsible for ensuring the data packets are transmitted across the network reliably and error free. LAN and WAN protocols are also critical protocols in network communications. The LAN protocols suite is for the physical and data link layers of communications over various LAN media such as Ethernet wires and wireless radio waves. The WAN protocol suite is for the lowest three layers and defines communication over various wide-area media, such as fiber optic and copper cables.

Network communication has slowly evolved. Today's new technologies are based on the accumulation over years of technologies, which may be either still existing or obsolete. Because of this, the protocols which define the network communication are highly inter-related. Many protocols rely on others for operation. For example, many routing protocols use other network protocols to exchange information between routers.

In addition to standards for individual protocols in transmission, there are now also interface standards for different layers to talk to the ones above or below (usually operating system specific). For example: Winsock and Berkeley sockets between layers 4 and 5; NDIS and ODI between layers 2 and 3.

The protocols for data communication cover all areas as defined in the OSI model. However, the OSI model is only loosely defined. A protocol may perform the functions of one or more of the OSI layers, which introduces complexity to understanding protocols relevant to the OSI 7 layer model. In real-world protocols, there is some argument as to where the distinctions between layers are drawn; there is no one black and white answer.

To develop a complete technology that is useful for the industry, very often a group of protocols is required in the same layer or across many different layers. Different protocols often describe different aspects of a single communication; taken together, these form a protocol suite. For example, Voice over IP (VOIP), a group of protocols developed by many vendors and standard organizations, has many protocols across the 4 top layers in the OSI model.

Protocols can be implemented either in hardware or software or a mixture of both. Typically, the lower layers are implemented in hardware, with the higher layers being implemented in software.

Protocols could be grouped into suites (or families, or stacks) by their technical functions, or origin of the protocol introduction, or both. A protocol may belong to one or multiple protocol suites, depending on how you categorize it. For example, the Gigabit Ethernet protocol IEEE 802.3z is a LAN (Local Area Network) protocol and it can also be used in MAN (Metropolitan Area Network) communications.

Most recent protocols are designed by the IETF for Internetworking communications and by the IEEE for local area networking (LAN) and metropolitan area networking (MAN). The ITU-T contributes mostly to wide area networking (WAN) and telecommunications protocols. ISO has its own suite of protocols for internetworking communications, which is mainly deployed in European countries.

3.3 DEFINITION OF NETWORK PROTOCOL

A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.

3.4 TYPES OF NETWORK PROTOCOLS

The most common network protocols are:

- Ethernet
- Local Talk
- Token Ring
- FDDI
- ATM

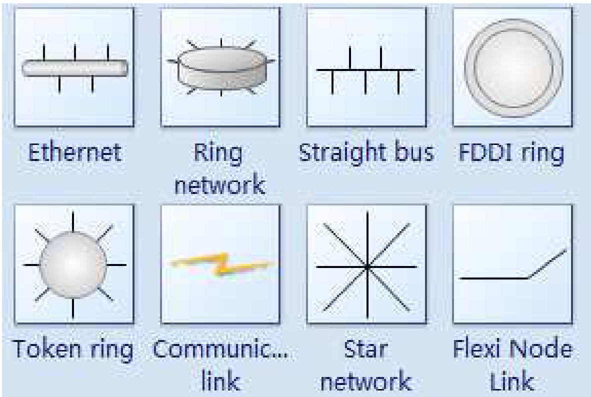


Figure 4.1: Commonly used network symbols for different kinds of network protocols

Ethernet

The Ethernet protocol is by far the most widely used. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.

The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over wireless access points, twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps up to 1000 Mbps.

Fast Ethernet

To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps. This is commonly called Fast Ethernet. Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary. Fast Ethernet is becoming common in schools that have been recently wired.

Local Talk

Local Talk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers. The method used by Local Talk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. Local Talk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software. With the addition of the server version of AppleShare software, a client/server network can be established.

The Local Talk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of Local Talk is speed. Its speed of transmission is only 230 Kbps.

Token Ring

The Token Ring protocol was developed by IBM in the mid-1980s. The access method used involves token-passing. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring in school environments has decreased.

FDDI

Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. A major advantage of FDDI is speed. It operates over fiber optic cable at 100 Mbps.

ATM

Asynchronous Transfer Mode (ATM) is a network protocol that transmits data at a speed of 155 Mbps and higher. ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets. ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable.

ATM is most often used to interconnect two or more local area networks. It is also frequently used by Internet Service Providers to utilize high-speed access to the Internet for their clients. As ATM technology becomes more cost-effective, it will provide another solution for constructing faster local area networks.

Gigabit Ethernet

The most recent development in the Ethernet standard is a protocol that has a transmission speed of 1 Gbps. Gigabit Ethernet is primarily used for backbones on a network at this time. In the future, it will probably be used for workstation and server connections also. It can be used with both fiber optic cabling and copper. The 1000BaseTX, the copper cable used for Gigabit Ethernet, is expected to become the formal standard in 1999.

Table 4.1 Comparison the Network Protocols

Protocol	**Cable**	**Speed**	**Topology**
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	.23 Mbps	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

4.0 CONCLUSION

This unit aims to teach the basic rudiments of Network Protocols, under which you were taught different types of Network Protocols which include ATM, FDDI etc.

5.0 SUMMARY

In this unit you have learnt

- What is referred to as Network protocols
- The different types of Network protocols that is in use
- You have also learnt the differences between different protocols

6.0 TUTOR MARKED ASSIGNMENT

- What do you understand by the term “Physical Media”
- State all the types of Physical Media you know
- Compare all the types of Physical Media you learnt in this lesson.

7.0 FURTHER READINGS

- *OGC-00-33R Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers*. Government Accountability Office. 7 July 2000. p. 5. http://www.gao.gov/new.items/og00033r.pdf.
- "DDN NIC". *IAB Recommended Policy on Distributing Internet Identifier Assignment*. http://www.rfc-editor.org/rfc/rfc1174.txt. Retrieved December 26, 2005.

MODULE 2 NETWORK DESIGN

UNIT 1 HARNESSING WIFI FOR USER MOBILITY

Table of Content

1.0 INTRODUCTION

This unit will give you a detailed explanation of the WiFi technology, the concept behind it and some of the features it carries.

2.0 OBJECTIVES

By the end of this unit, you must have learnt

- The concept of the Wifi technology
- The details of what brought about the Wifi technology

3.0 MAIN CONTENT

3.1 OVERVIEW OF THE WIFI TECHNOLOGY

Testing techniques developed for wired devices and networks fall short when applied to the WLAN market. The inherent instability of the unwired medium — air — in which the wireless world operates and the constant mobility of the WLAN user make the 802.11 protocol an order of magnitude more complex than equivalent wired protocols. As a result, the metrics used to benchmark wired protocols are only a starting point for the WLAN industry.

Differences between wired and wireless networks require metrics and methodology for performance benchmarking that address the intricacies of the

802.11 protocol. This unit addresses wireless-specific functions central to business-critical applications on a Wi-Fi infrastructure and includes typical results and interpretations.

3.2 INTRODUCTION TO THE WiFi TECHNOLOGY

The IEEE 802.11b standard is popularly known as “Wireless Fidelity” (or WiFi) in short. It has become widely popular for wireless LANs in office environments. Proponents of this technology consider it great competition to third generation wireless networks, which also provide high data rate mobile Internet access. WiFi can be used to provide broadband wireless Internet access .

Access Points (Aps) can be installed at various locations in the city. The Aps are also called “hotspot”. All the Aps in a city can be interconnected through an ATM-based backbone network. As the wireless device moves from one location to another, the mobile device is connected to the nearest AP.

3.3 WLAN PERFORMANCE METRICS

Wi-Fi protocols address differences between wired and wireless networks, and the implementation of the more advanced wireless protocol demands performance validation. Algorithms used in a network's clients and APs (and the capacity of these devices to process the algorithms) limit the network's performance. The objective of the validation process and test metrics is to identify critical test parameters and find the correct method of testing them.

Testing Ethernet network performance is essentially a measure of packet forwarding rate. In addition to packet forwarding measurements, WLANs must

undergo tests related to the unstable physical layer and end-user mobility, including automatic data rate adaptation, roaming, verification of security, QoS and overlapping BSSs, as well as behavioral tests that measure performance under abnormal network conditions. The primary focus of the testing effort should be parameters that eventually affect network efficiency and operation.

Data Rate Adaptation: Wired LANs support fixed data rates: 10/100/1000 Mb/s. Wireless networks support multiple data rates: 11/5.5/2/1 Mb/s for 802.11b; 54/48/36/24/18/12/9/6 Mb/s for 802.11a and 802.11g. The critical difference is that WLANs support dynamic rate adaptation and can operate at multiple data rates automatically determined by the end point (AP or client), based on the

In addition, because the 802.11 standard does not specify exact criteria for data rate adaptation, the algorithms can vary from device to device. The rate adaptation algorithm should be based on optimizing throughput; that is, when the number of errors at a specific data rate increases to the point where throughput is severely affected, the device should drop to a lower data rate to recover the best throughput at that distance from the AP.

The challenge is how to measure this repeatably, while creating a metric that can be set as the *golden standard*. To measure throughput at fixed points, many vendors often use an interference-free environment with a long, direct line-of-site area where they can simulate data rate adaptation by wheeling a client up and down on a cart. This method, however, lacks accurate rate adaptation data and is less efficient than newer devices that offer controlled RF environments and accurate signal attenuation through test setup automation. While characterizing *range vs. data* rate, the test should simultaneously characterize *range vs. throughput* and *range vs. packet* error rate.

Roaming: As a client moves out of range of one AP, it dissociates from the AP and must associate and authenticate with another. If the client predicts this roam will occur by noticing the drop in signal and searching for an alternate AP before it is actually disassociated from the first, it can optimize the roam time and network disruption caused by the roam.

The client device makes the decision to roam based on its position relative to different APs and their signal strengths. The client might periodically analyze signal strength of the APs that surround it and decide which one to associate with if it needs to roam. Load-sharing protocols used by some WLAN network vendors depart from the traditional client-based decision process, orchestrating client devices to associate with specific APs and spreading the load evenly among APs and optimizing the entire network throughput. In addition, the IEEE is advancing its work on roaming through better RF measurement (802.11k) and fast roaming processes (802.11r). As the roaming process increases in complexity, it is critical to have standard roaming metrics for testing WLAN networks and equipment.

Roaming is critical because it takes time, which can cause data loss that can ultimately disrupt a communication session. Data loss is particularly important for time-sensitive enterprise applications, such as VoWLAN, that are especially susceptible to packet delay caused by roaming. Roaming metrics include *roaming time*, *packet loss and session continuity*. Roaming time can be broken down into the following stages: scanning, associating to the new AP, authentication with the new AP and data flow. Analyzing the time of each phase of this process will help ensure the most efficient roam time.

Packet Forwarding: Forwarding rate is a function of a device: in wired networks, the Ethernet switch; in WLANs, the AP. Packet forwarding rate testing is always done at the highest signal strength and at the highest data rate because this puts the most demand on the device and measures its packet processing power in the most extreme case.

Like wired throughput tests, a wireless packet forwarding test varies the packet size to ensure the ability of the device to work with diverse traffic. But unlike wired devices, there are other factors to consider. The most critical is *security*, because wireless network devices must encrypt each packet. This additional overhead must be added to evaluate its effect on the packet forwarding rate. Another important factor is client capacity. Running the test with a large number of users stresses the AP's ability to handle a large number of users, each sending a portion of the bandwidth. This also affects how the AP functions under such conditions.

Security: security is a critical consideration for enterprise networks. Because they are susceptible to intruders, wireless networks have more stringent security requirements than their wired counterparts. Wireless security protocols (802.11i) rely heavily on authentication and encryption, which depend on the processing power of the AP and client, and cryptography accelerators for data encryption. The efficiency with which the devices handle key management and encryption will have an effect on performance measurements, such as forwarding rate and roaming.

When a client initially accesses the network or roams between APs, authentication occurs using protocols such as EAP-TLS, EAP-TTLS and LEAP. Complex key derivation algorithms can overload APs if multiple simultaneous authentication requests are made. Authentication of wireless networks is tested by measuring how efficiently and quickly an AP manages simultaneous authentication requests.

Encryption protocols used in Wi-Fi, such as WEP, TKIP and AES/CCMP, can also impact throughput performance. The security metric is performed by making a series of comparative throughput measurements using different encryption methods.

QoS: Because 802.11 is a shared media protocol without QoS, WLANs cannot prioritize real-time applications such as voice and video over data applications. QoS protocols for WLANs must account for jitter, delay and packet loss, which have required minimums for real-time applications including VoIP and multimedia streaming. Jitter, or inter-packet delay, is particularly critical in packetized voice.

3.4 TESTING METHODOLOGY FOR WIRELESS NETWORKS

Traditionally, wireless system designers have had a variety of testing options. Most are home-grown or custom-built, and include isolated screen rooms for RF control, large open spaces for testing mobility and expensive off-the-shelf meters that focus on point-to-point tests of the physical layer. Another approach is emerging for integrated chassis-based Wi-Fi testing. The older methods are costly, and in many cases do not provide the systems level configuration needed to accurately and usefully provide relevant information about the metrics discussed above.

Isolated screen rooms for controlling RF interference — WLAN system developers reduce the effects of RF interference by conducting tests in a large screen room that isolates devices under test from extraneous RF interference. It's the wireless equivalent of a "clean room." Although screen rooms can eliminate interference effects, they cannot test real-world network conditions such as mobility and roaming. Screen rooms can be expensive to erect and maintain and are not portable, which limits their use and effectiveness.

3.5 Test Setup and Sample Results

The roaming test is an example that shows the efficiency that can be achieved using a chassis-based test platform. Using two test modules — a WLA and an RFM — a phone or a PC client is connected between the two APs through two 80 dB programmable attenuators. The attenuators are programmed to force the client to roam in a controlled way from one AP to another. Data collection is performed on the source and destination channel simultaneously by the integrated dual-channel WLA module. The roaming test is fully automated and can be configured to repeat the measurements for a set period.

One attenuator is initially set to minimum and the other to maximum so that the client receives a strong signal from AP1 and associates with it while AP2 is out of the client's range. The attenuator between AP1 and the client is then gradually increased, eventually making AP1 invisible to the client while the attenuator between the client and AP2 is gradually decreased, "moving" AP2 within range and forcing a roam. The ranges and the rate of change of attenuators are configurable within the test script. At the end of the roaming test, the test script tabulates the details of each roam.

This automated roaming test implementation provides accurate time measurements and identifies specific time intervals in a way that emulates real-life roaming to the clients and access points: gradual signal strength decrease and increase. The entire test can be repeated as many times as is needed, and multiple roams can be performed in a short period without human involvement.

4.0 CONCLUSION

This unit introduces you to the Wifi technology and also teaches the advantage of the technology over the Wired technology. This unit also introduces the testing methodology for wireless networks**.**

5.0 SUMMARY

In this unit you have learnt:

- The concept of the Wifi technology

- The details of what brought about the Wifi technology

6.0 Tutor Marked Assignment

- What do you understand by the term “Wifi”
- In a tabular form, compare and contrast the Wifi and the WLAN

7.0 Further Readings

- http://www.azimuthsystems.com/
- NASA Successfully Tests First Deep Space Internet. NASA media release 08-298, November 18, 2008 Archived
- Prasad, K. V. (2009). “Principles of Digital Communication Systems and Computer Networks”, Dreamtech Press.

MODULE 2

UNIT 2 BUILDING INTERNETWORKS USING TCP/IP AND ROUTERS

Table of Content

1.0 INTRODUCTION

The language of the Internet is Transport Control Protocol/Internet Protocol (TCP/IP). No matter what type of computer platform or software is being used, the information must move across the internet in this format. This protocol calls for data to be grouped together, in bundles, called network packets.

2.0 OBJECTIVES

At the end of this unit, you must have learnt

- The fundamentals of the TCP/IP
- The relevance of TCP/IP in InterNetworks

3.0 MAIN CONTENT

3.1 TCP/IP Technology

3.1.1 TCP

TCP is a connection−oriented transport protocol that sends data as an unstructured stream of bytes. By using sequence numbers and acknowledgment messages, TCP can provide a sending node with delivery information about packets transmitted to a destination node. Where data has been lost in transit from source to destination, TCP can retransmit the data until either a timeout condition is reached or until successful delivery has been achieved. TCP can also recognize duplicate messages and will discard them appropriately. If the sending computer is transmitting too fast for the receiving computer, TCP can employ flow control mechanisms to slow data transfer. TCP can also communicates delivery information to the upper−layer protocols andapplications it supports. All these characteristics makes TCP an end−to−end reliable transport protocol. TCP is specified in RFC 793 .

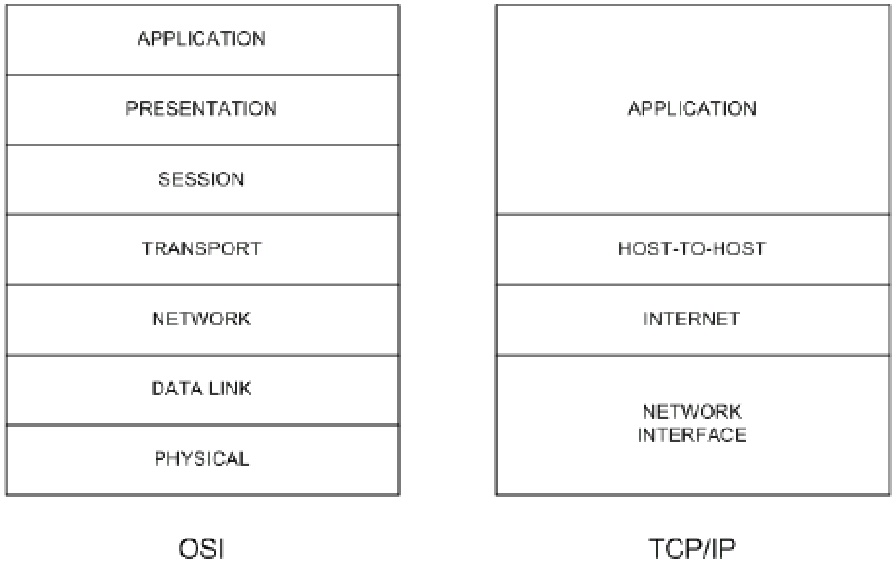


Figure 2.1: TCP/IP Protocol Suite in Relation to the OSI Reference Model

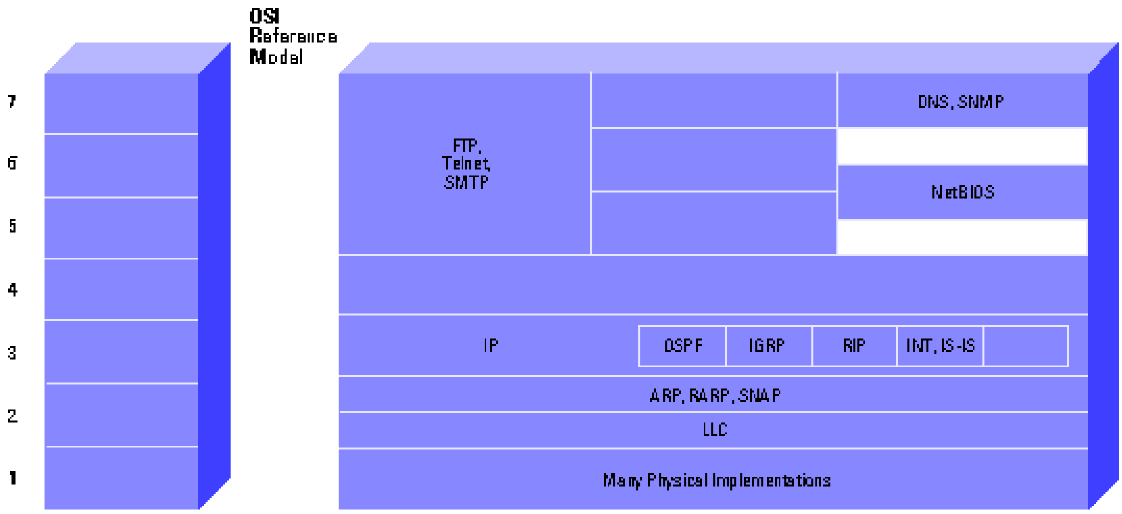


Figure2.2: Important Internet Protocols in Relation to the OSI Reference Model

3.1.2. IP

IP is the primary Layer 3 protocol in the Internet suite. In addition to internetwork routing, IP provides error reporting and fragmentation and reassembly of information units called datagrams for transmission over networks with different maximum data unit sizes. IP represents the heart of the Internet Protocol suite.

Note: The term IP in the section refers to IPv4 unless otherwise stated explicitly.

IP addresses are globally unique, 32−bit numbers assigned by the Network Information Center. Globally unique addresses permit IP networks anywhere in the world to communicate with each other.

An IP address is divided into two parts. The first part designates the network address while the second part designates the host address. The IP address space is divided into different network classes. Class A networks are intended mainly for use with a few very large networks, because they provide only 8 bits for the network address field. Class B networks allocate 16 bits, and Class C networks allocate 24 bits for the network address field. Class C networks only provide 8 bits for the host field, however, so the number of hosts per network may be a limiting factor. In all three cases, the left most bit(s) indicate the network class. IP addresses are written in dotted
decimal format; for example, 34.0.0.1. Figure 3 shows the address formats for Class A, B, and C IP networks.

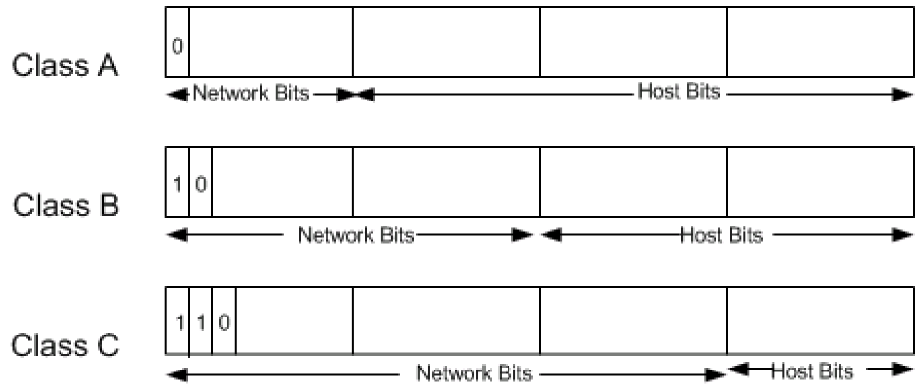


Figure2.3: Address Formats for Class A, B, and C IP Networks

IP networks also can be divided into smaller units called subnetworks or "subnets." Subnets provide extra flexibility for the network administrator. For example, assume that a network has been assigned a Class A address and all the nodes on the network use a Class A address. Further assume that the dotted decimal representation of this network's address is 34.0.0.0. (All zeros in the host field of an address specify the entire network.) The administrator can subdivide the network using subnetting. This is done by "borrowing" bits from the host portion of the address and using them as a subnet field, as depicted in Figure 2.4.

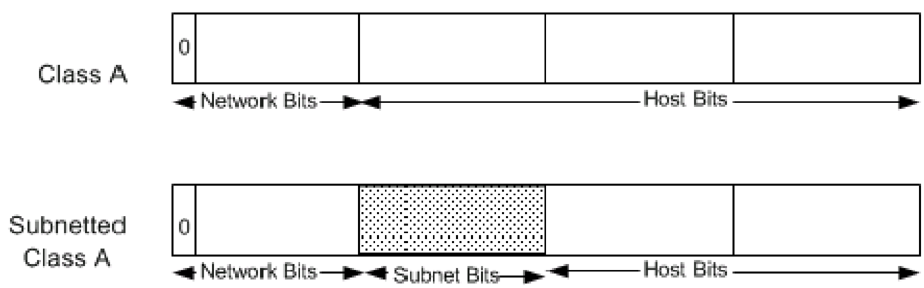


Figure 2.4: "Borrowing" Bits

If the network administrator has chosen to use 8 bits of subnetting, the second octet of a Class A IP address provides the subnet number. In our example, address 34.1.0.0 refers to network 34, subnet 1; address 34.2.0.0refers to network 34, subnet 2, and so on.

The number of bits that can be borrowed for the subnet address varies. To specify how many bits are used torepresent the network and the subnet portion of the address, IP provides subnet masks. Subnet masks use thesame format and representation technique as IP addresses. Subnet masks have ones in all bits except those thatspecify the host field. For example, the subnet mask that specifies 8 bits of subnetting for Class A address34.0.0.0 is 255.255.0.0. The subnet mask that specifies 16 bits of subnetting for Class A address 34.0.0.0 is255.255.255.0. Both of these subnet masks are pictured in Figure 2.5. Subnet masks can be passed through anetwork on demand so that new nodes can learn how many bits of subnetting are being used on their network.

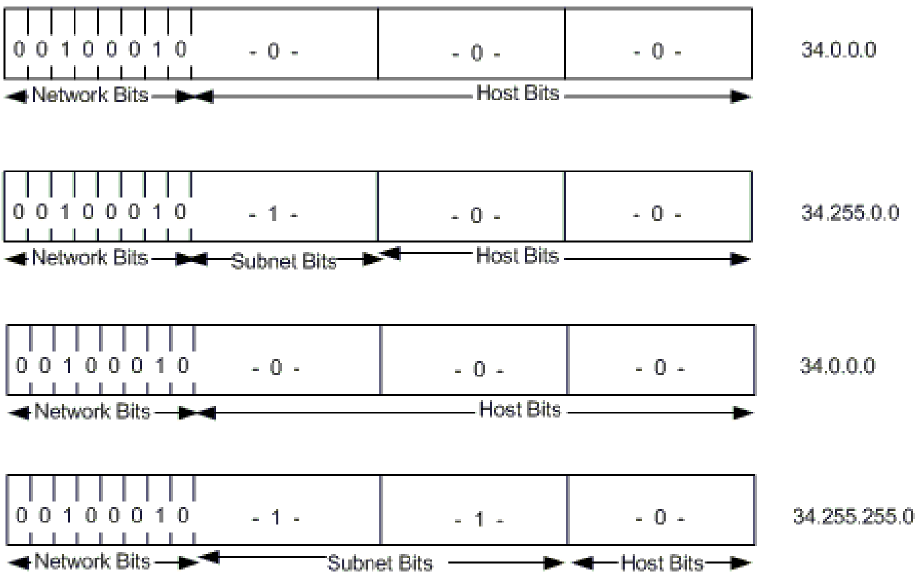


Figure 2.5: Subnet Masks

Traditionally, all subnets of the same network number used the same subnet mask. In other words, a networkmanager would choose an eight−bit mask for all subnets in the network. This strategy is easy to manage forboth network administrators and routing protocols. However, this practice wastes address space in somenetworks. Some subnets have many hosts and some have only a few, but each consumes an entire subnetnumber. Serial lines are the most extreme example, because each has only two hosts that can be connected viaa serial line subnet.
As IP subnets have grown, administrators have looked for ways to use their address space more efficiently.
One of the techniques that has resulted is called Variable Length Subnet Masks (VLSM). With VLSM, anetwork administrator can use a long mask on networks with few hosts and a short mask on subnets withmany hosts. However, this technique is more complex than making them all one size, and addresses must beassigned carefully.
Of course in order to use VLSM, a network administrator must use a routing protocol that supports it. Ciscorouters support VLSM with Open Shortest Path First (OSPF), Integrated Intermediate System to IntermediateSystem (Integrated IS−IS), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP), and static routing.

Refer to IP Addressing and Subnetting for New Users for more information about IP addressing andsubnetting.
On some media, such as IEEE 802 LANs, IP addresses are dynamically discovered through the use of twoother members of the Internet protocol suite: Address Resolution Protocol (ARP) and Reverse AddressResolution Protocol (RARP). ARP uses broadcast messages to determine the hardware (MAC layer) addresscorresponding to a particular network−layer address. ARP is sufficiently generic to allow use of IP withvirtually any type of underlying media access mechanism. RARP uses broadcast messages to determine thenetwork−layer address associated with a particular hardware address. RARP is especially important to
diskless nodes, for which network−layer addresses usually are unknown at boot time.

3.2 ROUTING IN IP ENVIRONMENTS

An "internet" is a group of interconnected networks. The Internet, on the other hand, is the collection ofnetworks that permits communication between most research institutions, universities, and many otherorganizations around the world. Routers within the Internet are organized hierarchically. Some routers areused to move information through one particular group of networks under the same administrative authorityand control. (Such an entity is called an autonomous system.) Routers used for information exchange withinautonomous systems are called interior routers, and they use a variety of interior gateway protocols (IGPs) to
accomplish this end. Routers that move information between autonomous systems are called exterior routers;they use the Exterior Gateway Protocol (EGP) or Border Gateway Protocol (BGP).

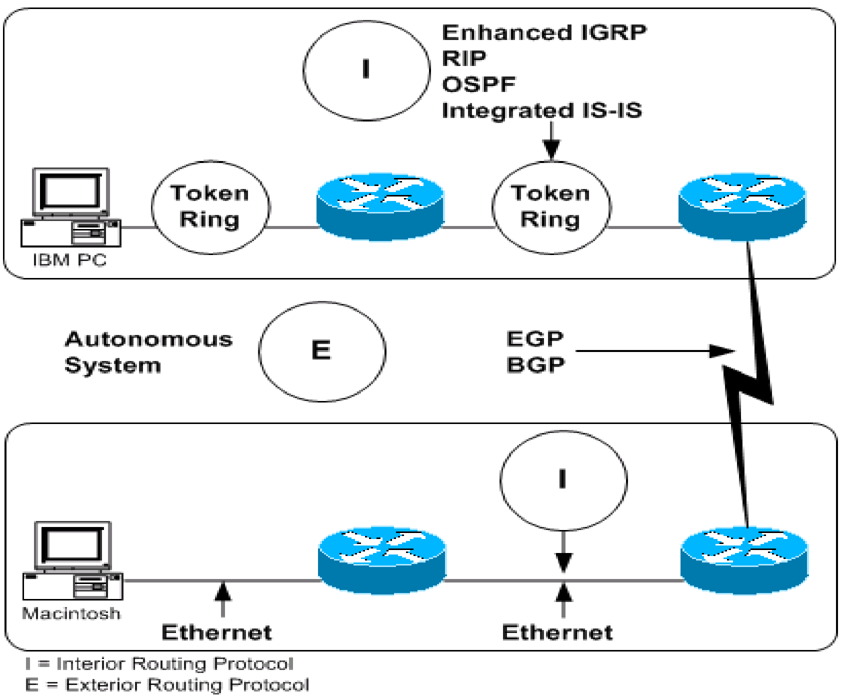


Figure 2.6: Representation of the Internet Architecture

Routing protocols used with IP are dynamic in nature. Dynamic routing requires the software in the routingdevices to calculate routes. Dynamic routing algorithms adapt to changes in the network and automaticallyselect the best routes. In contrast with dynamic routing, static routing calls for routes to be established by thenetwork administrator. Static routes do not change until the network administrator changes them.IP routing tables consist of destination address/next hop pairs.

4.0 CONCLUSION

This unit has taken you through the TCP/IP networks, the model and its implementation.

5.0 SUMMARY

In this unit you have learnt:

- The fundamentals of the TCP/IP
- The relevance of TCP/IP in InterNetworks

6.0 TUTOR MARKED ASSIGNMENT

- Explain all you can state in the TCP/IP model of Networking
- With the aid of diagram, explain the internet architecture
- What are the differences between the Class A, Class B and Class C IP Networks

7.0 FURTHER READINGS

- "Events in British Telecomms History". *Events in British TelecommsHistory*. Archived from the original on 2003-04-05.
- http://web.archive.org/web/20030405153523/http://www.sigtel.com/tel_hist_brief .html. Retrieved November 25, 2005.
- *A Brief History of Internet*. http://www.isoc.org/internet/history/brief.shtml. Retrieved 2009-05-28.
- Prasad, K. V. (2009). “Principles of Digital Communication Systems and Computer Networks”, Dreamtech Press.

MODULE 2

UNIT 3 NETWORK STANDARDS (IEEE 802 STANDARDS)

Table of Content

1.0 INTRODUCTION

IEEE 802 refers to a family of IEEE standards dealing with local area networks and metropolitan area networks.

2.0 OBJECTIVES

- Whatthe IEEE 802 standard stand for
- The layer the IEEE 802 services operates in the seven-layer OSI networking model

3.0 MAIN CONTENT

3.1 OVERVIEW OF IEEE 802

Specifically, the IEEE 802 standards are restricted to networks carrying variable-size packets. (By contrast, in cell relay networks data is transmitted in short, uniformly sized units called cells. Isochronous networks, where data is transmitted as a steady stream of octets, or groups of octets, at regular time intervals, are also out of the scope of this standard.) The number 802 was simply the next free number IEEE could assign[1], though “802” is sometimes associated with the date the first meeting was held — February 1980.

The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model. In fact, IEEE 802 splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC) , so that the layers can be listed like this:

- Data link layer
- Physical layer

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC). The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area.

Table 3.1 presents different IEEE network standards and their descriptions

Name	Description	Note
IEEE 802.1	Bridging (networking) and Network Management	
IEEE 802.2	LLC	Inactive
IEEE 802.3	Ethernet	
IEEE 802.4	Token bus	Disbanded
IEEE 802.5	Defines the MAC layer for a Token Ring	Inactive
IEEE 802.6	MANs	Disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	Disbanded
IEEE 802.8	Fiber Optic TAG	Disbanded
IEEE 802.9	Integrated Services LAN	Disbanded
IEEE 802.10	Interoperable LAN Security	Disbanded
IEEE 802.11 a/b/g/n	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	
IEEE 802.12	100BaseVG	Disbanded
IEEE 802.13	Unused	
IEEE 802.14	Cable modems	Disbanded
IEEE 802.15	Wireless PAN	
IEEE 802.15.1	Bluetooth certification	
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN	
IEEE 802.15.4	Low-Rate wireless PAN (e.g. ZigBee)	
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.17	Resilient packet ring	
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	

IEEE 802.23	Emergency Services Working Group	New(March, 2010

4.0 CONCLUSION

In this unit, you were taught that the IEEE 802 standards are restricted to networks carrying variable-size packets. You were as well taught that The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model

5.0 Summary

In this unit, you have learnt:

- Whatthe IEEE 802 standard stand for
- The layer the IEEE 802 services operates in the seven-layer OSI networking model

6.0 Tutor Marked Assignment

- State all the working group of the IEEE 802 standard and their description

7.0 Further Readings

- *The IEEE standard Sourcebook:*
- "The First Network Email". *The First Network Email*. http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html. Retrieved December 23, 2005

MODULE 2

UNIT 4 IMPLEMENTING BEST SECURITY PRACTICES

Table of Content

1.0 INTRODUCTION

Network security involves maintaining confidentiality, integrity and availability (CIA) of network. Confidentiality involves preventing unauthorized disclosure of resources or information on the network. Integrity means prevention of unauthorized modification of resources or information on the network. Integrity involves prevention of unauthorized denial of resources or information on the computer system.

2.0 OBJECTIVES

In this unit, you will learn

- What Network Securityis
- Best Security Networks
- Features of Best Security Network

3.0 MAIN CONTENT

3.1 OVERVIEW OF BEST NETWORK SECURITY

Best network security is the best solution for corporations, universities, schools, public libraries, internet cafes and other applications where administrator has to secure and maintain a lot of network pc workstations located in different places. Administrator does not need to physically visit workstations to change security settings or install patches. Best network security is intended for securing, protecting, and maintaining pc workstations within a corporate network. This network-based password-protected security software lets you completely secure pc workstations over your network as well as maintain them by uploading and installing any executable patches remotely. It supports tons of security restrictions, options and tweaks to control access to every bit of windows. You can deny access to each individual component of several control panel applets, including display, network, passwords, printers, system and internet options; disable the boot keys, context menus, DOS windows, registry editing, internet and network access; hide desktop icons, individual drives, start menu items, and taskbar; apply password protection to windows and restrict users to running specific applications only, control internet usage and much more. In total, best network security supports over 600 different security restrictions, options and tweaks that allow you to restrict access to almost every corner of windows. After you install the remote client service application on your workstations, the maintenance becomes absolutely hassle-free. You just connect your administrator's computer to the net from any place and remotely change security settings, upload and execute patches as well as schedule reboots, shutdowns, and windows explorer restarts just with a click of the mouse.

The best solution for corporations, universities, schools, public libraries, internet cafes etc. Upload and install any executable patches remotely, apply security restrictions, options and tweaks. It supports over 600 different security restrictions.

3.2 FEATURES OF BEST NETWORK SECURITY

Best network security helps implement network security. It is in a client server configuration. When both are installed the administrator can access all the clients on user machines. He can then apply access restrictions and security patches over the network without having to go to each individual machine in the organization. Scheduling reboots, shutdowns and windows explorer restarts become very simple. All it would take for the administrator are some mouse clicks. Best network security is intended for securing, protecting, and maintaining pc workstations within a corporate network and thus makes it ideal for corporations, universities, schools, public libraries, internet cafes and other applications. Typically these are situations where a lot of machines need to managed and may be located over a diverse area.

Best network security works as NT services and is able to help you apply something like 600 security restrictions. This application itself is protected by password to prevent unauthorized access. It supports tons of security restrictions, options and tweaks to control access to every bit of windows. You can remove user access to a whole lot of things such as individual component of several control panel applets, including display, network, passwords, printers, system and internet options; disable the boot keys, context menus, dos windows, registry editing, internet and network access; hide desktop icons, individual drives, start menu items, and taskbar; apply password protection to windows and restrict users to running specific applications only, internet usage for individual users also can be restricted as per company policies as well as overall safety & security.

Overall: quite a well designed package that makes security management quite easy for it administrators.

4.0 Conclusion

This unit teaches the security issues in the network, and you as well taught the best security practices in use

5.0 Summary

In this unit you have learnt:

- What a Network Security is
- Best Security Networks
- Features of Best Security Network

6.0 Tutor Marked Assignment

- Why do network need security.
- What kind of security measures are in use as of today

7.0 Further Readings

- http://www.azimuthsystems.com/
- NASA Successfully Tests First Deep Space Internet. NASA media release 08-298, November 18, 2008 Archived

MODULE 3 ENTERPRISE NETWORK

UNIT 1 CREATING ENTERPRISE NETWORK

Table of Content

1.0 INTRODUCTION

Enterprise administrator can create networks on the enterprise level. An enterprise network is represented by an FPCEnterpriseNetwork object and can include any IP addresses that are not being used to define another enterprise network.

2.0 OBJECTIVES

In this unit, you will learn

- about Enterprise Network
- What is being referred to as Predefined Enterprise Network

3.0 MAIN CONTENT

3.1 OVERVIEW OF ENTERPRISE NETWORK

Enterprise networks are used for configuring access rules in an enterprise policy that can be applied to any array in the enterprise and for configuring enterprise network rules that apply to all arrays in the enterprise. Only enterprise networks can be used to create enterprise-level rules. Enterprise networks can also be used for defining array-level access and publishing rules and for defining array-level network rules. However, you cannot use array-level networks when creating enterprise-level rules.

Any number of user-defined enterprise networks can also be included in a network defined in an array by including references to them in the EnterpriseNetworks property of the FPCNetwork object representing the array-level network. The set of IP address ranges defined by each enterprise network is then included in the array-level network, and the additional array-level configuration settings specified in the properties of the **FPCNetwork** object will apply to this set of IP address ranges. IP address ranges defined in an enterprise network that is included in an array-level network may overlap IP address ranges defined in the array-level network.

An enterprise network whose set of IP address ranges corresponds exactly to the IP addresses included in a protected array-level network, such as the Internal network, defined in one array can be used to reference that network in all the other arrays of the enterprise.

When you configure enterprise networks, you specify only the IP address ranges and do not specify any of the other properties that you would define for array-level networks. In particular, you cannot configure Network Load Balancing or Cache Array Routing Protocol (CARP) for an enterprise network.

The IP addresses that are included in an enterprise network are excluded from the default External network in each array in the enterprise even if the enterprise network is not included in any network defined in the array.

3.2 DEFINITION OF ENTERPRISE NETWORK

An enterprise private network is a network build by an enterprise to interconnect various company sites, e.g., production sites, head offices, remote offices, shops, in order to share computer resources.

3.3 PREDEFINED ENTERPRISE NETWORKS

The following predefined enterprise networks are created upon installation:

- External
- Local Host
- Quarantined VPN Clients
- VPN Clients

These predefined enterprise networks implicitly define the same IP address sets as their array-level counterparts. They can be used for defining rules in an enterprise policy and for defining enterprise network rules. When an enterprise policy is assigned to an array, each predefined enterprise network in a rule will be interpreted as the array-level network of the same name. For example, you can create an enterprise access rule that applies to requests sent to the Local Host enterprise network. When a request is handled in an array to which the enterprise policy containing this access rule is assigned, the rule will apply to the IP addresses in the Local Host network on the array member handling the request.

3.4 RESIDUAL NETWORKS

IP addresses that belong to a configurable enterprise network, but do not belong to any configurable array-level network are considered to be part of a residual network.

3.5 THREAT IN ENTERPRISE NETWORK

Today, there is an ever-growing dependency on computer networks for business transactions. With the free flow of information and the high availability of many resources, managers of enterprise networks have to understand all the possible threats to their networks. These threats take many forms, but all result in loss of privacy to some degree and possibly malicious destruction of information or resources that can lead to large monetary losses.

3.5.1 TYPES OF THREAT

Different types of threats exist, but many threats fall into three basic categories:

- Unauthorized access
- Impersonation
- Denial of service

4.0 CONCLUSION

This unit has taken you through the rudiment of enterprise network. It as well introduce you to residual networks

5.0 SUMMARY

In this unit you have learnt

- The general knowledge of enterprise network
- The definition of enterprise network
- Predefined Enterprise Network

6.0 TUTOR MARKED ASSIGNMENT

- Discuss the three types of threat to enterprise network
- What do you understand as Enterprise Network

7.0 FURTHER READINGS

- Abbate, Janet. *Inventing the Internet*. Cambridge: MIT Press, 1999.
- Bemer, Bob, "A History of Source Concepts for the Internet/Web"

MODULE 3

UNIT 2 PLANNING AND SELECTION OF ENTERPRISE NETWORK

Table of Content

1.0 INTRODUCTION

This unit discusses the overview of network and the steps involved in planning and selecting enterprise network.

2.0 OBJECTIVES

In this unit you will learn:

- The planning phases of an enterprise networks
- The Design phases in enterprise networks

3.0 MAIN CONTENT

3.1 Overview

The network planning and design methodology describes a process with 9 specific steps and a sequence for those activities. It is an engineering life cycle that supports technical initiatives such as Windows migration, IP telephony and wireless design to name a few examples. The methodology begins with examining company business requirements. It is absolutely essential that you understand the company business model, business drivers and how they are growing from a business perspective. That will build the foundation for a design proposal that serves the business, technical and operational requirements of the company.

3.2 STEPS TO EFFECTIVE NETWORK PLANNING AND DESIGN

STEP 1: Business Requirements

Any design project starts with an understanding of what the company does and what they need to accomplish from a business perspective. This begins with an understanding of their business model, which really describes how their company works from an operational and business perspective to generate revenues and reduce costs. Many vendors today have conducted their own return on investment (ROI) studies for new implementations such as Unified Communications and Telephony. It is an effective sales tool that illustrates the cost benefits compared with investment over a specified period of time.

This is a list of some typical business drivers:

- Reduce Operating Costs
- Generate Revenue
- Client Satisfaction
- Employee Productivity

This is a list of some typical project business requirements:

- Budget Constraints
- Office Consolidations
- Company Mergers and Acquisitions
- Business Partner Connectivity
- Telecommuter Remote Access
- Implement New Offices and Employees
- New Data Center Applications
- Reduce Network Outage Costs
- Cost Effective Network Management
- Vendor Contracts

STEP 2: Design Requirements

Now that you understand the basic business requirements of the company, you can determine the standard and specific design requirements. The design requirements process is focused on defining requirements from a technical perspective. Those requirements along with the business requirements will build the framework that is used to define infrastructure, security and management. Design requirements are defined as standard and miscellaneous. The standard design requirements are generic and represent those considered with many design projects. Miscellaneous requirements are those that aren't defined with any of the standard requirements.

Standard Design Requirements

- Performance
- Availability
- Scalability
- Standards Compatibility
- Rapid Deployment

STEP 3: Network Assessment

A network assessment is conducted after we have finished the business and design requirements of the company. A network assessment provides a quick snapshot of the current network with an examination of the infrastructure, performance, availability, management and security. That information is utilized for making effective strategy recommendations and design proposals to the client concerning specific information systems modifications. The network assessment model has 3 sequential activities, which are assessment, analysis and recommendations. The current network is examined using five primary surveys: infrastructure, performance, availability, management and security. When the surveys are completed, the information collected is then reviewed for trends, problems and issues that are negatively affecting the network.

STEP 4: Infrastructure Selection

After doing an network assessment we are ready to start selecting specific infrastructure components for the network design. This phase starts building the infrastructure with a specific sequence that promotes effective equipment selection and design. It is important that you consider business requirements, design requirements and the network assessment when building your infrastructure.

The following numbered list describes the specific infrastructure components and their particular sequence.

1. Enterprise WAN Topology
2. Campus Topology
3. Traffic Model
4. Equipment Selection
5. Circuits
6. Routing Protocol Design
7. Addressing
8. Naming Conventions
9. IOS Services
10. Domain Name Services
11. DHCP Services

STEP 5: Security Strategy

We must now define a security strategy for securing the infrastructure. The need for enterprise network security shouldn't be ignored with the proliferation of the Internet. Companies are continuing to leverage the public infrastructure for connecting national and international offices, business partners and new company acquisitions. The security requirements and network assessment recommendations should drive the selection of security equipment, protocols and processes. It identifies what assets must be protected, what users are allowed access and how those assets will be secured.

STEP 6: Network Management Strategy

This section will define a network management strategy for managing all equipment defined from infrastructure and security. It is necessary to define how the equipment is going to be monitored and determine if the current management strategy is adequate or if new applications, equipment, protocols and processes must be identified. Management components are then integrated with infrastructure and security to finish building the proposed design. These primary elements comprise any well-defined management strategy and should be considered when developing your strategy.

•Management Groups

• SNMP Applications

• Monitored Devices and Events

STEP 7: Proof of Concept

All infrastructure, security and management components must now be tested with a proof of concept plan. It is important to test the current design, configuration and IOS versions in a non-production environment or on the production network with limited disruption. Implementation of newer network modules at a router, for instance, could require that you change the current IOS version that is implemented. Making those changes could affect WAN or campus modules already installed at production routers. That is the real value of doing a proof of concept and certifying that the new equipment and IOS versions integrate with each device as well as the network. The following list describes the advantages of doing a proof of concept with your network design. The proof of concept test results should be examined and used to modify current infrastructure, security and management specifications before generating a design proposal. The proof of concept model suggested here involves prototype design, equipment provisioning, defining tests, building equipment scripts and examining test results.

1. Prototype Design

2. Provision Equipment

3. Define Tests

4. Build Equipment Scripts

5. Review Test Results

STEP 8: Design Proposal/Review

With the proof of concept finished, you are now ready to build a design proposal for the design review meeting. Your intended audience could be the Director, CIO, CTO, Senior Network Engineer, Consultant or anyone that is approving a budget for the project. It is important to present your ideas with clarity and professionalism. If a presentation is required, power point slides work well and could be used to support concepts from the design proposal document. The focus is on what comprises a standard design proposal and the sequence for presenting that information.

The working design proposal is presented to the client after addressing any concerns from proof of concept assurance testing. The design review is an opportunity for you to present your design proposal to the client and discuss any issues. It is an opportunity for the client to identify concerns they have and for the design engineer to clarify issues. The focus is to agree on any modifications, if required, and make changes to the infrastructure, security and management before implementation starts. Business and design requirements can change from when the project started which sometimes will necessitate changes to infrastructure, security and management specifications. Any changes should then go through proof of concept testing again before final changes to the design proposal.

STEP 9: Implementation

The final step will have us defining an implementation process for the specified design. This describes a suggested implementation methodology of the proposed design, which should have minimal disruption to the production network. As well it should be efficient and as cost effective as possible. As with previous methodologies there is a sequence that should be utilized as well.

Once the implementation is finished, there is monitoring of the network for any problems. Design and configuration modifications are then made to address any problems or concerns.

4.0 Conclusion

This unit has taught you the necessary steps to consider in implementing an enterprise network

5.0 Summary

In this unit you have learnt:

- The planning phases of an enterprise networks
- The Design phases in enterprise networks

6.0 Tutor Marked Assignment

- State and Explain the phases involved in creating an enterprise network

7.0 Further Readings

- Krol, Ed. *Whole Internet User's Guide and Catalog.*O'Reilly & Associates, 1992.
- *Scientific American Special Issue on Communications, Computers, and Networks*, September, 1991.
- http://www.amazon.com
- http://www.eBookmall.com

- Prasad, K. V. (2009). “Principles of Digital Communication Systems and Computer Networks”, Dreamtech Press.

MODULE 3

UNIT 3 ADVANCED WAN AND LAN CLASSES

Table of Content

1.0 INTRODUCTION

Computers networked together in a self-contained group form a Local Area Network, or LAN. A LAN typically is contained within a single building or a group of neighbouring buildings. Two computers linked together at home are the simplest form of a LAN. Several hundred computers cabled together across several buildings at school form a more complex LAN. LANs are usually connected with coaxial or CAT5 cable.

On the other hand, A WAN is geographically large. It is often formed by the joining together of LANs in distant places. A national banking organization, for example, may use a WAN to connect all of its branches across the country. The difference between LANs and WANs is getting blurry as fibre optic cables have allowed LAN technologies to connect devices many kilometers apart. WANs are usually connected using the Internet, ISDN landlines or satellite.

2.0 OBJECTIVES

In this unit you will learn

- The background of LAN and WAN
- The differences between LAN and WAN
- The relationship between LAN and WAN

3.0 MAIN CONTENT

3.1 LAN VS WAN

A local area network (LAN) exists in a house or a university campus, while a wide area network (WAN) exists over many office buildings separated by a vast distance. The office buildings in a WANmay be in different countries or even continents. For example, the headquarters building may be in the USA, the regional office building may be in the UK, and the branch office building may be in India. The workers in the three buildings can use WAN to collaborate with each other. The internet can also be considered as a WAN. Let's take a look at the LAN vs. WAN comparison check.

3.2 DIFFERENCES BETWEEN LAN AND WAN

One of the difference between LAN and WAN, is the speed of the network. The maximum speed of a LAN can be 1000 megabits per second, while the speed of a WANcan go up to 150 megabits per second. This means the speed of a WAN, is one-tenth of the speed of a LAN. A WANis usually slower because it has lower bandwidth.

Computers in a LAN can share a printer, if they are all in the same LAN. On the other hand, a WAN cannot share a printer, so a computer in one country cannot use a printer in another country. A LAN does not need a dedicated computer to direct traffic to and from the internet, unlike a WAN that needs a special-purpose computer, whose only purpose is to send and receive data from the internet.

Another LAN vs. WAN comparison is the cost of the network. A WAN is more expensive than a LAN. It is easier to expand a LAN than a WAN. The equipment needed for a LAN is a network interface card (NIC), a switch and a hub. On the other hand, the equipment needed to connect a WAN to the internet is a modem and a router. The modem may be a cable modem or a DSL modem that is connected to a wall jack, while the router should be configured so that it can handle the packets traveling between the WAN and the internet.

In LAN vs. WAN, there is a difference in the networking standard used. A LAN uses the ethernet standard, while a WAN uses the t1 standard. Before ethernet, the protocols used for LAN were attached resource computer network (ArcNet) and token ring. The protocols used for WAN are frame relay and asynchronous transfer mode (ATM). Another protocol for WAN is packet over SONET/SDH (POS), where SONET stands for synchronous optical networking and SDH stands for synchronous digital hierarchy. The first WAN protocol was x.25, while an advanced WAN protocol is multiprotocol label switching (mpls). The hardware in a LAN is connected with 10base-t cable connectors, while a WAN is connected via leased lines or satellites.

Here is an explanation of LANs and WANs. A LAN is easy to set up, as you need to slip the NIC into the PCI slot (for desktop computers) or PCMCIA slot (for laptop computers). You also need to install the driver for the NIC. The NIC can be connected to the network using the RJ45 port.

On the other hand, a WAN is very difficult to set up. There is often an appliance to optimize the WAN. There is also a device to cache WAN data, so workers in the branch office can quickly access documents. The router also has quality of service (QoS) built in, so that it gives priority to certain kinds of traffic.

There are various topologies available in LAN and WAN networking. The most common topologies in LAN and WAN networks are ring and star. The ring topology is a network in which every node (every computer) is connected to exactly two other nodes. The star topology is a network in which all the nodes (called leaf nodes or peripheral nodes) are connected to a central node.

4.0 CONCLUSION

This unit has taken you through the understanding of the LAN and WAN classes. It also examined the relationship between LAN and WAN and also the differences between the two types of network.

5.0 SUMMARY

In this unit you have learnt that

- A local area network (LAN) exists in a house or a university campus, while a wide area network (WAN) exists over many office buildings separated by a vast distance.
- One of the difference between LAN and WAN, is the speed of the network.
- In LAN vs. WAN, there is a difference in the networking standard used.

6.0 TUTOR MARKED ASSIGNMENT

- Discuss the differences between the LAN and the WAN classes.
- Discuss other types of Networks apart from the LAN and the WAN

7.0 FURTHER READINGS

- "http://en.wikipedia.org/wiki/History_of_the_Internet

MODULE FOUR COMMUNICATION TECHNOLOGY

UNIT 1 MODEM AND MODULATION CONCEPTS

1.0 Introduction

A **modem** (**mo**dulator-**dem**odulator) is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used over any means of transmitting analog signals, from driven diodes to radio.The most familiar example is a voice band modem that turns the digital data of a personal computer into modulated electrical signals in the voice frequency range of a telephone channel. These signals can be transmitted over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Modulation is the process of facilitating the transfer of information over a medium. Sound transmission in air has limited range for the amount of power your lungs can generate. To extend the range your voice can reach, we need to transmit it through a medium other than air, such as a phone line or radio. The process of converting information (voice in this case) so that it can be
successfully sent through a medium (wire or radio waves) is called modulation.

2.0 OBJECTIVES

By the end of this unit, you should be able to:

- Define a modem
- Explain modulation
- State the types of modulation
- State the list of common digital modulation techniques

3.0 Main content

3.1 History

News wire services in 1920s used multiplex equipment that met the definition, but the modem function was incidental to the multiplexing function, so they are not commonly included in the history of modems.

Modems grew out of the need to connect teletype machines over ordinary phone lines instead of more expensive leased lines which had previously been used for current loop-based teleprinters and automated telegraphs. George Stibitz connected a New Hampshire teletype to a computer in New York City by a subscriber telephone line in 1940.

In 1943, IBM adapted this technology to their unit record equipment and were able to transmit punched cards at 25 bits/second.[citation needed] Mass-produced modems in the United States began as part of the SAGE air-defense system in 1958, connecting terminals at various airbases, radar sites, and command-and-control centers to the SAGE director centers scattered around the U.S. and Canada. SAGE modems were described by AT&T's Bell Labs as conforming to their newly published Bell 101 dataset standard. While they ran on dedicated telephone lines, the devices at each end were no different from commercial acoustically coupled Bell 101, 110 baud modems.

In the summer of 1960, the name Data-Phone was introduced to replace the earlier term digital subset. The 202 Data-Phone was a half-duplex asynchronous service that was marketed extensively in late 1960. In 1962, the 201A and 201B Data-Phones were introduced. They were synchronous modems using two-bit-per-baud phase-shift keying (PSK). The 201A operated half-duplex at 2,000 bit/s over normal phone lines, while the 201B provided full duplex 2,400 bit/s service on four-wire leased lines, the send and receive channels running on their own set of two wires each.

The famous Bell 103A dataset standard was also introduced by Bell Labs in 1962. It provided full-duplex service at 300 baud over normal phone lines. Frequency-shift keying was used with the call originator transmitting at 1,070 or 1,270 Hz and the answering modem transmitting at 2,025 or 2,225 Hz. The readily available 103A2 gave an important boost to the use of remote low-speed terminals such as the KSR33, the ASR33, and the IBM 2741. AT&T reduced modem costs by introducing the originate-only 113D and the answer-only 113B/C modems.

3.2 Significance of Digital of Modulation

The aim of **digital modulation** is to transfer a digital bit stream over an analog bandpasschannel, for example over the public switched telephone network (where a bandpass filter limits the frequency range to between 300 and 3400 Hz), or over a limited radio frequency band.

The aim of **analog modulation** is to transfer an analogbaseband (or lowpass) signal, for example an audio signal or TV signal, over an analog bandpasschannel, for example a limited radio frequency band or a cable TV network channel.

Analog and digital modulation facilitate frequency division multiplexing (FDM), where several low pass information signals are transferred simultaneously over the same shared physical medium, using separate passband channels.

The aim of **digital baseband modulation** methods, also known as line coding, is to transfer a digital bit stream over a baseband channel, typically a non-filtered copper wire such as a serial bus or a wired local area network.

The aim of **pulse modulation** methods is to transfer a narrowband analog signal, for example a phone call over a wideband baseband channel or, in some of the schemes, as a bit stream over another digital transmission system.

In music synthesizers, modulation may be used to synthesise waveforms with a desired overtone spectrum. In this case the carrier frequency is typically in the same order or much lower than the modulating waveform. See for example frequency modulation synthesis or ring modulation.

3.3 Analog modulation methods

In analog modulation, the modulation is applied continuously in response to the analog information signal.

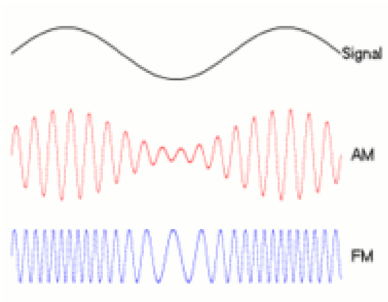


Figure 2.1: Representing the Analog Modulation Signal

A low-frequency message signal (top) may be carried by an AM or FM radio wave.

Common analog modulation techniques are:

- Amplitude modulation (AM) (here the amplitude of the carrier signal is varied in accordance to the instantaneous amplitude of the modulating signal)
    - Double-sideband modulation (DSB)
        - Double-sideband modulation with carrier (DSB-WC) (used on the AM radio broadcasting band)
        - Double-sideband suppressed-carrier transmission (DSB-SC)
        - Double-sideband reduced carrier transmission (DSB-RC)
    - Single-sideband modulation (SSB, or SSB-AM),
        - SSB with carrier (SSB-WC)
        - SSB suppressed carrier modulation (SSB-SC)
    - Vestigial sideband modulation (VSB, or VSB-AM)
    - Quadrature amplitude modulation (QAM)

- Angle modulation
    - Frequency modulation (FM) (here the frequency of the carrier signal is varied in accordance to the instantaneous amplitude of the modulating signal)
    - Phase modulation (PM) (here the phase shift of the carrier signal is varied in accordance to the instantaneous amplitude of the modulating signal)

The accompanying figure shows the results of (amplitude-)modulating a signal onto a carrier (both of which are sine waves). At any point along the y-axis, the amplitude of the modulated signal is equal to the sum of the carrier signal

3.4 Digital modulation methods

In digital modulation, an analog carrier signal is modulated by a digital bit stream. Digital modulation methods can be considered as digital-to-analog conversion, and the corresponding demodulation or detection as analog-to-digital conversion. The changes in the carrier signal are chosen from a finite number of M alternative symbols (the modulation alphabet).

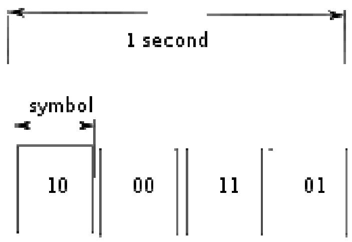


Figure 2.2: Schematic of 4 baud (8 bps) data link.

A simple example: A telephone line is designed for transferring audible sounds, for example tones, and not digital bits (zeros and ones). Computers may however communicate over a telephone line by means of modems, which are representing the digital bits by tones, called symbols. If there are four alternative symbols (corresponding to a musical instrument that can generate four different tones, one at a time), the first symbol may represent the bit sequence 00, the second 01, the third 10 and the fourth 11. If the modem plays a melody consisting of 1000 tones per second, the symbol rate is 1000 symbols/second, or baud. Since each tone (i.e., symbol) represents a message consisting of two digital bits in this example, the bit rate is twice the symbol rate, i.e. 2000 bits per second. This is similar to the technique used by dialup modems as opposed to DSL modems.

3.5 Digital modulation techniques

These are;

- Amplitude-Shift Keying (ASK)
- Frequency-Shift Keying (FSK)
- Phase-Shift Keying (PSK)

3.5.1 Amplitude-Shift Keying (ASK)

In ASK, the amplitude of the carrier is changed in response to information and all else is kept fixed. Bit 1 is transmitted by a carrier of one particular amplitude. To transmit 0, we change the amplitude keeping the frequency constant. On-Off Keying (OOK) is a special form of ASK.

3.5.2 Frequency-Shift Keying (FSK)

In FSK, we change the frequency in response to information, one particular frequency for a 1 and another frequency for a 0 as shown below for the same bit sequence. In the example below, frequency f1 for bit 1 is higher than f2 used for the 0 bit.

$$FSK(t) = \begin{cases} \sin(2\pi f_1 t) & for\ bit\ 1 \\ \sin(2\pi f_2 t) & for\ bit\ 0 \end{cases}$$

3.5.3 Phase-Shift Keying (PSK)

In PSK, we change the phase of the sinusoidal carrier to indicate information. Phase in this context is the starting angle at which the sinusoid starts. To transmit 0, we shift the phase of the sinusoid by 180. Phase shift represents the change in the state of the information in this case.

$$PSK(t) = \begin{cases} \sin(2\pi f t) & for\ bit\ 1 \\ \sin(2\pi f t + \pi) & for\ bit\ 0 \end{cases}$$

3.6 Fundamental digital modulation methods

The most fundamental digital modulation techniques are based on keying:

- In the case of PSK (phase-shift keying), a finite number of phases are used.
- In the case of FSK (frequency-shift keying), a finite number of frequencies are used.
- In the case of ASK (amplitude-shift keying), a finite number of amplitudes are used.
- In the case of QAM (quadrature amplitude modulation), a finite number of at least two phases, and at least two amplitudes are used.

In QAM, an inphase signal (the I signal, for example a cosine waveform) and a quadrature phase signal (the Q signal, for example a sine wave) are amplitude modulated with a finite number of amplitudes, and summed. It can be seen as a two-channel system, each channel using ASK. The resulting signal is equivalent to a combination of PSK and ASK.

In all of the above methods, each of these phases, frequencies or amplitudes are assigned a unique pattern of binarybits. Usually, each phase, frequency or amplitude encodes an equal number of bits. This number of bits comprises the symbol that is represented by the particular phase, frequency or amplitude.

If the alphabet consists of $M = 2^N$ alternative symbols, each symbol represents a message consisting of N bits. If the symbol rate (also known as the baud rate) is f_S symbols/second (or baud), the data rate is Nf_S bit/second.

For example, with an alphabet consisting of 16 alternative symbols, each symbol represents 4 bits. Thus, the data rate is four times the baud rate.

In the case of PSK, ASK or QAM, where the carrier frequency of the modulated signal is constant, the modulation alphabet is often conveniently represented on a constellation diagram, showing the amplitude of the I signal at the x-axis, and the amplitude of the Q signal at the y-axis, for each symbol.

3.7 Modulator and detector principles of operation

PSK and ASK, and sometimes also FSK, are often generated and detected using the principle of QAM. The I and Q signals can be combined into a complex-valued signal I+jQ (where j is the imaginary unit). The resulting so called equivalent lowpass signal or equivalent baseband signal is a complex-valued representation of the real-valued modulated physical signal (the so called passband signal or RF signal).

These are the general steps used by the modulator to transmit data:

1. Group the incoming data bits into codewords, one for each symbol that will be transmitted.
2. Map the codewords to attributes, for example amplitudes of the I and Q signals (the equivalent low pass signal), or frequency or phase values.
3. Adapt pulse shaping or some other filtering to limit the bandwidth and form the spectrum of the equivalent low pass signal, typically using digital signal processing.
4. Perform digital-to-analog conversion (DAC) of the I and Q signals (since today all of the above is normally achieved using digital signal processing, DSP).
5. Generate a high-frequency sine wave carrier waveform, and perhaps also a cosine quadrature component. Carry out the modulation, for example by multiplying the sine and cosine wave form with the I and Q signals, resulting in that the equivalent low pass signal is frequency shifted into a modulated passband signal or RF signal. Sometimes this is achieved using DSP technology, for example direct digital synthesis using a waveform table, instead of analog signal processing. In that case the above DAC step should be done after this step.
6. Amplification and analog bandpass filtering to avoid harmonic distortion and periodic spectrum

At the receiver side, the demodulator typically performs:

1. Bandpass filtering.
2. Automatic gain control, AGC (to compensate for attenuation, for example fading).
3. Frequency shifting of the RF signal to the equivalent baseband I and Q signals, or to an intermediate frequency (IF) signal, by multiplying the RF signal with a local oscillator sinewave and cosine wave frequency (see the superheterodyne receiver principle).
4. Sampling and analog-to-digital conversion (ADC) (Sometimes before or instead of the above point, for example by means of undersampling).
5. Equalization filtering, for example a matched filter, compensation for multipath propagation, time spreading, phase distortion and frequency selective fading, to avoid intersymbol interference and symbol distortion.
6. Detection of the amplitudes of the I and Q signals, or the frequency or phase of the IF signal.
7. Quantization of the amplitudes, frequencies or phases to the nearest allowed symbol values.
8. Mapping of the quantized amplitudes, frequencies or phases to codewords (bit groups).
9. Parallel-to-serial conversion of the codewords into a bit stream.
10. Pass the resultant bit stream on for further processing such as removal of any error-correcting codes.

As is common to all digital communication systems, the design of both the modulator and demodulator must be done simultaneously. Digital modulation schemes are possible because the transmitter-receiver pair have prior knowledge of how data is encoded and represented in the communications system. In all digital communication systems, both the modulator at the transmitter and the demodulator at the receiver are structured so that they perform inverse operations.

Non-coherent modulation methods do not require a receiver reference clock signal that is phase synchronized with the sender carrier wave. In this case, modulation symbols (rather than bits, characters, or data packets) are asynchronously transferred. The opposite is coherent modulation.

3.8 List of common digital modulation techniques

The most common digital modulation techniques are:

- Phase-shift keying (PSK):
    - Binary PSK (BPSK), using M=2 symbols
    - Quadrature PSK (QPSK), using M=4 symbols
    - 8PSK, using M=8 symbols

- 16PSK, using M=16 symbols
    - Differential PSK (DPSK)
    - Differential QPSK (DQPSK)
    - Offset QPSK (OQPSK)
    - π/4–QPSK
- Frequency-shift keying (FSK):
    - Audio frequency-shift keying (AFSK)
    - Multi-frequency shift keying (M-ary FSK or MFSK)
    - Dual-tone multi-frequency (DTMF)
    - Continuous-phase frequency-shift keying (CPFSK)
- Amplitude-shift keying (ASK)
- On-off keying (OOK), the most common ASK form
    - M-aryvestigial sideband modulation, for example 8VSB
- Quadrature amplitude modulation (QAM) - a combination of PSK and ASK:
    - Polar modulation like QAM a combination of PSK and ASK.[citation needed]
- Continuous phase modulation (CPM) methods:
    - Minimum-shift keying (MSK)
    - Gaussian minimum-shift keying (GMSK)
- Orthogonal frequency-division multiplexing (OFDM) modulation:
    - discrete multitone (DMT) - including adaptive modulation and bit-loading.
- Wavelet modulation
- Trellis coded modulation (TCM), also known as trellis modulation
- Spread-spectrum techniques:
    - Direct-sequence spread spectrum (DSSS)
    - Chirp spread spectrum (CSS) according to IEEE 802.15.4a CSS uses pseudo-stochastic coding
    - Frequency-hopping spread spectrum (FHSS) applies a special scheme for channel release

4.0 Conclusion

In this unit you have been introduced to the fundamental concepts of modem and modulation. You also learnt the types of modulation. You were also introduced to Various methods of modulation.

5.0 Summary

In this unit, you have learnt

- The definition of a modem
- The explanation of modulation
- The types of modulation
- The list of common digital modulation techniques

6.0 Tutor Marked Assignment

- How does the Modem perform its function
- Explain what you understand by the term “modulation”
- State and Explain the different types of Modulation

7.0 References

- J.R.Barry, E.A.Lee, D.G.Messerschmidt, Digital Communication, Kluwer Academic Publishers, 2004.

MODULE FOUR

UNIT2 MULTIPLEXERS

1.0 INTRODUCTION

In electronics, a **multiplexer** or **mux** is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A multiplexer of 2^n inputs has n select lines, which are used to select which input line to send to the output.An electronic multiplexer makes it possible for several signals to share one device or resource, for example one A/D converter or one communication line, instead of having one device per input signal.On the other end, a demultiplexer (or **demux**) is a device taking a single input signal and selecting one of many data-output-lines, which is connected to the single input. A multiplexer is often used with a complementary demultiplexer on the receiving end.An electronic multiplexer can be considered as a multiple-input, single-output switch, and a demultiplexer as a single-input, multiple-output switch. The schematic symbol for a multiplexer is an isosceles trapezoid with the longer parallel side containing the input pins and the short parallel side containing the output pin. The schematic on the right shows a 2-to-1 multiplexer on the left and an equivalent switch on the right. The *sel* wire connects the desired input to the output.

2.0 OBJECTIVES

By the end of this unit, you should be able to:

- Explain the meaning of a multiplexer
- Describe the types of multiplexers
- State the areas of applications of multiplexers
- Describe how the TCP/IP protocol suite maps to the Department of Defense Advanced Research Projects Agency (DARPA) and Open System Interconnection (OSI) models.

3.0 Main Content

3.1 Types of Multiplexing

Multiplexing technologies may be divided into several types, all of which have significant variations:[1]space-division multiplexing (SDM), frequency-division multiplexing (FDM), time-division multiplexing (TDM), and code division multiplexing (CDM). Variable bit rate digital bit streams may be transferred efficiently over a fixed bandwidth channel by means of statistical multiplexing, for example packet mode communication. Packet mode communication is an asynchronous mode time-domain multiplexing which resembles time-division multiplexing.

Digital bit streams can be transferred over an analog channel by means of code-division multiplexing (CDM) techniques such as frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS).

In wireless communications, multiplexing can also be accomplished through alternating polarization (horizontal/vertical or clockwise/counterclockwise) on each adjacent channel and satellite, or through phased multi-antenna array combined with a Multiple-input multiple-output communications (MIMO) scheme.

3.1.1 Space-division multiplexing

In wired communication, space-division multiplexing simply implies different point-to-point wires for different channels. Examples include an analogue stereo audio cable, with one pair of wires for the left channel and another for the right channel, and a multipairtelephone cable. Another example is a switched star network such as the analog telephone access network (although inside the telephone exchange or between the exchanges, other multiplexing techniques are typically employed) or a switched Ethernet network. A third example is a mesh network. Wired space-division multiplexing is typically not considered as multiplexing.

In wireless communication, space-division multiplexing is achieved by multiple antenna elements forming a phased array antenna. Examples are multiple-input and multiple-output (MIMO), single-input and multiple-output (SIMO) and multiple-input and single-output (MISO) multiplexing. For example, a IEEE 802.11n wireless router with *N* antennas makes it possible to communicate with *N* multiplexed channels, each with a peak bit rate of 54 Mbit/s, thus increasing the total peak bit rate with a factor *N*. Different antennas would give different multi-path propagation (echo) signatures, making it possible for digital signal processing techniques to separate different signals from each other. These techniques may also be utilized for space diversity (improved robustness to fading) or beam-forming (improved selectivity) rather than multiplexing.

3.1.2 Frequency-division multiplexing

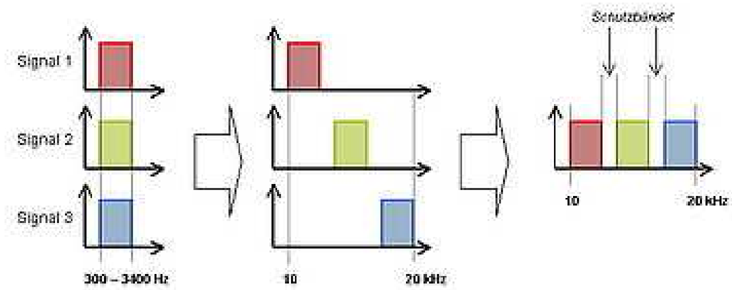


Fig 3.1: Frequency-division multiplexing

Frequency-division multiplexing (FDM): The spectrums of each input signal are swifted in several distinct frequency ranges.

Frequency-division multiplexing (FDM) is inherently an analog technology. FDM achieves the combining of several digital signals into one medium by sending signals in several distinct frequency ranges over that medium.

One of FDM's most common applications is cable television. Only one cable reaches a customer's home but the service provider can send multiple television channels or signals simultaneously over that cable to all subscribers. Receivers must tune to the appropriate frequency (channel) to access the desired signal.[1]

A variant technology, called wavelength-division multiplexing (WDM) is used in optical communications.

3.1.3 Time-division multiplexing

Figure 3.2: Time-division multiplexing (TDM).

Time-division multiplexing (TDM) is a digital technology. TDM involves sequencing groups of a few bits or bytes from each individual input stream, one after the other, and in such a way that they can be associated with the appropriate receiver. If done sufficiently and quickly, the receiving devices will not detect that some of the circuit time was used to serve another logical communication path.

Consider an application requiring four terminals at an airport to reach a central computer. Each terminal communicated at 2400 bps, so rather than acquire four individual circuits to carry such a low-speed transmission, the airline has installed a pair of multiplexers. A pair of 9600 bps modems and one dedicated analog communications circuit from the airport ticket desk back to the airline data center are also installed.[1]

3.1.4 Code-division multiplexing

Code division multiplexing (CDM) is a technique in which each channel transmits its bits as a coded channel-specific sequence of pulses. This coded transmission typically is accomplished by transmitting a unique time-dependent series of short pulses, which are placed within chip times within the larger bit time. All channels, each with a different code, can be transmitted on the same fiber and asynchronously demultiplexed. Other widely used multiple access techniques are Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA).

Code Division Multiplex techniques are used as an access technology, namely Code Division Multiple Access (CDMA), in Universal Mobile Telecommunications System (UMTS) standard for the third generation (3G) mobile communication identified by the ITU. Another important application of the CDMA is the Global Positioning System (GPS).

However, the term *Code Division Multiple access* is also widely used to refer to a group of specific implementations of CDMA defined by Qualcomm for use in digital cellular telephony, which include IS-95 and IS-2000. The two different uses of this term can be confusing. Actually, CDMA (the Qualcomm standard) and UMTS have been competing for adoption in many markets.

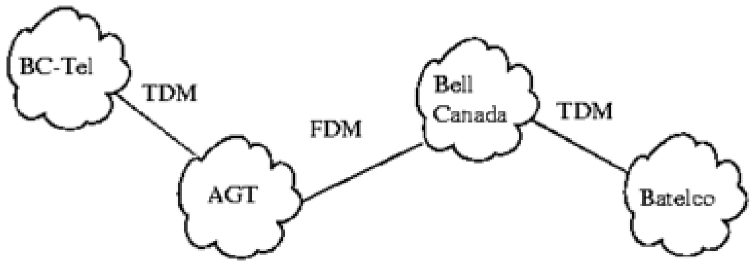


Figure 3.3 Telecommunication multiplexing

3.2 Relation to multiple access

A multiplexing technique may be further extended into a multiple access method or channel access method, for example TDM into Time-division multiple access (TDMA) and statistical multiplexing into carrier sense multiple access (CSMA). A multiple access method makes it possible for several transmitters connected to the same physical medium to share its capacity.

Multiplexing is provided by the Physical Layer of the OSI model, while multiple access also involves a media access control protocol, which is part of the Data Link Layer.

The Transport layer in the OSI model as well as TCP/IP model provides statistical multiplexing of several application layer data flows to/from the same computer.

3.3 Application areas

3.3.1 Telegraphy

The earliest communication technology using electrical wires, and therefore sharing an interest in the economies afforded by multiplexing, was the electric telegraph. Early experiments allowed two separate messages to travel in opposite directions simultaneously, first using an electric battery at both ends, then at only one end.

- ÉmileBaudot developed a time-multiplexing system of multiple Hughes machines in the 1870s.
- In 1874, the quadruplex telegraph developed by Thomas Edison transmitted two messages in each direction simultaneously, for a total of four messages transiting the same wire at the same time.
- Several workers were investigating acoustic telegraphy, a frequency-division multiplexing technique, which led to the invention of the telephone.

3.3.2 Telephony

In telephony, a customer's telephone line now typically ends at the remote concentrator box down the street, where it is multiplexed along with other telephone lines for that neighborhood or other similar area. The multiplexed signal is then carried to the central switching office on significantly fewer wires and for much further distances than a customer's line can practically go. This is likewise also true for digital subscriber lines (DSL).

Fiber in the loop (FITL) is a common method of multiplexing, which uses optical fiber as the backbone. It not only connects POTS phone lines with the rest of the PSTN, but also replaces DSL by connecting directly to Ethernet wired into the home. Asynchronous Transfer Mode is often the communications protocol used.

Because all of the phone (and data) lines have been clumped together, none of them can be accessed except through a demultiplexer. This provides for more-secure communications, though they are not typically encrypted.

The concept is also now used in cable TV, which is increasingly offering the same services as telephone companies. IPTV also depends on multiplexing.

3.3.3 Video processing

In video editing and processing systems, multiplexing refers to the process of interleaving audio and video into one coherent MPEG transport stream (time-division multiplexing).

In digital video, such a transport stream is normally a feature of a container format which may include metadata and other information, such as subtitles. The audio and video streams may have variable bit rate. Software that produces such a transport stream and/or container is commonly called a statistical multiplexor or **muxer**. A **demuxer** is software that extracts or otherwise makes available for separate processing the components of such a stream or container.

3.3.4 Digital broadcasting

In digital television and digital radio systems, several variable bit-rate data streams are multiplexed together to a fixed bitrate transport stream by means of statistical multiplexing. This makes it possible to transfer several video and audio channels simultaneously over the same frequency channel, together with various services.

In the digital television systems, this may involve several standard definition television (SDTV) programmes (particularly on DVB-T, DVB-S2, ISDB and ATSC-C), or one HDTV, possibly with a single SDTV companion channel over one 6 to 8 MHz-wide TV channel. The device that accomplishes this is called a statistical multiplexer. In several of these systems, the multiplexing results in an MPEG transport stream. The newer DVB standards DVB-S2 and DVB-T2 has the capacity to carry several HDTV channels in one multiplex. Even the original DVB standards can carry more HDTV channels in a multiplex if the most advanced MPEG-4 compressions hardware is used.

On communications satellites which carry broadcasttelevision networks and radio networks, this is known as **multiple channel per carrier** or **MCPC**. Where multiplexing is not practical (such as where there are different sources using a single transponder), single channel per carrier mode is used.

Signal multiplexing of satellite TV and radio channels is typically carried out in a central signal playout and uplinkcentre, such as ASTRA Platform Services in Germany, which provides playout, digital archiving, encryption, and satellite uplinks, as well as multiplexing, for hundreds of digital TV and radio channels.

In digital radio, both the Eureka 147 system of digital audio broadcasting and the in-band on-channelHD Radio, FMeXtra, and Digital Radio Mondiale systems can multiplex channels. This is essentially required with DAB-type transmissions (where a multiplex is called an **ensemble**), but is entirely optional with IBOC systems.

3.3.5 Analog broadcasting

In FM broadcasting and other analogradio media, multiplexing is a term commonly given to the process of adding subcarriers to the audio signal before it enters the transmitter, where modulation occurs. Multiplexing in this sense is sometimes known as **MPX**, which in turn is also an old term for stereophonic FM, seen on stereo systems since the 1960s.

4.0 Conclusion

In this unit you have been introduced to the fundamental concepts of Multiplexers. You also learnt the types of multiplexers.You were also introduced to the Various application areas of multiplexers.

5.0 References

- M. Morris Mano; Charles R. Kime (2008). *Logic and Computer Design Fundamentals* (4 ed.). Prentice Hall. ISBN 013198926X.
- *Voice and Data Communications*, ISBN 978-0-0-07-225732-9.
- Multiplexing filehandles with select() in perl". http://www.perlfect.com/articles/select.shtml.

- "Federal Standard 1037C: Glossary of Telecommunications Terms". Institute for Telecommunication Services. http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm. Retrieved 2009-10-19.

MODULE FOUR

UNIT 3DIGITAL TECHNOLOGIES

1.0 INTRODUCTION

A **digital** system is a data technology that uses discrete (discontinuous) values. By contrast, non-digital (or analog) systems use a continuous range of values to represent information. Although digital representations are discrete, the information represented can be either discrete, such as numbers, letters or icons, or continuous, such as sounds, images, and other measurements of continuous systems.The word *digital* comes from the same source as the word digit and *digitus* (the Latin word for *finger*), as fingers are used for discrete counting. It is most commonly used in computing and electronics, especially where real-world information is converted to binary numeric form as in digital audio and digital photography.

2.0 OBJECTIVES

By the end of this unit, you should be able to:

- Explain the meaning of a digital system

- State the properties of digital information

3.0 MAIN CONTENT

3.1 History

Although digital signals are generally associated with the binary electronic digital systems used in modern electronics and computing, digital systems are actually ancient, and need not be binary nor electronic.

- Written text in books (due to the limited character set and the use of discrete symbols - the alphabet in most cases)
- An *abacus* was created sometime between 1000 BC and 500 BC , it later become a form of calculation frequency, nowadays it can be used as a very advanced, yet basic digital calculator that uses beads on rows to represent numbers. Beads only have meaning in discrete up and down states, not in analog in-between states.
- A *beacon* is perhaps the simplest non-electronic digital signal, with just two states (on and off). In particular, *smoke signals* are one of the oldest examples of a digital signal, where an analog "carrier" (smoke) is modulated with a blanket to generate a digital signal (puffs) that conveys information.
- Morse code uses six digital states—dot, dash, intra-character gap (between each dot or dash), short gap (between each letter), medium gap (between words), and long gap (between sentences)—to send messages via a variety of potential carriers such as electricity or light, for example using an electrical telegraph or a flashing light.
- The Braille system was the first binary format for character encoding, using a six-bit code rendered as dot patterns.
- Flag semaphore uses rods or flags held in particular positions to send messages to the receiver watching them some distance away.
- International maritime signal flags have distinctive markings that represent letters of the alphabet to allow ships to send messages to each other.
- More recently invented, a modem modulates an analog "carrier" signal (such as sound) to encode binary electrical digital information, as a series of binary digital sound pulses. A slightly earlier, surprisingly reliable version of the same concept was to bundle a sequence of audio digital "signal" and "no signal" information (i.e. "sound" and "silence") on magnetic cassette tape for use with early home computers.

Properties of digital information

All digital information possesses common properties that distinguish it from analog communications methods:

- **Synchronization:** Since digital information is conveyed by the sequence in which symbols are ordered, all digital schemes have some method for determining the beginning of a sequence. In written or spoken human languages synchronization is typically provided by pauses (spaces), capitalization, and punctuation. Machine communications typically use special synchronization sequences.

- **Language:** All digital communications require a *language*, which in this context consists of all the information that the sender and receiver of the digital communication must both possess, in advance, in order for the communication to be successful. Languages are generally arbitrary and specify the meaning to be assigned to particular symbol sequences, the allowed range of values, methods to be used for synchronization, etc.
- **Errors:** Disturbances (noise) in analog communications invariably introduce some, generally small deviation or error between the intended and actual communication. Disturbances in a digital communication do not result in errors unless the disturbance is so large as to result in a symbol being misinterpreted as another symbol or disturb the sequence of symbols. It is therefore generally possible to have an entirely error-free digital communication. Further, techniques such as check codes may be used to detect errors and guarantee error-free communications through redundancy or retransmission. Errors in digital communications can take the form of *substitution errors* in which a symbol is replaced by another symbol, or *insertion/deletion* errors in which an extra incorrect symbol is inserted into or deleted from a digital message. Uncorrected errors in digital communications have unpredictable and generally large impact on the information content of the communication.
- **Copying:** Because of the inevitable presence of noise, making many successive copies of an analog communication is infeasible because each generation increases the noise. Because digital communications are generally error-free, copies of copies can be made indefinitely.
- **Granularity:** When a continuously variable analog value is represented in digital form there is always a decision as to the number of symbols to be assigned to that value. The number of symbols determines the precision or resolution of the resulting datum. The difference between the actual analog value and the digital representation is known as *quantization error*.

4.0 Conclusion

In this unit you have been introduced to the fundamental concepts of digital technologies. You have also learnt the history of digital technologies, and some of the properties of digital technologies were also discussed in this unit.

5.0 Summary

In this unit you have learnt:

- The meaning of a digital system
- The properties of digital information
- The history of the digital system

6.0 Tutor Marked Assignment

- What are the differences between the digital and the analog signals
- What property of the digital signal makes it better than the analog signal

7.0 Further Readings

- "Internet History: People". *Internet History People*. http://www.unc.edu/depts/jomc/academics/dri/pioneers2d.html. Retrieved July 3, 2006.
- Clark, David D., "The Design Philosophy of the DARPA Internet Protocols", Computer Communications Review 18:4, August 1988, pp. 106–114
- "The Risks Digest". *Great moments in e-mail history*. http://catless.ncl.ac.uk/Risks/20.25.html#subj3. Retrieved April 27, 2006.

MODULE FOUR

UNIT 4 SIGNAL TRANSMISSION AND IMPAIRMENT

1.0 INTRODUCTION

Transmission impairment is a property of a transmission medium which causes the signal to bedegraded, reduced in amplitude, distorted or contaminated. Impairment can introduce errors intodigital signals. Examples of transmission impairments are attenuation, delay distortion, andseveral sources of noise including, thermal noise, impulse noise, and inter-modulation noise.It is important to understand transmission impairments for several reasons. Understanding thesource of a transmission impairment like attenuation or dispersion will enable the user to partially correct for (equalize the signal) these effects. Understanding the source of transmissionimpairments (dispersion, attenuation, impulse noise, thermal noise) can also help the userunderstand some of the constraints placed on the transmission of data as a result of these effects.Such constraints include the maximum length of network links, the choice of physicaltransmission media, the choice of encoding methods, and the data rate supported by the medium.

Attenuation is a property of the transmission medium. It measures how much energy is absorbedand/or radiated from the traveling signal due to it's interaction with the transmission medium.Attenuation is measured as a function of the distance traveled through the transmission medium.The transmission medium absorbs energy because the signal is influenced by small impuritieswithin it. Such impurities have different sizes and distributions depending on the type ofmedium. Impurities of different sizes effect different frequencies in the signal. The effect ofattenuation is, therefore, a function of frequency. The frequency variation of attenuation can bepartially corrected, or equalized, by applying corrections based on a physical model. When asignal is attenuated it's amplitude is reduced. The interpretation of a received signal depends onbeing able to tell the difference between different signal levels. If the amplitude is reduced toomuch by attenuation it becomes impossible to accurately tell the difference between the different signal levels, and the information in the signal is lost.

2.0 Objectives

By the end of this unit, you should be able to:

- Explain the meaning of transmission impairment
- Describe the types of transmission impairment
- State the effects of noise
- Explain the bit error rate.
- State the differences between analog and digital transmission

3.0 Main Content

3.1 Types of impairments

- ✓ Attenuation
- ✓ Delay distortion
- ✓ Noise

3.1.1 Attenuation

Signal amplitude decrease along a transmission medium. This is known as*signal attenuation*. Amplifiers or repeaters are inserted at intervals along themedium to improve the received signal as closed as to its original level.Attenuation and amplification are measured in decibel (dB), which isexpressed as a constant number of decibels per unit distance.

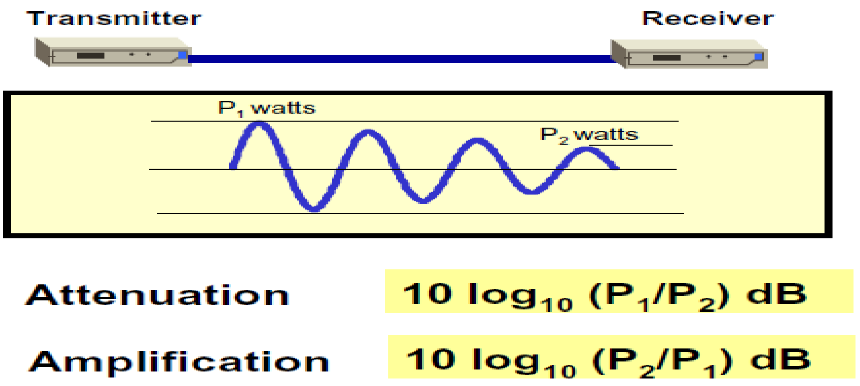
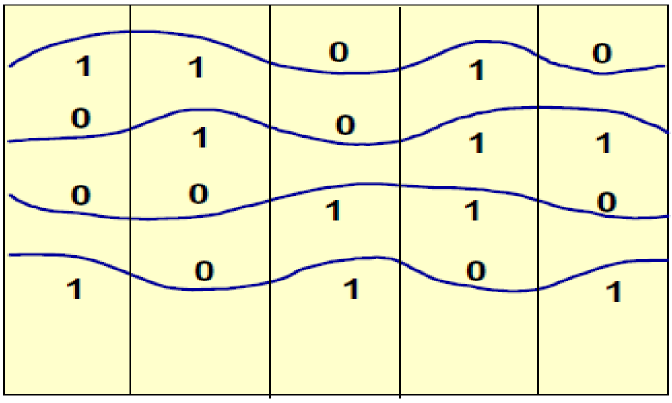


Fig 5.1: Attenuated and Amplified Signal along the Transmission Media

3.1.1 Delay distortion

The various frequency components in digital signal arrive at the receiver withvarying delays, resulting in *delay distortion*.As bit rate increase, some of the frequency components associated with eachbit transition are delayed and start to interfere with frequency componentsassociated with a later bit, causing *intersymbol interference*, which is a majorlimitation to maximum bit rate.



- **Velocity of propagation of a signal through a guided medium varies with frequency**
- **Signal components of one bit position will spill over into other bit position**
- **Results : limit max, bit rate transmission**
- **Solving : equalizing**

Fig 5.2: Velocity of propagation of a signal through guided media

3.1.2 Noise

Signal-to-noise ratio (S/N) is a parameter used to quantify how much noisethere is in a signal. A high SNR means a high power signal relative to noiselevel, resulting in a good-quality signal.

- **Effect**
  - **distorted a transmitted signal**
  - **attenuated a transmitted signal**
- **signal-to-noise ratio to quantify noise**

$$S/N_{db} = 10 \log_{10} \frac{S}{N}$$

S = average signal power

N = noise power

3.2 Noise types

Atmospheric Noise

- Lightning : static discharge of clouds
- Solar noise : sun's ionized gases
- Cosmic noise : distant stars radiate high frequency signal

Gaussian Noise

Thermal noise : generated by random motion of free electrons

Crosstalk

- NEXT
- FEXT

Impulse Noise : sudden bursts of irregularly pulses

Crosstalk

Crosstalk is interference generated when magnetic fields or current nearby wires interrupt electrical current in a wire. As electrical current travels through a wire, the current generates a magnetic field. Magnetic field from wires that are closed together can interfere each other.

Shielding the wire and twisting wire pairs around each other help decrease Crosstalk

NEXT (near-end crosstalk)

- interference in a wire at the transmitting end of a signal sent on a different wire

FEXT (far-end crosstalk)

- interference in a wire at the receiving end of a signal sent on a different wire

EFFECTS OF NOISE

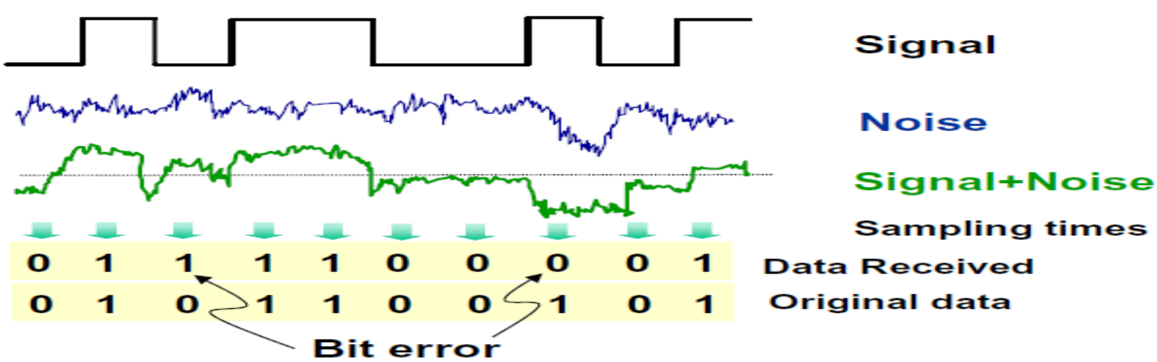


Fig 5.3: Effect of Noise

Impulse noise is the primary source of error for digital data. A sharp spike of energy of 0.01 seconds duration would not destroy any voice data, but would wash out many bits of digital data.

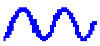
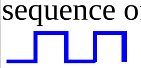
3.3 Bit Error Rate

- ✓ The BER (Bit Error Rate) is the probability of asingle bit being corrupted in a define time interval.
- ✓ BER of 10-5 means on average 1 bit in 10-5 will becorrupted
- ✓ A BER of 10-5 over voice-graded line is typical.
- ✓ BERs of less than 10-6 over digital communication iscommon.

A Bit Error Rate (BER) is a significant measure of system performance in terms of noise. A BER of 10-6, for example, means that one bit of every million may be destroyed during transmission. Several factors effect the BER:

- Bandwidth
- S/N
- Transmission medium
- Transmission distance
- Environment
- Performance of transmitter and receiver

Table 5.1 Analog and Digital Transmissions

	Analog	**digital**
Data	continuous (e.g., voice)	discrete (e.g., text)
Signal	continuous electromagnetic waves  Used mainly for transmitting data across a network.	sequence of voltage pulses  Used mainly internally within computers.
transmission	transmission of analog signals without regards to their content (the data may be analog or binary). The signals become weaker (attenuated) with the distance. Amplifiers may be used to strengthen the signals, but as side effect they also boost the noise. This might not be a problem for analog data, such as voice, but is a problem for digital data.	Transmission that is concerned with the content of the signal. Repeaters are used to overcome attenuation. A repeater recovers the digital pattern from the signal it gets, and resubmits a new signal.

3.4 ADVANTAGES OF DIGITAL TRANSMISSION.

- **Technology** Sees a drop in cost due to LSI and VLSI
- **Data integrity** Repeaters allow longer distances over lines of lesser quality.
- **Capacity utilization** Digital techniques can more easily and cheaply utilize, through multiplexing, available transmission links of high bandwidth.
- **Security and privacy** Encryption techniques are more readily applied to digital data
- **Integration** Simplified if digitized data is used everywhere.

3.5 SIGNAL TRANSMISSION ANALYSIS

The analysis of electrical signals is a fundamental problem for many engineers and scientists. Even if the immediate problem is not electrical, the basic parameters of interest are often changed into electrical signals by means of transducers. Common transducers include accelerometers and load cells in mechanical work, EEG electrodes and blood pressure probes in biology and medicine, and pH and conductivity probes in chemistry. The rewards for transforming physical parameters to electrical signals are great, as many instruments are available for the analysis of electrical signals in the time, frequency and modal domains. The powerful measurement and analysis capabilities of these instruments can lead to rapid understanding of the system under study.

4.0 Conclusion

In this unit you have been introduced to the fundamental concepts of transmission impairment. You also learnt the types of transmission impairments. You were also introduced to Bit error rate and some of the major differences between analog and digital transmissions.

5.0 Summary

In this unit you have learnt:

- The meaning of transmission impairment
- The types of transmission impairment
- The effects of noise
- The bit error rate.
- The differences between analog and digital transmission

6.0 Tutor Marked Assignment

- What do you understand by Transmission Impairment
- What is the difference between FEXT and NEXT
- What do you understand by the term “Noise”

7.0 Further Readings

- "Brazil, Russia, India and China to Lead Internet Growth Through 2011". Clickz.com. http://clickz.com/showPage.html?page=3626274. Retrieved 2009-05-28.
- FriedhelmHillebrand, ed. (2002): "GSM and UMTS, The Creation of Global Mobile Communications", John Wiley & Sons, ISBN 0-470-84322-5

MODULE FIVE NETWORK TECHNOLOGIES

UNIT 1: INTEGRATED SERVICE DIGITAL NETWORK (ISDN)

Table of Contents

1.0 INTRODUCTION

Having read through the course guide, you will have a general understanding of what this unit is about and how it fits into the course as a whole. This unit will describe the general concept of ISDN.

2.0 OBJECTIVES

By the end of this unit, you should be able to:

- Explain the term ISDN
- Describe the ISDN interfaces
- Explain how ISDN works

- Explain the usefulness of ISDN

3.0 MAIN CONTENT

3.1 What is ISDN?

ISDN (Integrated Services Digital Network) is a digital communications technology that enables a smallbusiness or an individual to connect directly to both the Internet and other sites/users (e.g.: forvideoconferencing). ISDN provides a standard interface for voice, fax, video, graphics, and data – all on asingle telephone line.

"***Integrated Services***" refers to ISDN's ability to deliver two simultaneous connections, in anycombination of voice, fax,, data, and video, over a single line. Multiple devices can be attached to theline, and used as needed.

"***Digital***" refers to the fact that it is a purely digital transmission, as opposed to the analog transmissionmethod used by conventional telephone lines.

"***Network***" refers to the fact that ISDN is not simply a point-to-point connection like a leased telephoneline – ISDN networks extend from the local telephone exchange to the remote user, and include all theswitching equipment in between. If your ISDN equipment includes analog capabilities, you can alsoconnect to telephones, fax machines, and analog modems – even though they may be connected tostandard analog telephone lines.

ISDN service is provided by the same companies that provide telephone service – you get much faster,more dependable connections for voice, fax, data, and video – all through a single connection.While not new (ISDN has been around for over 15 years), the advent of international standards has madeISDN viable as telephone companies around the world have upgraded their equipment to these ISDNstandards. It is now commonly available in Europe, Japan, Australia, and from most major North Americantelephone companies – AT&T, MCI, and Sprint can provide long-distance ISDN lines for global
connections. One of the reasons for its widespread use is that it works on the ordinary copper wire alreadyin place in the telephone system.

One advantage of ISDN over other digital communications technologies is its ability to handle all types ofinformation such as voice, computer data, studio-quality sound, and video.

3.2 History

The early phone network consisted of a pure analog system that connected telephone users directly by a mechanical interconnection of wires. This system was very inefficient, was very prone to breakdown and noise, and did not lend itself easily to long-distance connections. Beginning in the 1960s, the telephone system gradually began converting its internal connections to a packet-based, digital switching system. Today, nearly all voice switching in the U.S. is digital within the telephone network. Still, the final connection from the local central office to the customer equipment was, and still largely is, an analog Plain-Old Telephone Service (POTS) line.

A standards movement was started by the International Telephone and Telegraph Consultative Committee (CCITT), now known as the International Telecommunications Union (ITU). The ITU is a United Nations organization that coordinates and standardizes international telecommunications. Original recommendations of ISDN were in CCITT Recommendation I.120 (1984) which described some initial guidelines for implementing ISDN.

Local phone networks, especially the regional Bell operating companies, have long hailed the system, but they had been criticized for being slow to implement ISDN. One good reason for the delay is the fact that the two major switch manufacturers, Northern Telecom (now known as Nortel Networks), and AT&T (whose switch business is now owned by Lucent Technologies), selected different ways to implement the CCITT standards. These standards didn't always interoperate. This situation has been likened to that of earlier 19th century railroading. "People had different gauges, different tracks... nothing worked well."

In the early 1990s, an industry-wide effort began to establish a specific implementation for ISDN in the U.S. Members of the industry agreed to create the National ISDN 1 (**NI-1**) standard so that end users would not have to know the brand of switch they are connected to in order to buy equipment and software compatible with it. However, there were problems agreeing on this standard. In fact, many western states would not implement NI-1. Both Southwestern Bell and U.S. West (now Qwest) said that they did not plan to deploy NI-1 software in their central office switches due to incompatibilities with their existing ISDN networks.

Ultimately, all the Regional Bell Operating Companies (RBOCs) did support NI-1. A more comprehensive standardization initiative, National ISDN 2 (**NI-2**), was later adopted. Some manufacturers of ISDN communications equipment, such as Motorola and U S Robotics (now owned by 3Com), worked with the RBOCs to develop configuration standards for their equipment. These kinds of actions, along with more competitive pricing, inexpensive ISDN connection equipment, and the desire for people to have relatively low-cost high-bandwidth Internet access have made ISDN more popular in recent years.

Most recently, ISDN service has largely been displaced by broadband internet service, such as xDSL and Cable Modem service. These services are faster, less expensive, and easier to set up and maintain than ISDN. Still, ISDN has its place, as backup to dedicated lines, and in locations where broadband service is not yet available

3.3 Components of ISDN

While individual operating companies and ministries will define the specific services, within the ISDN architecture the ITU standards define a number of component parts and functions:

- ISDN CHANNELS
- ACCESS TYPES
- DEVICES
- INTERFACES
- PROTOCOLS

ISDN Channels

A CHANNEL is the basic unit of ISDN service. The ISDN Standards define three basic types of channels:

- Bearer channels (B channels)
- Delta (or "Demand") channels (D channels)
- High-capacity channels (H channels)

B Channel

A B channel is a 64-Kbps unit of clear digital bandwidth. Based on the data rate required to carry one digital voice conversation, a B channel can carry any type of digital information (voice, data, or video) with no restrictions on format or protocol imposed by the ISDN carrier.

D Channel

A D channel is a signaling channel. It carries the information needed to connect or disconnect calls and to negotiate special calling parameters (i.e., automatic number ID, call waiting, data protocol). The D channel can also carry packet-switched data using the X.25 protocol.

The D channel is not a clear channel. It operates according to a well-defined pair of layered protocols:

- Q.921 (LAPD) at the Data Link Layer (Layer 2)
- Q.931 at the upper layers (Layers 3 and above)

The data rate of a D channel varies according to the type of access it serves: a Basic Rate Access D channel operates at 16 Kbps and a Primary Rate Access D channel operates at 64 Kbps.

Signaling on the D Channel

The ISDN D channel carries all signaling between the customer's terminal device and the carrier's end switching office.

Signaling information with end-to-end significance (i.e., which must be received by the terminal device at a call's destination, such as Automatic Calling Number Identification information) travels between the carrier's switching offices on the carrier's common-channel signaling network and on to the destination terminal through the receiving user's D channel.

H Channel

An H channel is a special, high-speed clear channel. H channels, designed primarily for full-motion color video, are not yet in common use. There are currently three kinds of H channel:

- H0 ("H-zero")
- H11 ("H-one-one")
- H12 ("H-one-two")

An H0 channel operates at 384 Kbps (roughly one fourth of a North American Primary Rate Access or one fifth of a European Primary Rate Access). An H1 channel operates at 1.536 Mbps and occupies one whole North American Primary Rate Access. An H12 channel occupies an entire European Primary Rate Access.

ISDN Access Types

ISDN offers two general types of access:

- BASIC RATE ACCESS (BRA)
- PRIMARY RATE ACCESS (PRA)

These differ from one another by the amount of information they can carry.

Basic Rate Access

Basic Rate Access is based on new technology conceived especially for ISDN. Designed to provide service to individual users or small businesses, Basic Rate Access provides two 64-Kbps B channels and one 16-Kbps D channel (referred to as 2B+D). In other words, it provides transmission facilities for one voice conversation (one B channel), one medium-speed data session (the other B channel), and the signaling exchanges needed to make them work (the D channel).

Two B channels at 64 Kbps plus one D channel at 16 Kbps equals 144K bps. The ISDN Basic Rate transmission protocol uses an additional 48 Kbps of bandwidth for maintenance and synchronization, so an ISDN Basic Rate Access actually uses 192 Kbps.

Primary Rate Access

Primary Rate Access, which is based on pre-ISDN digital carrier technology, is designed to provide high-capacity service to large customers for applications such as PBX-to-PBX trunking. There are two kinds of Primary Rate Access: 23B+D and 30B+D. Each depends on the kind of digital carrier available in a given country.

In North America and Japan, 23B+D Primary Rate Access operates at 1.544 Mbps and offers 23 B channels plus 1 64-Kbps D channel (usually located in time-slot 23), or 4 H0 channels, or 1 H11 channel. In most of the rest of the world, 30B+D Primary Rate Access operates at 2.048 Mbps and offers 30 B channels plus 1 64-Kbps D channel (located in time-slot 16), or 5 H0 channels, or 1 H12 channel.

3.4 ISDN Devices

In the context of ISDN standards, STANDARD DEVICES refers not to actual hardware, but to standard collections of functions that can usually be performed by individual hardware units. The ISDN Standard Devices are:

- Terminal Equipment (TE)
- Terminal Adapter (TA)
- Network Termination 1 (NT1)
- Network Termination 2 (NT2)
- Exchange Termination (ET)

Terminal Equipment (TE)

A TE is any piece of communicating equipment that complies with the ISDN standards. Examples include: digital telephones, ISDN data terminals, Group IV Fax machines, and ISDN-equipped computers.

In most cases, a TE should be able to provide a full Basic Rate Access (2B+D), although some TEs may use only 1B+D or even only a D channel.

Terminal Adapter (TA)

A TA is a special interface-conversion device that allows communicating devices that don't conform to ISDN standards to communicate over the ISDN.

The most common TAs provide Basic Rate Access and have one RJ-type modular jack for voice and one RS-232 or V.35 connector for data (with each port able to connect to either of the available B channels). Some TAs have a separate data connector for the D channel.

Network Termination (NT1 and NT2)

The NT devices, NT1 and NT2, form the physical and logical boundary between the customer's premises and the carrier's network. NT1 performs the logical interface functions of switching and local-device control (local signaling). NT2 performs the physical interface conversion between the dissimilar customer and network sides of the interface.

In most cases, a single device, such as a PBX or digital multiplexer, performs both physical and logical interface functions. In ISDN terms, such a device is called NT12 ("NT-one-two") or simply NT.

Exchange Termination (ET)

The ET forms the physical and logical boundary between the digital local loop and the carrier's switching office. It performs the same functions at the end office that the NT performs at the customer's premises.

In addition, the ET:

1. Separates the B channels, placing them on the proper interoffice trunks to their ultimate destinations
2. Terminates the signaling path of the customer's D channel, converting any necessary end-to-end signaling from the ISDN D-channel signaling protocol to the carrier's switch-to- switch trunk signaling protocol

3.5 ISDN Interfaces (Standard Reference Points)

The ISDN standards specify four distinct interfaces in the customer's connection to the network: R, S, T, and U.

From the standards viewpoint, these are not "real" physical interfaces, but simply STANDARD REFERENCE POINTS where physical interfaces may be necessary. However, in common practice, the names of reference points are used to refer to physical interfaces.

3.5.1 The R Interface

The interface at reference point R is the physical and logical interface between a non-ISDN terminal device and a terminal adapter (TA). The R interface is not really part of the ISDN; it can conform to any of the common telephone or data interface standards.

3.5.2 The S Interface

The interface at reference point S is the physical and logical interface between a TE (or TA) and an NT. The S interface uses four wires and employs a bipolar transmission technique known as Alternate Mark Inversion (AMI).

A special feature of the S interface is the "Short Passive Bus" configuration, which allows up to eight ISDN devices (TE or TA) to contend for packet access to the D channel in a prioritized, round-robin fashion. Only one device at a time can use a given B channel.

3.5.3 The T Interface

The interface at reference point T is the physical and logical interface between NT1 and NT2, whenever the two NTs are implemented as separate pieces of hardware. The specification for the T interface is identical to the specification for the S interface.

In most implementations, NT1 and NT2 exist in the same physical device, so there is no real T interface.

3.5.4 The U Interface

The interface at reference point U is the physical and logical interface between NT (or NT2) and the ISDN carrier's local transmission loop. It is also the legal demarcation between the carrier's loop and the customer's premises.

The U interface is implemented with two wires and uses a special quaternary signal format (i.e., four possible electrical states, with one pulse encoding a predefined combination of 2 bits) called 2B1Q. Quaternary encoding allows the U interface to carry data with a logical bit rate of 192 Kbps over a signal with a physical pulse rate of only 96 Kbps. The slower pulse rate is better suited to the less-predictable environment of the outside-plant loop carrier system.

3.6 How Does ISDN Work?

The simplest ISDN connection (called Basic Rate or BRI) consists of two 64 Kbps (kilobits-per-second)data channels (called B-channels) plus a 16 Kbps control channel (called the D-channel). This is sometimesReferred to as “2B+D.”On the other end of the spectrum is Primary Rate ISDN (called PRI) with 23 B-channels plus a D-channel (i.e.: “23B+D”).

To connect to the ISDN line, you need a black-box called an NT1 Network Terminator – a power supply(which you also need) is often built-in.You will also need a Terminal Adapter (often called a "TA") to connect non-ISDN equipment (such as yourcomputer or fax machine) to the line – these are also available as plug-in cards for PC's. Some TA's workas Ethernet bridges so that you can connect your LAN directly to the ISDN line.

3.7 The Usefulness of ISDN

One of the most common uses for this technology today is videoconferencing. By using from one to fourBRI lines, a videoconference can be established between two or more sites – the more lines, the faster theconnection. For a videoconference application, higher connection speed translates to higher resolution andvideo frame rates. The telephone company infrastructure allows these connections to be made in a similarfashion to dialing a telephone.While video conferencing has been around for a long time, in the past it has primarily been confined to large corporations. The ability to transmit quality voice and video over long distances used to require expensive equipment and costly leased lines – these could only be justified by the largest of companies. Due to this dependency on leased lines, videoconferences were point-to-point (e.g.: headquarters might be permanently linked to a manufacturing plant). Videoconferencing on the scale of teleconferencing was simply impractical.
The advent of new low-cost videoconference hardware that can utilize ISDN is rapidly changing this. Both desktop conferencing (a participant uses a PC equipped with a microphone, a small video camera, and an ISDN interface) and true videoconferencing (where more sophisticated equipment and remote control cameras allow group participation) have become as easy to set up as voice conferencing. Due to ISDN's versatility, videoconferences can include the sharing of graphic images and presentations, computer applications, documents, and computer files. This capability is proving popular for telecommuting, long distance meetings, workgroup collaboration, security and surveillance, and dozens of other innovative applications.

4.0 Conclusion

In this unit you have been introduced to the fundamental concepts of ISDN. You have also learnt the different components and interfaces of ISDN.

5.0 Summary

At the end of this unit, you have learnt:

- The explanation of the term ISDN
- The Description of the ISDN interfaces
- How ISDN works
- The usefulness of ISDN

MODULE FIVE

UNIT 2 DIGITAL SUBSCRIBER LINE (DSL)

Table of Contents

1.0 INTRODUCTION

A DSL is a specialized and problem-oriented language. Contrarily to a General Purpose Language (GPL) (e.g., UML, Java or C#), a DSL serves to accurately describe a domain of knowledge. The interest to combine a DSL and a transformation function is to raise the abstraction level of software. A DSL user concentrates her/his efforts on domain description while complexity, design and implementation decisions and details are hidden. The stake is to improve productivity and software quality.

However, what is the next consensus beyond this general definition? An experience consists in starting the development of a DSL editor coupled to a generator. Quickly, the issue of the variants of DSL editors and generators emerges. Regarding the language, is it a tree-based DSL or a set of data without real structure? Is it a graphical or textual notation? Is it a declarative or imperative style?

2.0 OBJECTIVES

By the end of this unit, you should be able to:

- Explain the term DSL
- Describe the benefits of DSL
- State the features of DSL
- Explain how DSL works
- State the advantages and disadvantages of DSL

3.0 MAIN CONTENT

3.1 What is DSL?

DSL is a telephone loop technology that uses existing copper phones lines, and provides a dedicated, high speed Internet connection. One of the big advantages of some DSLs (notably ADSL), are that they can co-exist on the same line with a traditional voice service such as "POTS" (Plain Old Telephone Service), and even ISDN. This is accomplished by utilizing different frequency ranges above the voice range (voice is up to 4KHz). Essentially, this gives two lines in one: one for voice, and one for Internet connectivity. When all is working normally, there should be no interference between the two "lines". This gives DSL a potentially broad consumer base, and helps minimize costs for service providers.

DSL is positioned for the Home and Small Office (SOHO) market that is looking for high speed Internet access at reasonable prices. Since it also typically provides dedicated, "always on" access, it can be used for interconnecting low to mid range bandwidth servers, and provides a great access solution for small LANs. It is also great for those Linux power users that just want a fat pipe :-).

Phone companies, and other independent telecommunications providers (CLECs), are now deploying DSL to stay ahead of the Cable companies -- the main consumer and SOHO competition for DSL providers. This mad rush to get "a piece of the pie", is bringing much competition (a good thing!), much diversity, and some confusion, into the consumer market. The DSL provider (often, but not always, the phone company) will provide the DSL infrastructure. This would include your line, the DSLAM, and physical connection to the outside world. From there it is typically picked up by an ISP, who provides the traditional Internet services.

Consumer DSL plans are typically "best effort" services. While boasting speeds approaching T1, and even surpassing that in some cases, it is not necessarily as reliable as T1 however. Business class DSL offers more reliability at a higher cost than consumer plans, and is a good compromise where both reliability and bandwidth are at a premium. All in all, the cost of DSL compared to traditional telco services, such as T1, is attractive and substantially more affordable for home and small business users.

DSL providers often do not have service contracts for home users, while business class DSL services typically do include similar SLAs (Service Level Agreements) to that offered for a T1 line.

The downside is that DSL is not available everywhere. Availability, and available bit rate (speed), are purely a function of where you live, where the telco has installed the prerequisite hardware, how far you are from the DSLAM/CO, and the quality of your phone line (loop). Not all loops are created equal, unfortunately. The primary limitation is distance.

3.2 History of DSL

Implementation of Digital Subscriber Line technology originally was part of the Integrated Services Digital Network (ISDN) specification published in 1984 by the CCITT and ITU as part of Recommendation I.120, later reused as ISDN Digital Subscriber Line (IDSL). Engineers have developed higher-speed DSL facilities such as High bit rate Digital Subscriber Line (HDSL) and Symmetric Digital Subscriber Line (SDSL) to provision traditional Digital Signal 1 (DS1) services over standard copper pair facilities. Consumer-oriented Asymmetric Digital Subscriber Line (ADSL), first tested at Bellcore in 1988, was designed to operate on existing lines already conditioned for BRI ISDN services, which itself is a switched digital service (non-IP), though most incumbent local exchange carriers (ILECs) provision Rate-Adaptive Digital Subscriber Line (RADSL) to work on virtually any available copper pair facility—whether conditioned for BRI or not.

The development of DSL, like many other forms of communication, can be traced backtoClaude Shannon]'s seminal 1948 paper: 'A Mathematical Theory of Communication". Employees at Bellcore (now Telcordia Technologies) developed ADSL in 1988 by placing wide-band digital signals above the existing [[baseband]] analog voice signal carried between [[telephone company]] [[central office]]s and customers on conventional [[twisted pair]] cabling facilitiesA DSL circuit provides "digital service". The underlying technology of transport across DSL facilities uses high-frequency [[sinusoidal]] [[carrier wave]] modulation, which is an analog signal transmission. A DSL circuit terminates at each end in a [[modem]] which modulates patterns of [[Binary digit|bits]] into certain high-frequency impulses for transmission to the opposing modem. Signals received from the far-end modem are demodulated to yield a corresponding bit pattern that the modem retransmits, in digital form, to its interfaced equipment, such as a computer, router, switch, etc. Unlike traditional dial-up modems, which modulate bits into signals in the 300–3400 Hz baseband (voice service), DSL modems modulate frequencies from 4000 Hz to as high as 4 MHz. This frequency band separation enables DSL service and [[plain old telephone service]] (POTS) to coexist on the same copper pair facility. Generally, higher bit rate transmissions require a wider frequency band, though the ratio of bit rate to bandwidth are not linear due to significant innovations in [[digital signal processing]] and [[Digital_modulation#Digital_modulation_methods|digital modulation methods]].

Early DSL service required a dedicated [[dry loop]], but when the U.S. [[Federal Communications Commission]] (FCC) required ILECs to lease their lines to competing DSL service providers, shared-line DSL became available. Also known as DSL over [[Unbundled Network Element]], this unbundling of services allows a single subscriber to receive two separate services from two separate providers on one cable pair. The DSL service provider's equipment is co-located in the same central office as that of the ILEC supplying the customer's pre-existing voice service. The subscriber's circuit is then rewired to interface with hardware supplied by the ILEC which combines a DSL frequency and POTS frequency on a single copper pair facility.

On the subscriber's end of the circuit, inline [[low-pass]] [[DSL filter]]s (splitters) are installed on each telephone to filter the high-frequency "hiss" that would otherwise be heard. Conversely, [[High-pass filter|high-pass]] filters already incorporated in the circuitry of DSL modems filter out voice frequencies. Although ADSL and RADSL modulation do not use the voice-frequency band, nonlinear elements in the phone could otherwise generate audible intermodulation and may impair the operation of the data modem in the absence of low-pass filters

3.3FEATURES OF DSL

- Language feature
- Transformation feature
- Tool feature
- Process feature

At the root level, language and transformation are mandatory features because they are parts of the DSL definition. Tool is also mandatory because it serves to automate transformation from a domain, the problem space, down to lower abstraction levels, the solution space. Process is optional because it can be undefined or implicit.

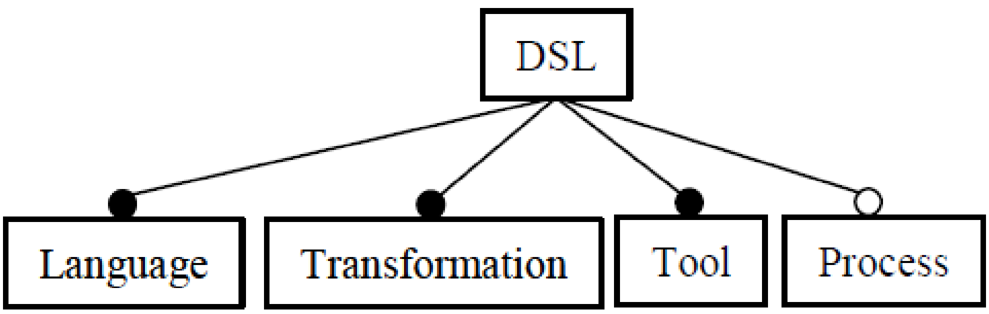


Figure 2.1: Root of the DSL Feature Model

3.4 Benefits of DSL

Fast DSL access allows you to download images, videos and other large files at lightning-fast speeds.

It's always on: There is no waiting to get connected, no busy signals, no dialing required with DSL.

No extra phone line necessary: DSL technology uses your existing phone line, allowing you to share phone and Internet on the same line — at the same time. You can also use other devices as usual on your telephone
line. DSL won't interfere.

Fast Internet connection. You'll be able to download information, graphics and video from the Internet at speeds up to 2.3 Mb/s. A:d, you can upload information as fast as 2.3 Mb/s.

Dedicated line: You'll be the only person using your connection and line. Unlike cable or modems, you don't
share your connection with other users, so your Internet speed will be more private, stable and will have
fewer delays.

Available in limited areas: DSL users must be within a certain radius of the area telephone switch.

3.5 How DSL Works

DSL is an innovative technology that allows your computer to transmit information over your existing phone line, but at a higher frequency than telephones, fax machines and other devices. Because it utilizes the higher frequencies, you can use the same phone line for telephone calls and your Internet connection at the same time, without any interference. Your telephone calls will still be clear and crisp, and your Internet connection will seem like lightning compared to a 56K modem connection.

3.6 Advantages of DSL

- The speed is much higher than a regular modem
- DSL doesn't necessarily require new wiring
- The company that offer DSL will usually provide the modem as part of the installation

3.7 Disadvantages of DSL

- The service is not available everywhere
- The connection is fast for receiving data than it is for sending data over the internet
- A DSL works better when you are closer to the provider's central office

4.0 Conclusion

A DSL is a problem-oriented language, which combined to transformation tools, such asgenerators, serves to raise the abstraction level of software and ease software development.But beyond this general definition, DSL and DSL tool variants are numerous. The reason of aDSL feature model is to formalize DSL and DSL tool variants. A first application of thisfeature model is a DSL tool factory, which applies variations during production of DSL tools.A second application is the selection of pertinent DSL families among all possible familiesfrom the feature model. A third application is the definition of DSL tool foundations. A fourthusage is the selection of DSL tools. The feature model, combined with classification criteria,contains needed information to evaluate DSL tools. DSL feature model is in the scope ofdomain analysis of DSLs. Its clarification becomes a prerequisite for long-term and largescaleDSL developments.

5.0 Summary

In this unit you have learnt

- The definition of the term DSL
- The benefits of DSL
- The features of DSL
- How DSL works
- The advantages and disadvantages of DSL

7.0 Further Readings

[1] ANT, Apache Project, http://ant.apache.org/

[2] ATL, Atlas Transformation Language, official web-site. http://www.sciences.univnantes.fr/lina/atl.

[3] Bass, L., Clements, P., Kazman, R., Software Architecture in Practice, Addison Wesley, 2003.

[4] Czarnecki, K., Eisenecker, U.W. Generative Programming, Addison-Wesley, 2000.

[5] Czarnecki, K., Helsen, S., Classification of Model Transformation Approaches, OOPSLA 2003, Workshop on Generative Techniques in the Context of Model-Driven Architecture.

[6] Eclipse, GMF web site, http://www.eclipse.org/gmf/

[7] Greenfield, J., Short, K., Cook, S., and Kent, S., Software Factories, Assembling applications with Patterns, Models, Framework, and Tools, Wiley, 2004.

[8] IEEE, IEEE Recommended Practice for Architectural Description of Software-IntensiveSystems, IEEE Std 1471-2000, 21 September 2000.

MODULE FIVE

UNIT 3 SYNCHRONOUS OPTICAL NETWORK (SONET)

1.0 INTRODUCTION

In today's business world, each industry is looking for different ways to create competitiveadvantages to deliver information, products and services in a more timely and costeffective manner. End-to-end SONET (Synchronous Optical Networking) networksolutions are one important ingredient in creating a competitive edge. As a convergencetechnology, SONET provides for the unification of voice, data and video over the sametransport service.

This guide is intended to offer an operational overview of SONET (Synchronous Optical

Networking) for those who are not familiar with the standard, or those who want torefresh their knowledge. At the beginning of this document, an important point toremember is this: SONET is a powerful, highly scalable technology. Although it may appear to be complex, most of what goes on in a SONET network is transparent to the user. Another note of importance: This guide briefly discusses Wave DivisionMultiplexing (WDM) for awareness purposes only, since WDM is another highperformancetransport technology that also leverages fiber optics.
SONET is a *transport* technology, designed to provide enterprise and government users – as well as service providers – a network infrastructure with survivability characteristics, sothat business operations continue uninterrupted. SONET's self-healing fiber optic ring functionality enables automatic network recovery due to failures that can be caused by a fiber optic cable cut, lost signal, or degraded signal (e.g. due to aging laser) ornode/system failure. SONET is also a technology that is designed to ensure network traffic is restored within 60 milliseconds in the event of a failure.

2.0 OBJECTIVES

By the end of this unit, you should be able to:

- Define the term SONET
- Explain the inception of SONET
- State the standards of SONET
- Describe the topologies of SONET
- Describe the SONET equipment layers
- Explain SONET synchronization and timing

3.0 MAIN CONTENT

3.1 Definition

Synchronous optical network (SONET) is a standard for opticaltelecommunications transport formulated by the Exchange Carriers StandardsAssociation (ECSA) for the American National Standards Institute (ANSI), whichsets industry standards in the U.S. for telecommunications and other industries.
The comprehensive SONET standard is expected to provide the transport infrastructure for worldwide telecommunications for at least the next two or three decades.

3.2 INCEPTION OF SONET

SONET was conceived of and written about back in the early 1980's, when submitted tothe members of American National Standard Institute (ANSI) T1 Committee as auniversal transport system. In the mid-1980's the T1 Committee further enhanced thestandard to arrive at the Synchronous Transport Signal One

(STS-1) as the base-signalingrate. Around this time, the ITU-T (International Telecommunication Union-Telecommunications standard) (formerly CCITT) adopted SONET as the basis ofor itsinternational standard referred to as SDH (Synchronous Digital Hierarchy) transportsystem, where the STS-1 rate (51.84Mbps) was to be a factor of 3 in terms of theEuropean base rate of 155.52Mbps.

3.3 SONET STANDARDS

The base standard for SONET is the T1.105-1991 American National Standard (ANSI)for Telecommunications- Digital Hierarchy-Optical Interface Rates and FormatsSpecification (SONET). SONET standards define rates and formats as well as opticalinterfaces. The following American National Standards Institute (ANSI) specificationsprovide the primary standards, which define SONET:

- ANSI T1.106-1998 Specification for Optical Parameters
- ANSI T1.102-1993 Specification for Electrical Parameters
- ANSI T1.105-1991 Specification for Multiplexing Methods to Map Existing
- Digital Signals (e.g. DS1) into SONET Payload Signals
- ANSI T1.105-1991 Specification for Criteria for Optical Line Automatic
- Protection Switching
- ANSI T1.105-1991 Specification for Overhead Channels to Support Standard
- Operation, Administration and Provisioning (OAM&P)

3.4 SONET TOPOLOGIES

SONET technology enables a number of different network topologies to solve networkingrequirements, including survivability, cost, and bandwidth efficiencies. The followingprovides a description of 3 different SONET configurations, which are deployed in avariety of enterprise situations. The SONET configurations include:

- Point-to-point configuration
- Hubbed configuration
- Linear Add/Drop configuration
- Ring configuration

3.4.1 Point-to-Point Configuration

SONET point-to-point configurations (see figure 2) create a simple topology that terminates a SONET payload at each point of a fiber optic cable span. Point-to-pointconfigurations are typically deployed in transport applications, which require a singleSONET multiplexer in a single route. Point-to-point configurations can be enhanced toincrease survivability by to deploying a protection path (second fiber span) over a differentpath between two or more SONET multiplexers.

3.4.2 Hubbed Configuration

Hubbed configurations (see figure 3) consolidate traffic from multiple sites onto a singleoptical channel, which then can be forwarded to another site. This topology is often usedin applications where the user wants to consolidate traffic from multiple satellite sites to asingle site such as corporate headquarters, before extending it, in some cases to a centraloffice. This topology helps to reduce the number of hops as well as the equipmentrequired to create a multisite topology.

3.4.3 Linear Add/Drop Configuration

In the asynchronous digital signal hierarchy environment, every time a digital signal isaccessed the entire signal needs to be multiplexed/demultiplexed, costing time and moneyat each site along a given path. However, a Linear Add/Drop configuration enables direct access to VTS/STS channels at each intermediate site along a fiber opticpath. Therefore the Linear Add/Drop configuration eliminates the need to process(multiplex/demultiplex) the entire optical signal for pass-through traffic.

3.4.4 Self-Healing Ring Configuration

In a Self-Healing Ring configuration, a mechanism referred to as Automatic ProtectionSwitching is employed. There are two types of protection ring topologies. The first isUPSR (unidirectional Path Switched Ring), the other is BLSR (Bi-directional LineSwitched Ring). Each of these ring topologies is discussed later in this section of thisdocument. The Self-Healing Ring configuration is the most commonly deployed SONETtopology in mission critical government and enterprise backbones, due to its survivabilitycharacteristics.Automatic Protection Switching is a mechanism provided within the SONET specificationthat is designed to provide duplicate finer span paths. In this configuration, a backup fiberspan (protection ring) is enabled when and if there is a failure within the fiber spancurrently carrying traffic on a SONET network. It should be noted that during normaloperating conditions, both fiber spans are always active, and a SONET multiplexer selectswhich fiber span to receive traffic, based on an internal algorithm (e.g. based on whichfiber module was installed in the multiplexer first). The SONET standard specifies that the

protection ring should automatically become the fiber span (ring) the SONET multiplexerreceives traffic from within 60 milliseconds (unnoticeable to the user) in the event of afailure on the other fiber span

3.5 SONET EQUIPMENT LAYERS

SONET defines the end-to-end connection as being made up of 3 different equipmentlayers, including Path Terminating Equipment (PTE), Line Terminating Equipment (LTE),and Section Terminating Equipment (STE). Figure 10 illustrates where each terminatingequipment function resides within a SONET network.

3.6 Path Terminating Equipment (PTE)

STS (Synchronous Transport Signal) path terminating equipment provides the multiplexing and demultiplexing functions within a SONET network. Path terminatingequipment can originate, access, modify, or terminate path overhead in any combination.

3.7 Line Terminating Equipment (LTE)

SONET line terminating equipment provides the function that originates and terminatesline signals. SONET line terminating equipment can originate, access, modify, or terminateline overhead in any combination

3.8 Section Terminating Equipment (STE)

A SONET "section" is any two neighboring SONET network elements. SONET sectionterminating equipment can be a network element or a SONET regenerator. SONETsection terminating equipment can originate, access, modify, or terminate section overheadin any combination

3.9 Importance of Synchronized Timing

Network timing between SONET devices is an integral part of maintaining accurateinformation transmitted over a SONET network.In the earlier days of networking, the method used in timing was Asynchronous. InAsynchronous timing each switch runs its own clock. In Synchronous timing, switchescan use a single common clock to maintain timing. This single common clock is referred to as a Primary Reference Source (PRS) or Master Clock. Synchronous timing maintainsbetter accuracy than Asynchronous timing because it uses a single common clockingscheme to maintain timing. This accurate timing often becomes important to governmentand enterprise applications, particularly when they are running time sensitive applications(e.g. video streaming applications).There are three methods typically used in obtaining synchronous timing in SONETmultiplexers (e.g. Lucent DDM-2000 Multiplexer), they include:

- Timing from an onboard internal oscillator
- Timing from an incoming optical signal from a high-speed interface
- Timing from an external source coming from a DS1 timing reference that can bestratum 3 or higher clocking

4.0 Conclusion

In this unit you have been introduced to the fundamental concepts of SONET. You also learnt the inception of SONET,the various standards of SONET. You were also introduced to various topologies of SONET.

5.0 Summary

In this unit you have learnt

- Definition of the term SONET
- Explain the inception of SONET
- State the standards of SONET
- Describe the topologies of SONET
- Describe the SONET equipment layers
- Explain SONET synchronization and timing

6.0 Tutor Marked Assignment

State and Explain all you have learnt about SONET

7.0 Further Readings

"About Rand". *Paul Baran and the Origins of the Internet*. http://www.rand.org/about/history/baran.html. Retrieved January 14, 2006.

"How does the Internet Work?". http://tldp.org/HOWTO/Unix-and-Internet-Fundamentals-HOWTO/internet.html. Retrieved June 15, 2009.

Johna Till Johnson. "Net was born of economic necessity, not fear". http://www.networkworld.com/columnists/2004/0607johnson.html. Retrieved June 15, 2009.URL is sufficient attribution

Leonard Kleinrock (2005). *The history of the Internet*. http://www.lk.cs.ucla.edu/personal_history.html. Retrieved 2009-05-28.

MODULE FIVE

UNIT 4 PACKET SWITCHING

1.0 INTRODUCTION

Packet switching is the basis for the Internet Protocol (IP) [152, 172]. In packet switching, information flows are broken into variable-size packets (or fixed-size cellsas in the case of ATM). These packets are sent, one by one, to the nearest router, whichwill look up the destination address, and then forward them to the corresponding nexthop. This process is repeated until the packet reaches its destination. The routing ofthe information is thus done locally, hop-by-hop. Routing decisions are independentof other decisions in the past and in other routers; however, they are based on networkstate and topology information that is exchanged among routers using BGP, IS-IS orOSPF [148]. The network does not need to keep any state to operate, other than therouting tables.The forwarding mechanism is called store-and-forward because IP packets arecompletely received, stored in the router while being processed, and then transmitted.Additionally, packets may need to be buffered locally to resolve contention for resources. If the system runs out of buffers, packets are dropped.

2.0 Objectives

By the end of this unit, you should be able to:

- Define the term Packet Switching
- State the advantages and disadvantages of packet switching
- State various packet switching methods

3.0 Main Content

3.1 History

The concept of switching small blocks of data was first explored by Paul Baran in the early 1960s. Independently, [[Donald Davies]] at the National Physical Laboratory in the UK had developed the same ideas (Abbate, 2000).[[Leonard Kleinrock]] conducted early research in [[queueing theory]] which would be important in packet switching, and published a book in the related field of digital [[message switching]] (without the packets) in 1961; he also later played a leading role in building and management of the world's first packet switched network, the ARPANET

Baran developed the concept of message block switching during his research at the RAND Corporation for the US Air Force into survivable communications networks, first presented to the Air Force in the summer of 1961 as briefing B-265Baran's P-2626 paper described a general architecture for a large-scale, distributed, survivable communications network. The paper focuses on three key ideas: first, use of a decentralized network with multiple paths between any two points; and second, dividing complete user messages into what he called "message blocks" (later called packets); then third, delivery of these messages by store and forward switching.

Baran's study made its way to Robert Taylor (computer scientist)|Robert Taylor and J.C.R. Licklider at the Information Processing Technology Office, both wide-area network evangelists, and it helped influence Lawrence Roberts to adopt the technology when Taylor put him in charge of development of the ARPANET.Baran's work was similar to the research performed independently by Donald Davies at the National Physical Laboratory, UK. In 1965, Davies developed the concept of packet-switched networks and proposed development of a UK wide network. He gave a talk on the proposal in 1966, after which a person from the Ministry of Defense told him about Baran's work. A member of Davies' team met Lawrence Roberts at the 1967 [[Association for Computing Machinery|ACM]] Symposium on Operating System Principles, bringing the two groups together.

Interestingly, Davies had chosen some of the same parameters for his original network design as Baran, such as a packet size of 1024 bits. In 1966 Davies proposed that a network should be built at the laboratory to serve the needs of NPL and prove the feasibility of packet switching. The NPL Data Communications Network entered service in 1970. Roberts and the ARPANET team took the name "packet switching" itself from Davies's work.The first computer network and packet switching network deployed for computer resource sharing was the Octopus Network at the [[Lawrence Livermore National Laboratory]] that began connecting four [[CDC 6600|Control Data 6600 computers]] to several shared storage devices (including an [[IBM 2321 Data Cell].

3.2 Packet Switching Definition

Packet switching is the dividing of messages into *packets* before they are sent, transmitting each packet individually, and then reassembling them into the original message once all of them have arrived at the intended destination.

Packets are the fundamental unit of information transport in all modern computer networks, and increasingly in other communications networks as well. Each packet, which can be of fixed or variable size depending on the protocol, consists of a *header*, body (also called a *payload*) and a *trailer*. The body contains a segment of the message being transmitted.

3.3 ADVANTAGES

- Share link usage è Greater link efficiency
- Links can transmit at different rates è Rate conversion
- Under heavy load, calls can still be accepted but with greater delay
- Can prioritize packet transmission

3.4 DISADVANTAGES

- Packet delay at each node (Processing, Queuing, Transmission)
- A packet can acquire jitter while passing through the network
- Packets may contain metadata i.e Higher overhead than circuit Switching (e.g., telephone system)

- More processing required at each node in the network.

3.5 Packet Switching Methods

- **Datagram (Connectionless)**

- Each packet carries a header with full destination address.
- Each packet is treated independent of other packets.
- Each network node chooses the next hop for each packet.

- **Virtual Circuit Switching (Connection-Oriented)**

- Each packet header contains a virtual circuit identifier (VCI)
- Each node routes packets based on the VCI field
- A preplanned route is established before sending packets
- Faster routing

Source Routing: Full path stored in packet.

4.0 Conclusion

In this unit you have been introduced to the fundamental concepts of Packet switching. You also learnt the advantages and disadvantages of packet switching. You were also introduced to various packet switching methods.

5.0 Summary

In this unit you have learnt

- The definitionof the term Packet Switching
- The advantages and disadvantages of packet switching
- The various packet switching methods

6.0 Tutor Marked Assignment

- State the advantages and the disadvantages of Packet Switching
- What do you understand by the term “Datagram”

7.0 Further Readings

- Ronda Hauben (2001). *From the ARPANET to the Internet*. http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt. Retrieved 2009-05-28.
- "NORSAR and the Internet". NORSAR. http://www.norsar.no/pc-5-30-NORSAR-and-the-Internet.aspx. Retrieved 2009-06-05.
- tsbedh. "History of X.25, CCITT Plenary Assemblies and Book Colors". Itu.int. http://www.itu.int/ITU-T/studygroups/com17/history.html. Retrieved 2009-06-05.
- Prasad, K. V. (2009). “Principles of Digital Communication Systems and Computer Networks”, Dreamtech Press.

MODULE FIVE

UNIT 4 INTERNET AND TCP/IP

1.0 **INTRODUCTION**

The '''Internet Protocol Suite''' is the set of [[communications protocol]]s used for the Internet and other similar networks. It is commonly also known as '''TCP/IP''', named from two of the most important protocols in it:

The Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were the first two networking protocols defined in this standard. Modern IP networking represents a synthesis of several developments that began to evolve in the 1960s and 1970s, namely the Internetand local area networks, which emerged during the 1980s, together with the advent of the World Wide Web in the early 1990s.

The Internet Protocol Suite consists of four abstraction layers. From the lowest to the highest layer, these are the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer.

The Link Layer contains communication technologies for the local network the host is connected to directly, the link. It provides the basic connectivity functions interacting with the networking hardware of the computer and the associated management of interface-to-interface messaging. The Internet Layerprovides communication methods between multiple links of a computer and facilitates the interconnection of networks. As such, this layer establishes the Internet. It contains primarily the Internet Protocol, which defines the fundamental addressing namespaces, IPv4Internet Protocol Version 4 (IPv4) and IPv6|Internet Protocol Version 6 (IPv6) used to identify and locate hosts on the network. Direct host-to-host communication tasks are handled in the Transport Layer, which provides a general framework to transmit data between hosts using protocols like the Transmission Control Protocol and the User Datagram.

2.0 OBJECTIVES

By the end of this unit, you should be able to:

- Describe the Internet standards process
- Define common terms used in TCP/IP
- Describe the advantages of including TCP/IP components in Windows
- Describe how the TCP/IP protocol suite maps to the Department of Defense Advanced Research Projects Agency (DARPA) and Open System Interconnection (OSI) models.

3.0 MAIN CONTENT

3.1 History

The Internet Protocol Suite resulted from research and development conducted by the Defense Advanced Research Projects Agency ([[DARPA]]) in the early 1970s. After initiating the pioneering [[ARPANET]] in 1969, DARPA started work on a number of other data transmission technologies. In 1972, [[Robert E. Kahn]] joined the DARPA [[Information Processing Technology Office]], where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. In the spring of 1973, [[Vinton Cerf]], the developer of the existing ARPANET [[Network Control Program]] (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol generation for the ARPANET.

By the summer of 1973, Kahn and Cerf had worked out a fundamental reformulation, where the differences between network protocols were hidden by using a common [[internetwork protocol]], and, instead of the network being responsible for reliability, as in the ARPANET, the hosts became responsible. Cerf credits [[Hubert Zimmerman]] and [[Louis Pouzin]], designer of the [[CYCLADES]] network, with important influences on this design.

The design of the network included the recognition that it should provide only the functions of efficiently transmitting and routing traffic between end nodes and that all other intelligence should be located at the edge of the network, in the end nodes. Using a simple design, it became possible to connect almost any network

to the ARPANET, irrespective of their local characteristics, thereby solving Kahn's initial problem. One popular expression is that TCP/IP, the eventual product of Cerf and Kahn's work, will run over ""two tin cans and a string.""
A computer, called a [[router]], is provided with an interface to each network. It forwards [[packet (information technology)|packets]] back and forth between them.<ref>RFC 1812, "Requirements for IP Version 4 Routers", F. Baker (June 1995)</ref> Originally a router was called "gateway", but the term was changed to avoid confusion with other types of [[Gateway (computer networking)|gateways]].

The idea was worked out in more detailed form by Cerf's networking research group at Stanford in the 1973–74 period, resulting in the first TCP specification

The Internet Protocol Suite resulted from research and development conducted by the Defense Advanced Research Projects Agency ([[DARPA]]) in the early 1970s. After initiating the pioneering [[ARPANET]] in 1969, DARPA started work on a number of other data transmission technologies. In 1972, [[Robert E. Kahn]] joined the DARPA [[Information Processing Technology Office]], where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. In the spring of 1973, [[Vinton Cerf]], the developer of the existing ARPANET [[Network Control Program]] (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next proto

3.2 The Internet Standards Process

The TCP/IP is the protocol of the Internet, it has evolved based on fundamental standards thathave been created and adopted over more than 30 years. The future of TCP/IP is closely associatedwith the advances and administration of the Internet as additional standards continue to be developed.
Although no one organization owns the Internet or its technologies, several organizations oversee and manage these new standards, such as the Internet Society and the Internet Architecture Board.
The Internet Society (ISOC) was created in 1992 and is a global organization responsible for theinternetworking technologies and applications of the Internet. Although the society's principal purpose isto encourage the development and availability of the Internet, it is also responsible for the furtherdevelopment of the standards and protocols that allow the Internet to function.The ISOC sponsors the Internet Architecture Board (IAB), a technical advisory group that sets Internetstandards, publishes RFCs, and oversees the Internet standards process. The IAB governs thefollowing bodies:

- The Internet Assigned Number Authority (IANA) oversees and coordinates the assignment of protocolidentifiers used on the Internet.
- The Internet Research Task Force (IRTF) coordinates all TCP/IP-related research projects.

- The Internet Engineering Task Force (IETF) solves technical problems and needs as they arise on theInternet and develops Internet standards and protocols. IETF working groups define standards knownas RFC

3.3 TCP/IP Terminology

The Internet standards use a specific set of terms when referring to network elements and conceptsrelated to TCP/IP networking.Common terms and concepts in TCP/IP are defined as follows:

- **Node:** Any device, including routers and hosts, which runs an implementation of IP.
- **Router:** A node that can forward IP packets not explicitly addressed to itself. On an IPv6 network, a

  Router also typically advertises its presence and host configuration information.
- **Host:** A node that cannot forward IP packets not explicitly addressed to itself (a non-router). A host istypically the source and the destination of IP traffic. A host silently discards traffic that it receives butthat is not explicitly addressed to itself.
- **Upper-layer protocol :**A protocol above IP that uses IP as its transport. Examples include Internet layer protocols such as the Internet Control Message Protocol (ICMP) and Transport layer protocolssuch as the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). (However, Application layer protocols that use TCP and UDP as their transports are not considered upper-layerprotocols. File Transfer Protocol [FTP] and Domain Name System [DNS] fall into this category). Fordetails of the layers of the TCP/IP protocol suite, "Architectural Overview of the TCP/IPProtocol Suite."
- **LAN segment :**A portion of a subnet consisting of a single medium that is bounded by bridges or Layer2 switches.
- **Subnet:** One or more LAN segments that are bounded by routers and use the same IP address prefix.Other terms for subnet are network segment and link.
- **Network:** Two or more subnets connected by routers. Another term for network is internetwork.
- **Neighbor:** A node connected to the same subnet as another node.
- **Interface :**The representation of a physical or logical attachment of a node to a subnet. An example of a physical interface is a network adapter. An example of a logical interface is a tunnel interface that isused to send IPv6 packets across an IPv4 network.
- **Address:** An identifier that can be used as the source or destination of IP packets and that is assignedat the Internet layer to an interface or set of interfaces.
- **Packet :**The protocol data unit (PDU) that exists at the Internet layer and comprises an IP head payload.a common [[internetwork protocol]], and, instead of the network being responsible for reliability, as in the ARPANET, the hosts became responsible. Cerf credits [[Hubert Zimmerman]] and [[Louis Pouzin]], designer of the [[CYCLADES]] network, with important influences on this design.

Table 4-1: Lists the advantages of the TCP/IP protocol suite and the inclusion of TCP/IP components in Windows.

Advantages of the TCP/IP protocol suite	Advantages of TCP/IP components in Windows
A standard, routable enterprise networking protocol that is the most complete and accepted protocol available. All modern operating systems support TCP/IP, and most large private networks rely on TCP/IP for much of their traffic.	TCP/IP components in Windows enable enterprise networking and connectivity for Windows and non-Windows–based computers.
A technology for connecting dissimilar systems. Many TCP/IP application protocols were designed to access and transfer data between dissimilar systems. These protocols include HTTP, FTP, and Telnet.	TCP/IP components in Windows allow standards-based connectivity to other operating system platforms.
A robust, scaleable, cross-platform client/server framework.	TCP/IP components in Windows support the Windows Sockets application programming interface, which developers use to create client/server applications.
A method of gaining access to the Internet.	Windows-based computers are Internet-ready.

3.4 The TCP/IP Protocol Suite

The TCP/IP protocol suite maps to a four-layer conceptual model known as the DARPA model, whichwas named after the U.S. government agency that initially developed TCP/IP. The four layers of theDARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPAmodel corresponds to one or more layers of the seven-layer OSI model.

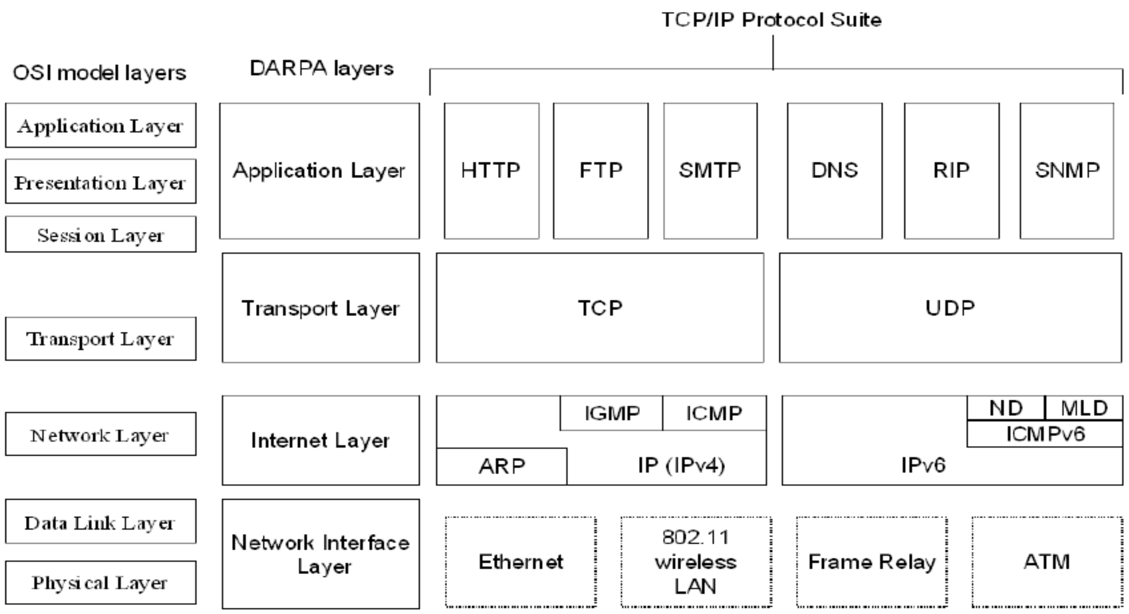


Fig 4-1: The Architecture of the TCP/IP model

A The TCP/IP protocol suite has two sets of protocols at the Internet layer:

- IPv4, also known as IP, is the Internet layer in common use today on private intranets and the Internet
- IPv6 is the new Internet layer that will eventually replace the existing IPv4 Internet layer.

3.5 Network Interface Layer

The Network Interface layer (also called the Network Access layer) sends TCP/IP packets on thenetwork medium and receives TCP/IP packets off the network medium. TCP/IP was designed to beindependent of the network access method, frame format, and medium. Therefore, you can use TCP/IPto communicate across differing network types that use LAN technologies—such as Ethernet and802.11 wireless LAN—and WAN technologies—such as Frame Relay and Asynchronous TransferMode (ATM). By being independent of any specific network technology, TCP/IP can be adapted to newtechnologies.The Network Interface layer of the DARPA model encompasses the Data Link and Physical layers ofthe OSI model. The Internet layer of the DARPA model does not take advantage of sequencing and acknowledgment services that might be present in the Data Link layer of the OSI model. The Internetlayer assumes an unreliable Network Interface layer and that reliable communications through sessionestablishment and the sequencing and acknowledgment of packets is the responsibility of either theTransport layer or the Application layer.

3.6 Internet Layer

The Internet layer responsibilities include addressing, packaging, and routing functions. The Internetlayer is analogous to the Network layer of the OSI model.The core protocols for the IPv4 Internet layer consist of the following:

- The Address Resolution Protocol (ARP) resolves the Internet layer address to a Network Interface layeraddress such as a hardware address.
- The Internet Protocol (IP) is a routable protocol that addresses, routes, fragments, and reassemblespackets.
- The Internet Control Message Protocol (ICMP) reports errors and other information to help youdiagnose unsuccessful packet delivery.

3.7 Application Layer

The Application layer allows applications to access the services of the other layers, and it defines theprotocols that applications use to exchange data. The Application layer contains many protocols, andmore are always being developed.

The most widely known Application layer protocols help users exchange information:

- The Hypertext Transfer Protocol (HTTP) transfers files that make up pages on the World Wide Web.
- The File Transfer Protocol (FTP) transfers individual files, typically for an interactive user session.
- The Simple Mail Transfer Protocol (SMTP) transfers mail messages and attachments.

Additionally, the following Application layer protocols help you use and manage TCP/IP networks:

- The Domain Name System (DNS) protocol resolves a host name, such as www.microsoft.com, to an IPaddress and copies name information between DNS servers.
- The Routing Information Protocol (RIP) is a protocol that routers use to exchange routing information on an IP network., called a router, is provided with an interface to each network.

4.0 Conclusion

In this unit you have been introduced to the fundamental concepts of internet TCP/IP. You also learnt the internet standard process and some TCP/IP terminologies. You were also introduced to Various TCP/IP protocol suites.

5.0 Summary

In the unit you have learnt:

- The Internet standards process
- Definition of common terms used in TCP/IP
- The advantages of including TCP/IP components in Windows
- How the TCP/IP protocol suite maps to the Department of Defense Advanced Research Projects Agency (DARPA) and Open System Interconnection (OSI) models.

6.0 Tutor Marked Assignment

- Discuss the history of the TCP/IP model
- What is the function of the Internet and the Application Layer

7.0 Further Readings

"About Rand". *Paul Baran and the Origins of the Internet*. http://www.rand.org/about/history/baran.html. Retrieved January 14, 2006.

http://tldp.org/HOWTO/Unix-and-Internet-Fundamentals-HOWTO/internet.html. Retrieved June 15, 2009.

Johna Till Johnson. "Net was born of economic necessity, not fear". http://www.networkworld.com/columnists/2004/0607johnson.html. Retrieved June 15, 2009.URL is sufficient attribution