NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF SCIENCE AND TECHNOLOGY

COURSE CODE: CIT 722

COURSE TITLE: COMPUTER NETWORKS

Introduction

Computer Networks is a second semester course. It is a three units degree course available to all students offering Bachelor of Science (B.Sc) Computer Technology (CTT).

A computer network is simply two or more computers connected together so they can exchange information. A small network can be as simple as two computers linked together by a single cable. This course introduces you to the hardware and software needed for a network, and explains how a small network is different from larger networks and the Internet. Most networks use hubs to connect computers together. A large network may connect thousands of computers and other devices together. A wireless network connects computers without a hub or network cables but use radio communications to send data between each other. Networking allows you to share resources among a group of computer users. If you have a printer connected to your computer, you can share the printer with other computers on the network. Then instead of buying a printer for every computer, all the computers can print across the network to the printer. If you already have access to the Internet from one computer on your network, you can share that Internet connection with other computers on the network. Then all the computers on your network can browse the Web at the same time, using this single Internet connection.

What You Will Learn in this Course

This course is made up of modules, units and a course guide. This course guide tells you briefly what the course is all about. It tells you about the course materials you will be using and how you can work with it. In addition, it gives some general guidelines for the amount of time you are likely to spend on each unit of the course in order to complete this course successfully. You have quite a number of tutor-marked assignment meant to test your in-depth understanding of the course. There will be regular tutorial classes that are related to this course. You are advised to attend tutorial classes. The course will prepare you for the challenges you will meet in the field of computer networks.

Course Aims

The aim of this course is to provide you with an understanding of Computer Networks. Additionally, it also aims at letting you know the benefits of computer network and the requirements for setting up Computer Networks.

Course Objectives

To achieve the aims set out, the course has a set of objectives. Each unit has specific objectives which are presented at the beginning of the unit. You are expected to read these objectives before you study the unit. You may wish to refer to them during your study to check on your progress. You should always look at the unit objectives after completion of each unit. By so doing, you would have followed the instructions in the unit.

Below are the comprehensive objectives of the course as a whole. By meeting these objectives, you should have achieved the aims of the course as a whole. In addition to the aims above, this course sets to achieve some objectives. Thus, after going through the course, you should be able to:

- Define the basic terminology of computer networks
- Recognize the individual components of the big picture of computer networks
- Outline the basic network configurations
- Cite the reasons for using a network model and how those reasons apply to current network systems
- List the layers of the OSI model and describe the duties of each layer
- List the layers of the TCP/IP model and describe the duties of each layer
- Compare the OSI and TCP/IP models and list their differences and similarities
- Understand the transmission methods underlying Ethernet, Token Ring, FDDI, and *ATM networks
- Addressing Techniques

Working through this Course

To complete this course you are required to read each study unit, read the reading materials specified at the end of each unit in conjunction with the ones which may be provided by the National Open University of Nigeria.

Each unit contains self-assessment exercises and at certain points in the course you would be required to submit assignments for assessment purposes. At the end of the course there will be a final examination. The course should take you about a total of 21 weeks to complete. All the components of the course are listed below so as to assist you in allocating your time to each unit in order to complete the course on time and successfully.

You are required to spend a lot of time in reading and to attend tutorial sessions for you to have opportunity of interacting with other people offering this course.

The Course Materials

The main components of this course are:

1. The course guide
2. Study units
3. References/Further Readings
4. Assignments

Study Unit

The study units in this course are as follows:

Module 1 Introduction

Unit 1 History of Network
Unit 2 Introduction to Computer Network
Unit 3 Networking hardware
Unit 4 Network operating system

Module 2 Introduction

Unit 1 Computer topologies
Unit 2 Network protocols
Unit 3 Network configuration

Module 3 Introduction

Unit 1 Open Systems Interconnection Reference Model (OSI Model)
Unit 2 Interaction between OSI Model Layers Protocols
Unit 3 TCP/IP Model

Module 4 Introduction

Unit 1 Types of Network- LAN, WAN and MAN
Unit 2 Metropolitan Area Network and Wide Area Network
Unit 3 Transmission Media
Unit 4 Basic Addressing
Unit 5 Basic network troubleshooting

The first unit of module 1 covers the very basics of networking history. We'll start with a little history that describes how the networking industry evolved. It describes the developments in communication, explaining problems in communication and their solutions and describes how networks do grow. Unit 2 defines computer network and discusses the concept of networking, outlining the basic network application areas and explains key issues to computer network. Unit 3 explain the individual components of the big picture of computer networks and outline the basic network configurations. Unit 4 Explain network operating system. It describes the functions of network operating system and gives the difference between peer-to-peer network operating system and client-server network operating system.

Unit 1 of module 2 describes network topology concept and explain the geometric representation of computer network. It explains the merits and demerits of various network topologies and discusses how to choose the right topology. Unit 2 explains network protocols and how to analyze networking requirements while unit 3 is about network configuration.

The first unit of module 3 gives detail explanation of the seven layers of Open System Interconnection reference model. It describes the functions of each of the models. Unit 2 describes the interaction between OSI model layers protocols. It explains communications among the OSI layers and discusses the benefits of the OSI model. Unit 3 describes the workings of TCP/IP model and explain the functions of the four layers of TCP/IP model. It distinguishes between the OSI model and TCP/IP model.

The first unit of module 4 discusses the concept of local area network and the major characteristics of LANs. It describes various components of LANs and explains LAN topologies. Unit 2 explains the concepts of metropolitan area network (MAN) and wide area network (WAN) . It discusses the major characteristics of MAN and WAN.

Unit 3 covers various transmission media available for transferring information, the characteristics and the ways to carry data during its transmission are also included. Unit 4 explains the basics of a network addressing and the standard networking addresses. It describes the variations on standard networking addresses and the role of address in a network. Unit 5 explains basic network troubleshooting.

Presentation Schedule

Your course materials have important dates for the early and timely completion and submission of your TMAs and attending tutorials. You should remember that you are required to submit all your assignments by the stipulated time and date. You should guard against falling behind in your work.

Assessment

There are three aspects to the self-assessment of the course. The first self-assessment is made up of exercises, second consists of the tutor-marked assignments and third is the written examination/end of course examination.

You are advised to do the exercises. In tackling the assignments, you are expected to apply information, knowledge and techniques you gathered during the course. You are to submit the assignments to your facilitators for formal assessment in accordance with the deadlines stated in the presentation schedule and the assignment file. The work you submit to your tutor for assessment will count for 30% of your total course work. At the end of the course you will need to sit for a final or end of course examination of about three hours duration. This examination will count for 70% of your total course mark.

Tutor-Marked Assignment

The TMA is a continuous assessment component of your course. It accounts for 30% of the total score. You will be given four (4) TMAs to answer. Three of these must be answered before you are allowed to sit for the end of course examination. The TMAs would be given to you by your facilitator and returned after you have done the assignment. Assignment questions are given at the end of each unit in this course. You will be able to complete your assignment from the information and material contained in your reading, references and study units. However, it is desirable in all degree level of education to demonstrate that you have read and researched more into your references, which will give you a wider view point and may provide you with a deeper understanding of the subject.

Make sure that each assignment reaches your facilitator on or before the deadline given in the presentation schedule and assignment file. If for any reason you cannot complete your work on time, contact your facilitator before the assignment is due to discuss the possibility of an extension. Extension will not be granted after the due date unless there are exceptional circumstances.

Final Examination and Grading

The end of course examination for Computer Networks will be for about 3 hours and it has a value of 70% of the total course work. The examination will consist of questions, which will reflect the type of self-testing, practice exercise and tutor-marked assignment problems you have previously encountered. All areas of the course will be assessed.

Use the time between finishing the last unit and sitting for the examination to revise the whole course. You might find it useful to review your self-test, TMAs and comments on them before the examination. The end of course examination covers information from all parts of the course.

Course Marking Scheme

Assignment	**Marks**
Assignment 1 – 4	Four assignments, best three marks of the four count at 10% each – 30% of course marks.
End of course examination	70% of overall course marks
Total	100% of course materials

Facilitators/Tutors and Tutorials

There are 16 hours of tutorials provided in support of this course. You will be notified of the dates, times and location of these tutorials as well as the name and phone number of your facilitator, as soon as you are allocated a tutorial group.

Your facilitator will mark and comment on your assignments, keep a close watch on your progress and any difficulties you might face and provide assistance to you during the course. You are expected to mail your Tutor Marked Assignment to your facilitator before the schedule 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 delay to contact your facilitator by telephone or e-mail if you need assistance.

The following might be circumstances in which you would find assistance necessary, hence you would have to contact your facilitator if:

- You do not understand any part of the study or the assigned readings.
- You have difficulty with the self-tests
- You have a question or problem with an assignment or with the grading of an assignment.

You should endeavor to attend the tutorials. This is the only chance to have face contact with your course facilitator and to ask questions which are answered instantly. You can raise any problem encountered in the course of your study.

To gain much benefit from course tutorials prepare a question list before attending them. You will learn a lot from participating actively in discussions.

Summary

Computer network is a course that intends to provide the basic concepts of how computers can be networked together so as to enhance sharing of resources. A computer network is simply two or more computers connected together so they can exchange information. A small network can be as simple as two computers linked together by a single cable. To network computers together, you need to install networking hardware and software. Every network includes these three components: (1) The computers that are connected together. Computers and similar devices are called *nodes* when connected to a network. (2) The networking hardware that connects the computers together, including hardware installed in your computer, network cables, and devices that connect all the cables together. (3) Networking software that runs on each computer and enables it to communicate with other computers on the network.

Here is the networking hardware you need to set up a small network:

- **Network adapter cards:** expansion cards that provide the physical connection between each computer and the network. The card installs into a slot on your computer, just like a sound card or modem card. Some newer computers have a network adapter already built into the system. Laptop computers often use a card that slides into a PC card slot.

- **Network hub:** the central connection point for network cables that connect to computers or other devices on a network. The hub has several network cable jacks or *ports* that you use to connect network cables to computers. The hub contains circuitry that enables each computer to communicate with any other computer connected to the hub.
- **Network cables:** special, unshielded twisted-pair (UTP) cables used to connect each computer to the hub.

You may want to network computers where it is expensive or difficult to run network cables, for example, between two rooms or two buildings. However, recent advances in wireless networking technology make wireless networking practical and affordable. New wireless standards have facilitated the development of wireless products with good performance and the ability to integrate easily into a wired Ethernet network. The Ethernet standard for wireless networking is the IEEE 802.11b wireless standard.

In addition, you will be able to answer the following type of questions:

1. Discuss the history of networking.
2. What are the problems faced with the early communication.
3. What is meant by computer network?
4. Enumerate the concept of networking
5. Explain the basic network application areas
6. What are the key issues of computer network
7. What are the major components of networking hardware?
8. Briefly discuss the following hardware components:

- File Servers
- Workstations
- Network Interface Cards
- Switches
- Repeaters
- Bridges
- Routers

9. What is Network Operating System?
10. What are the functions of network operating system
11. Differentiate between peer-to-peer network operating system and client-server network operating system.
12. In networking, what does the term *topology* refer to?
13. Describe the geometric representations of computer network
14. Explain the merits and demerits of various network topologies
15. What are the considerations for choosing the right topology?
16. Define Protocol.
17. Explain in brief the key elements of a protocol.
18. Compare and contrast the functions of Carrier Sense on Multi-Access Networks (CSMA) and Carrier Sense Multiple Access with Collision Detect (CSMA/CD).
19. Discuss the main characteristics of OSI reference model
20. Describe the interaction between OSI model layers protocols
21. Explain communications among the OSI layers
22. Discuss the benefits of the OSI model
23. Explain the interaction among the various layers of the OSI mode

24. Distinguish between the OSI model and TCP/IP model.

25. What are the functions of the four layers of TCP/IP model.

26. Describe what a Local Area Network is.

27. Describe the different types of LANs.
28. Describe some of the key components of a network system.
29. **in this course.**
32. Enumerate on the functions of various addressing techniques.

However, the list of questions that you can answer is not limited to the above list. To gain the most from this course you should endeavor to apply the principles you have learnt to your understanding of computer network.

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

NATIONAL OPEN UNIVERSITY OF NIGERIA

COURSE MATERIAL

Course Code	CIT 722
Course Title:	Computer Networks

Page

MODULE 1: BASIC NETWORKING CONCEPTS

Unit 1: History of Networks

1.0 **Introduction** **2**

2.0 **Objectives** **2**

3.0 **Networking History** **2**

3.1 **Developments in Communication** **3**

3.2 **How networks are growing** **6**

4.0 **Conclusion** **7**

5.0 **Summary** **7**

6.0 **Tutor Marked Assignment** **7**

7.0 **Further Reading and Other Resources** **7**

1.0 INTRODUCTION

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

2.0 OBJECTIVES

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

- Understand the history of networking
- Describe the developments in communication
- Explain the problems in communication and their solutions
- Understand how networks do grow

3.0 NETWORKING HISTORY

Early networks

From a historical perspective, electronic communication has actually been around a long time, beginning with Samuel Morse and the telegraph. He sent the first telegraph message May 24, 1844 from Washington DC to Baltimore MD, 37 miles away. The message? "What hath God wrought."

Less than 25 years later, Alexander Graham Bell invented the telephone – beating out a competitor to the patent office only by a couple of hours on Valentine's Day in 1867. This led to the development of the ultimate analog network – the telephone system.

The first bit-oriented language device was developed by Emile Baudot – the printing telegraph. By bit-oriented we mean the device sent pulses of electricity which were either positive or had no voltage at all. These machines did not use Morse code. Baudot's five-level code sent five pulses down the wire for each character transmitted. The machines did the encoding and decoding, eliminating the need for operators at both ends of the wires. For the first time, electronic messages could be sent by anyone.

Telephone Network

But it's really the telephone network that has had the greatest impact on how businesses communicate and connect today. Until 1985, the Bell Telephone Company, now known as AT&T, owned the telephone network from end to end. It represented a phenomenal network, the largest then and still the largest today.

Let’s take a look at some additional developments in the communications industry that had a direct impact on the networking industry today.

3.1 Developments in Communication

In 1966, an individual named “Carter” invented a special device that attached to a telephone receiver that would allow construction workers to talk over the telephone from a two-way radio.

Bell telephone had a problem with this and sued – and eventually lost. As a result, in 1975, the Federal Communications Commission ruled that devices could attach to the phone system, if they met certain specifications. Those specifications were approved in 1977 and became known as FCC Part 68. In fact, years ago you could look at the underside of a telephone not manufactured by Bell, and see the “Part 68” stamp of approval.

This ruling eventually led to the breakup of American Telephone and Telegraph in 1984, thus creating nine regional Bell operating companies like Pacific Bell, Bell Atlantic, Bell South, Mountain Bell, etc. The break up of AT&T in 1984 opened the door for other competitors in the telecommunications market. Companies like Microwave Communications, Inc. (MCI), and Sprint. Today, when you make a phone call across the country, it may go through three or four different carrier networks in order to make the connection.

1960's - 1970's Communication

In the 1960’s and 1970’s, traditional computer communications centered around the mainframe host. The mainframe contained all the applications needed by the users, as well as file management, and even printing. This centralized comput ing environment used low-speed access lines that tied terminals to the host. These large mainframes used digital signals – pulses of electricity or zeros and ones, what is called binary -- to pass information from the terminals to the host. The information processing in the host was also all digital.

Problems faced in communication

This brought about a problem. The telephone industry wanted to use computers to switch calls faster and the computer industry wanted to connect remote users to the mainframe using the telephone service. But the telephone networks speak analog and computers speak digital. Let’s take a closer look at this problem. Digital signals are seen as one’s and zero’s. The signal is either on or off. Whereas analog signals are like audio tones – for example, the high-pitched squeal you hear when you accidentally call a fax machine.

So, in order for the computer world to use the services of the telephone system, a conversion of the signal had to occur.

The solut ion – a modulator/demodulator or "modem." The modem takes the digital signals from the computer and modulates the signal into analog format. In sending information from a desktop computer to a host using POTS or plain old telephone service, the modem takes the digital signals from the computer and modulates the signal into analog format to go through the telephone system. From the telephone system, the analog signal goes through another modem which converts the signal to digital format to be processed by the host computer. This helped solve some of the distance problems, at least to a certain extent.

Multiplexing or muxing

Another problem is how to connect multiple terminals to a single cable. The technology solution is multiplexing or muxing. What we can do with multiplexing is we can take multiple remote terminals, connect them back to our single central site, our single mainframe at the central site, but we can do it all over a single communications channel, a single line. So what you see is we have some new terminology here in our diagram. Our single central site we refer to as a broadband connection. That's referred to as a broadband connection because whenever we talk about broadband we're talking about carrying multiple communications channels over a single communication pipe. So what we're saying here is we have multiple communication channels as in four terminals at the remote site going back to a single central site over one common channel. But again in the case of our definition of broadband here, we're referring to the fact that we have four communication channels, one for each remote terminal over a single physical path. Now out at the end stations at the terminals, you see we have the term Baseband and what we mean by the term Baseband is, in our example, between the terminal and the multiplexer we have a single communication channel per wire, so each of those wires leading into the multiplexer has a dedicated channel or a dedicated path. Now the function of the multiplexer is to take each of those Baseband paths and break it up and allocate time slots. What that allows us to do is allocate a time slot per terminal so each terminal has its own time slot across that common Baseband connection between the remote terminals and the central mainframe site. That is the function of the multiplexer is to allocate the time slots and then also on the other side to put the pieces back together for delivery to the mainframe.

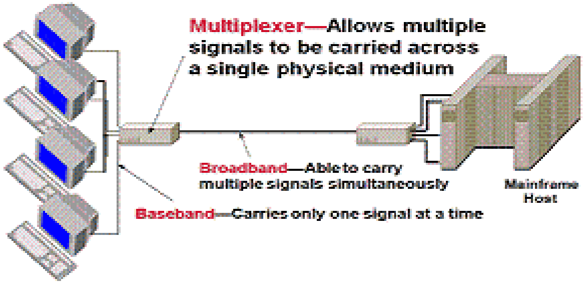

Multiplexer—Allows multiple signals to be carried across a single physical medium
Broadband—Able to carry multiple signals simultaneously
Mainframe Host
Baseband—Carries only one signal at a time

Fig. 1.1.1 Multiplexing

Source: http://www.infinitygroup.com/images/internetworking.gif

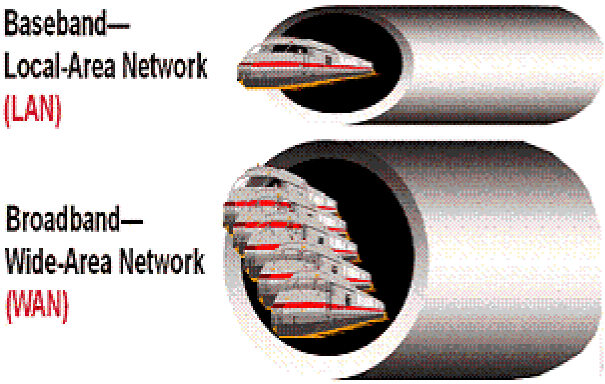


Fig. 1.1.2 Baseband and broadband

Source: http://www.infinitygroup.com/images/internetworking.gif

Baseband had a single communications channel per physical path. An example of some Baseband technology you're probably familiar with is Ethernet for example. Most implementations of Ethernet use Baseband technology. We have a single communications channel going over a single physical path or a single physical cable. On the other hand on the bottom part of our diagram you see a reference to broadband and the analogy here would be multiple trains inside of a single tunnel. Maybe we see that in the real world, we're probably familiar with broadband as something we do every day, is cable TV. With cable TV we have multiple channels coming in over a single cable. We plug a single cable into the back of our TV and over that single cable certainly we know we can get 12 or 20 or 40 or 60 or more channels over that single cable. So cable TV is a good example of broadband.

3.2 How networks are growing

With all the technologies available, companies were able to team up with the phone company and tie branch offices to the headquarters. The speeds of data transfer were often slow and were still dependent on the speed and capacity of the host computers at the headquarters site. The phone company was also able to offer leased line and dial-up options. With leased-lines, companies paid for a continuous connection to the host computer. Companies using dial-up connections paid only for time used. Dial-up connections were perfect for the small office or branch.

Birth of the personal computer

The birth of the personal computer in 1981 really fueled the explosion of the networking marketplace. No longer were people dependent on a mainframe for applications, file storage, processing, or printing. The PC gave users incredible freedom and power.

The Internet 1970's - 1980's

The 70's and 80's saw the beginnings of the Internet. The Internet as we know it today began as the ARPANET — The Advanced Research Projects Agency Network – built by a division of the Department of Defense essentially in the mid '60's through grant-funded research by universities and companies. The first actual packet-switched network was built by BBN. It was used by universities and the federal government to exchange information and research. Many local area networks connected to the ARPANET with TCP/IP. TCP/IP was developed in 1974 and stands for Transmission Control Protocol / Internet Protocol. The ARPANET was shut down in 1990 due to newer network technology and the need for greater bandwidth on the backbone. In the late '70's the NSFNET, the National Science Foundation Network was developed. This network relied on super computers in San Diego; Boulder; Champaign; Pittsburgh; Ithaca; and Princeton. Each of these six super computers had a microcomputer tied to it which spoke TCP/IP. The microcomputer really handled all of the access to the backbone of the Internet. Essentially this network was overloaded from the word "go".

Further developments in networking lead to the design of the ANSNET -- Advanced Networks and Services Network. ANSNET was a joint effort by MCI, Merit and IBM specifically for commercial purposes. This large network was sold to AOL in 1995. The National Science Foundation then awarded contracts to four major network access providers: Pacific Bell in San Francisco, Ameritech in Chicago, MFS in Washington DC and Sprint in New York City. By the mid '80's the collection of networks began to be known as the "Internet" in university circles. TCP/IP remains the glue that holds it together. In January 1992 the Internet Society was formed – a misleading name since the Internet is really a place of anarchy. It is controlled by those who have the fastest lines and can give customers the greatest service today. The primary Internet-related applications used today include: Email, News retrieval, Remote Login, File Transfer and World Wide Web access and development.

1990's Global Internetworking

With the growth and development of the Internet came the need for speed – and bandwidth. Companies want to take advantage of the ability to move information around the world quickly. This information comes in the form of voice, data and video – large files which increase the demands on the network. In the future, global internetworking will provide an environment for emerging applications that will require even greater amounts of bandwidth.

4.0 CONCLUSION

In this unit, we get a brief overview of the history of networking. The Unit describes how the networking industry evolved and it familiarizes you with much of the networking vocabularies.

5.0 SUMMARY

In this unit we have learnt about:

- the history of networking
- the developments in communication
- the problems in communications and their solutions
- how networks are growing

6.0 TUTOR MARKED ASSIGNMENT

1. Discuss the history of networking.
2. What are the problems faced with the early communication.
3. Explain the following terms:
   (i) Multiplexing (ii) Baseband (iii) Broadband

7.0 FURTHER READINGS

1. Computer Networks by A.S. Tanenbaum, 2003[2],
2. Computer Networks by P.J. Irving, 2003[3],
3. Ed, T. Theory and Problems of Computer Networking. USA: Schaum's Outline Series, McGRAW-HILL, 2002.

MODULE 1: BASIC NETWORKING CONCEPTS

Unit 2: Introduction to computer network

		Page
1.0	**Introduction**	**9**
2.0	**Objectives**	**9**
3.0	**Definition of computer network**	**9**
3.1	**Networking concept**	**9**
3.2	**Benefits of computer network**	**10**
3.3	**Network application areas**	**11**
3.4	**Key issues to computer network**	**12**
4.0	**Conclusion**	**13**
5.0	**Summary**	**13**
6.0	**Tutor Marked Assignment**	**13**
7.0	**Further Reading and Other Resources**	**13**

1.0 INTRODUCTION

In the world of computers, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- Define computer network
- Recognize the concept of networking
- Outline the basic network application areas
- Understand key issues for computer network

3.0 DEFINITION OF COMPUTER NETWORK

A computer network may be defined as the coordination or interconnection of a number of individual computers. A computer network is basically established by the network layer in the Open Systems Infrastructure model, popularly known as the OSI model. Computer networks exist on various scales, from links between machines in the same room up through wiring connecting the machines in a building or campus to regional, national and global networks. Various media are used to carry the communications signals: copper wire, fibre-optic cables and wireless or radio transmissions etc.

3.1 NETWORKING CONCEPT

Networking is the concept of sharing resources and services. A network of computers is a group of interconnected systems sharing resources and interacting using a shared communications link. A network, therefore, is a set of interconnected systems with something to share. The shared resource can be data, a printer, a fax modem, or a service such as a database or an email system. The individual systems must be connected through a pathway (called the transmission medium) that is used to transmit the resource or service between the computers. All systems on the pathway must follow a set of common communication rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules governing computer communication are called protocols. In summary, all networks must have the following:

1. A resource to share (resource)
2. A pathway to transfer data (transmission medium)
3. A set of rules governing how to communicate (protocols)

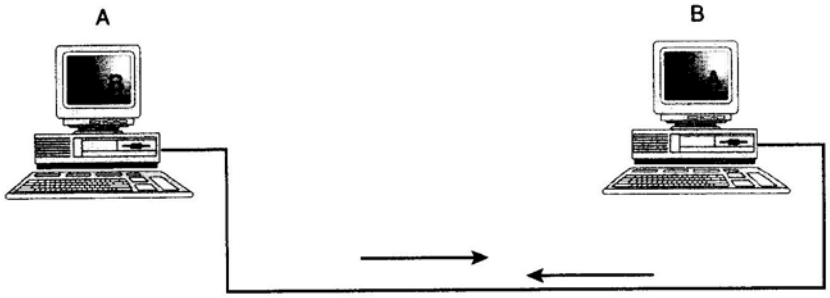


Fig. 1.2.1 Simplest form of a computer network

Source: **http://fcit.usf.edu/Network/glossary.html**

Having a transmission pathway does not always guarantee communication. When two entities communicate, they do not merely exchange information; rather, they must understand the information they receive from each other. The goal of computer networking, therefore, is not simply to exchange data but to understand and use data received from other entities on the network. An analogy is people speaking, just because two people can speak, it does not mean they automatically can understand each other. These two people might speak different languages or interpret words differently. One person might use sign language, while the other uses spoken language. As in human communication, even though you have two entities who "speak," there is no guarantee they will be able to understand each other. Just because two computers are sharing resources, it does not necessarily mean they can communicate. Because computers can be used in different ways and can be located at different distances from each other, enabling computers to communicate often can be a daunting task that draws on a wide variety of technologies.

3.2 BENEFITS OF COMPUTER NETWORK

Assuming you have six people in your family. Each has their own computer and wants to be able to print and have internet access. you don't want to pay for six modems (for internet connections) and six printers. Why not have one internet connection and one printer connected to one computer. This computer has all other computers attached to it. They all share its internet and printer. They can also each have some shared folders that everyone on the network can access (upon providing a password). Properly planned, an efficient network brings a wide range of benefits to a company such as:

File Sharing: Networks offer a quick and easy way to share files directly. Instead of using a disk or USB key to carry files from one computer or office to another, you can share files directly using a network.

Security: Specific directories can be password protected to limit access to authorized users. Also, files and programs on a network can be designated as "copy inhibit" so you don’t have to worry about the illegal copying of programs.

Resource Sharing: All computers in the network can share resources such as printers, fax machines, modems, and scanners.

Communication: Even outside of the internet, those on the network can communicate with each other via electronic mail over the network system. When connected to the internet, network users can communicate with people around the world via the network.

Flexible Access: Networks allow their users to access files from computers throughout the network. This means that a user can begin work on a project on one computer and finish up on another. Multiple users can also collaborate on the same project through the network.

Workgroup Computing: Workgroup software like Microsoft BackOffice enables many users to contribute to a document concurrently. This allows for interactive teamwork.

Error reduction and improve consistency: One can reduce errors and improve consistency by having all staff work from a single source of information, so that standard versions of manuals and directories can be made available, and data can be backed up from a single point on a scheduled basis, ensuring consistency.

3.3 NETWORK APPLICATION AREAS

There is a long list of application areas, which can be benefited by establishing Computer Networks. Few of the potential applications of Computer Networks are:

1. Information retrieval systems which search for books, technical reports, papers and articles on particular topics
2. News access machines, which can search past news, stories or abstracts with given search criteria.
3. Airline reservation, hotel booking, railway-reservation, car-rental, etc.
4. A writer's aid: a dictionary, thesaurus, phrase generator, indexed dictionary of quotations, and encyclopedia.
5. Stock market information systems which allow searches for stocks that meet certain criteria, performance comparisons, moving averages, and various forecasting techniques.
6. Electronic Financial Transactions (EFT) between banks and via cheque clearing house.
7. Games of the type that grow or change with various enthusiasts adding to the complexity or diversity.
8. Electronic Mail Messages Systems (EMMS).
9. Corporate information systems such as marketing information system, customer information system, product information system, personnel information system, etc.
10. Corporate systems of different systems such as Order-Entry System, Centralized Purchasing, Distributed Inventory Control, etc.
11. On-line systems for Investment Advice and Management, Tax Minimization, etc.
12. Resources of interest to a home user.
13. Sports results.

14. Theatre, movies, and community events information.
15. Shopping information, prices, and advertisements.
16. Restaurants; good food guide.
17. Household magazine, recipes, book reviews, film reviews.
18. Holidays, hotels, travel booking.
19. Radio and TV programmes.
20. Medical assistance service.
21. Insurance information.
22. Computer Assisted Instruction (CAI).
23. School homework, quizzes, tests.
24. Message sending service.
25. Directories.
26. Consumer reports.
27. Employment directories and Job opportunities.
28. Tax information and Tax assistance.
29. Journey planning assistance viz. Train, bus, plane etc.
30. Catalogue of Open University and Virtual University courses.

3.4 KEY ISSUES TO COMPUTER NETWORK

The following are the major key issues to be trashed out very carefully before we go for a computer network:

1. *Nature of Nodes* -Whether participating nodes are homogeneous or heterogeneous in nature?
2. *Topology* - Which of the computer topology has to be followed? Computer topology accounts for the physical arrangement of participating computers in the network.
3. *Interconnection Type* - Whether interconnection type is point-to-point, multi-point, or broadcast type.
4. *Reliability* - How reliable our network is? Reliability aspect includes error rate, redundancy and recovery procedures.
5. *Channel Capacity Allocation* - Whether allocation of channel capacity is time-division or frequency division?
6. *Routing Techniques* - Whether message between nodes are to be routed through: Deterministic, Stochastic, and Distributed routing techniques?
7. *Models* - Which of the models i.e. analytical models, queuing models, simulation models, measurement and validation models are applicable?
8. *Channel Capacity* - What are the channel capacities of the communication lines connecting nodes?
9. *Access* - Whether computer access in the network is direct-access or through a sub-network?
10. *Protocols* - What levels, standards and formats are to be followed while establishing communication between participating nodes?
11. *Performance* - How is higher performance of computer network achieved? Response time, time to connect, resource utilization, etc. contribute towards performance of computer network.

12. *Control* - Whether centralized control, distributed control or hierarchical control of participating nodes of computer network is suitable?

4.0 CONCLUSION

In this unit we define computer network to be the coordination or interconnection of a number of individual computers. Various advantages of computer networks, network applications and key issues for computer networks are discussed.

5.0 SUMMARY

In this unit we have learnt:

- Various definitions of computer network
- Merits of computer network
- Various application areas of computer network
- Key issues for computer network

6.0 TUTOR MARKED ASSIGNMENT

1. What is meant by computer network?
2. Enumerate the concept of networking
3. Explain the basic network application areas
4. What are the key issues of computer network

7.0 FURTHER READING

1. Communication Networks: A First Course, 2nd edition, Jean Walrand, McGraw Hill, 1998.
2. Computer Networks, Andrew Tanenbaum, Prentice-Hall, 4th Edition, 2002.
3. Computer Networks: A Systems Approach, Larry Peterson & Bruce Davie, Morgan Kaufmann

MODULE 1: BASIC NETWORKING CONCEPTS

Unit 3: Networking hardware

Page

1.0	Introduction	15
2.0	Objectives	15
3.0	Networking hardware	15
4.0	Conclusion	20
5.0	Summary	20
6.0	Tutor Marked Assignment	20
7.0	Further Readings	20

1.0 INTRODUCTION

This unit describes the various components of networking hardware.

2.0 OBJECTIVES

At the end of this unit you should able to :

- Recognize and explain the individual components of the big picture of computer networks
- Outline the basic network configuration

3.0 NETWORKING HARDWARE

Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network.

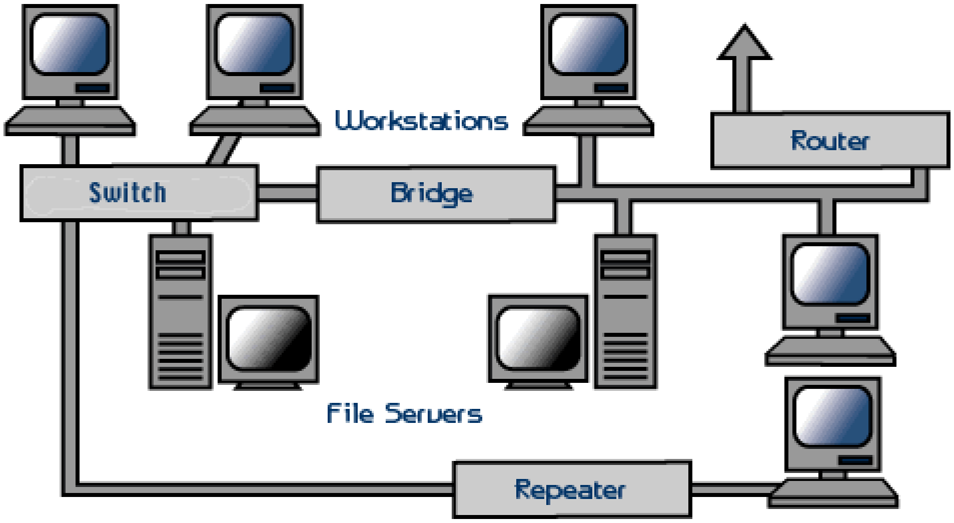


Fig. 1.3.1 Networking Hardware

Source : Florida Center for Instructional Technology College of Education, University of South Florida ©1997-2005.

This section provides information on the following components:

- File Servers
- Workstations
- Network Interface Cards
- Switches
- Repeaters
- Bridges
- Routers

File Servers

A file server stands at the heart of most networks. It is a very fast computer with a large amount of RAM and storage space, along with a fast network interface card. The network operating system software resides on this computer, along with any software applications and data files that need to be shared.

The file server controls the communication of information between the nodes on a network. For example, it may be asked to send a word processor program to one workstation, receive a database file from another workstation, and store an e-mail message during the same time period. This requires a computer that can store a lot of information and share it very quickly. File servers should have at least the following characteristics:

- 800 megahertz or faster microprocessor (Pentium 3 or 4, G4 or G5)
- A fast hard drive with at least 120 gigabytes of storage
- A RAID (Redundant Array of Inexpensive Disks) to preserve data after a disk casualty
- A tape back-up unit (i.e. DAT, JAZ, Zip, or CD-RW drive)
- Numerous expansion slots
- Fast network interface card
- At least 512 MB of RAM

Workstations

All of the user computers connected to a network are called workstations. A typical workstation is a computer that is configured with a network interface card, networking software, and the appropriate cables. Workstations do not necessarily need floppy disk drives because files can be saved on the file server. Almost any computer can serve as a network workstation.

Network Interface Cards

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, with the card fitting into an expansion slot inside the computer. Some computers, such as Mac Classics, use external boxes which are attached to a serial port or a SCSI port. Laptop computers can now be purchased with a network interface card built-in or with network cards that slip into a PCMCIA slot.

Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using.

The three most common network interface connections are Ethernet cards, LocalTalk connectors, and Token Ring cards. According to a International Data Corporation study, Ethernet is the most popular, followed by Token Ring and LocalTalk.

Ethernet Cards

Ethernet cards are usually purchased separately from a computer, although many computers (such as the Macintosh) now include an option for a pre-installed Ethernet card. Ethernet cards contain connections for either coaxial or twisted pair cables (or both) (See fig. 1.3.2). If it is designed for coaxial cable, the connection will be BNC. If it is designed for twisted pair, it will have a RJ-45 connection. Some Ethernet cards also contain an AUI connector. This can be used to attach coaxial, twisted pair, or fiber optics cable to an Ethernet card. When this method is used there is always an external transceiver attached to the workstation.

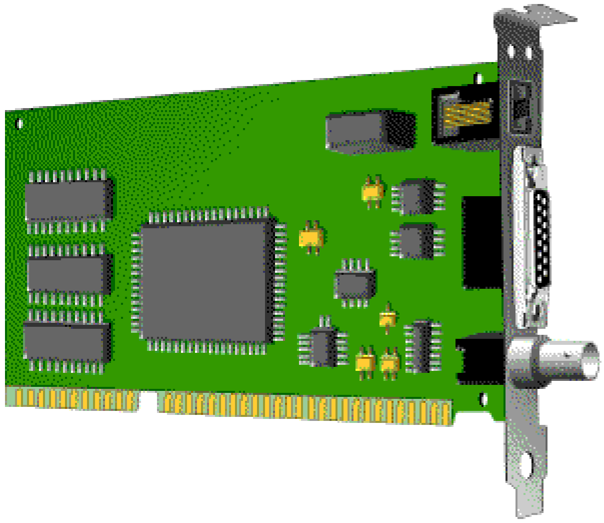


Fig. 1.3.2 Ethernet card.(From top to bottom: RJ-45, AUI, and BNC connectors)

Source: http://blue.utb.edu/libertad/clipart/pi_wireless_pc_card_b.jpg

LocalTalk Connectors

LocalTalk is Apple's built-in solution for networking Macintosh computers. It utilizes a special adapter box and a cable that plugs into the printer port of a Macintosh. A major disadvantage of LocalTalk is that it is slow in comparison to Ethernet. Most Ethernet connections operate at 10 Mbps (Megabits per second). In contrast, LocalTalk operates at only 230 Kbps (or .23 Mbps).

Token Ring Cards

Token Ring network cards look similar to Ethernet cards. One visible difference is the type of connector on the back end of the card. Token Ring cards generally have a nine pin DIN type connector to attach the card to the network cable.

Switch

A concentrator is a device that provides a central connection point for cables from workstations, servers, and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central switch/hub. Most switches are active, that is they electrically amplify the signal as it moves from one device to another. Switches no longer broadcast network packets as hubs did in the past, they memorize addressing of computers and send the information to the correct location directly. Switches are:

- Usually configured with 8, 12, or 24 RJ-45 ports
- Often us ed in a star or star-wired ring topology
- Sold with specialized software for port management
- Also called hubs
- Usually installed in a standardized metal rack that also may store net-modem, bridges, or routers.

Repeaters

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted-pair cable to a multi-port active concentrator. The concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.

Bridges

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. You might say that the bridge is like a traffic cop at a busy intersection during rush hour. It keeps information flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be used to connect different types of cabling, or physical topologies. They must, however, be used between networks with the same protocol..

Routers

A router translates information from one network to another; it is similar to a super-intelligent bridge. Routers select the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts.

While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges, and other routers on the network. Routers can even "listen" to the entire network to determine which sections are busiest -- they can then redirect data around those sections until they clear up. Routers can:

- Direct signal traffic efficiently
- Route messages between any two protocols
- Route messages between linear bus, star, star-wired ring topologies
- Route messages across fiber optic, coaxial and twisted-pair cabling

Exercise 1.3.1 Describe circuit switching.

Answer: Circuit switching entails a dedicated (non-shared) path between a sender and a receiver. Circuit switching requires circuit establishment, datatransfer, and disconnect.

Exercise 1.3.2 In the context of circuit switching, what is "blocking"?

Answer: A blocking switching may deny connections due to resource limitation. That is, two idle connected stations may not be able to communicate due to lack of resources in a switch caused by other connections.

4.0 CONCLUSION

Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network.

5.0 SUMMARY

This unit provides information on the following networking components:

- File Servers
- Workstations
- Network Interface Cards
- Switches
- Repeaters
- Bridges
- Routers

6.0 TUTOR MARKED ASSIGNMENT

1. What are the major components of networking hardware?
2. Briefly discuss the following hardware components:
   - File Servers
   - Workstations
   - Network Interface Cards
   - Switches
   - Repeaters
   - Bridges
   - Routers

7.0 FURTHER READINGS

1. Communication Networks*: A First Course,* 2nd edition, Jean Walrand, McGraw Hill, 1998.
2. Computer Networks, Andrew Tanenbaum, Prentice-Hall, 4th Edition, 2002.
3. Computer Networks: A Systems Approach, Larry Peterson & Bruce Davie, Morgan Kaufmann

MODULE 1: BASIC NETWORKING CONCEPTS

Unit 4: Network operating system

		Page
1.0	Introduction	22
2.0	Objectives	22
3.0	Network operating system	22
4.0	Conclusion	25
5.0	Summary	25
6.0	Tutor Marked Assignment	25
7.0	Further Reading and Other Resources	25

1.0 INTRODUCTION

Network operating system, NOS is the software that allows multiple computers to communicate, share files and hardware devices with one another. Network operating systems (NOS) typically are used to run computers that act as servers. They provide the capabilities required for network operation. Network operating systems are also designed for client computers and provide functions so the distinction between network operating systems and stand alone operating systems is not always obvious.

2.0 OBJECTIVES

At the end of this unit you will be able:

- Explain network operating system
- Describe the functions of network operating system
- Differentiate between peer-to-peer network operating system and client-server network operating system.

3.0 NETWORK OPERATING SYSTEM

A network operating system (NOS) is a computer operating system that is designed primarily to support workstation, personal computer, and, in some instances, older terminal that are connected on a local area network (LAN). Artisoft's LANtastic, Banyan VINES, Novell's Netware, and Microsoft's LAN Manager are examples of network operating systems. In addition, some multi-purpose operating systems, such as Windows NT and Digital's OpenVMS come with capabilities that enable them to be described as a network operating system.

A network operating system provides printer sharing, common file system and database sharing, application sharing, and the ability to manage a network name directory, security, and other housekeeping aspects of a network.

Unlike operating systems, such as DOS and Windows, that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly.

The two major types of network operating systems are:

- Peer-to-Peer
- Client Server

Peer-to-Peer

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source (See fig. 1.4.1). In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. AppleShare and Windows for Workgroups are examples of programs that can function as peer-to-peer network operating systems.

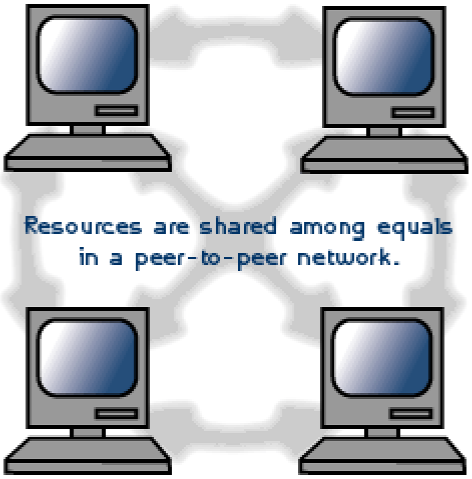


Fig. 1.4.1 Peer-to-peer network

Source: http://www.infinitygroup.com/images/internetworking.gif

Advantages of a peer-to-peer network:

- Less initial expense - No need for a dedicated server.
- Setup - An operating system (such as Windows XP) already in place may only need to be reconfigured for peer-to-peer operations.

Disadvantages of a peer-to-peer network:

- Decentralized - No central repository for files and applications.
- Security - Does not provide the security available on a client/server network.

Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers (See fig. 1.4.2). The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. Novell Netware and Windows 2000 Server are examples of client/server network operating systems.

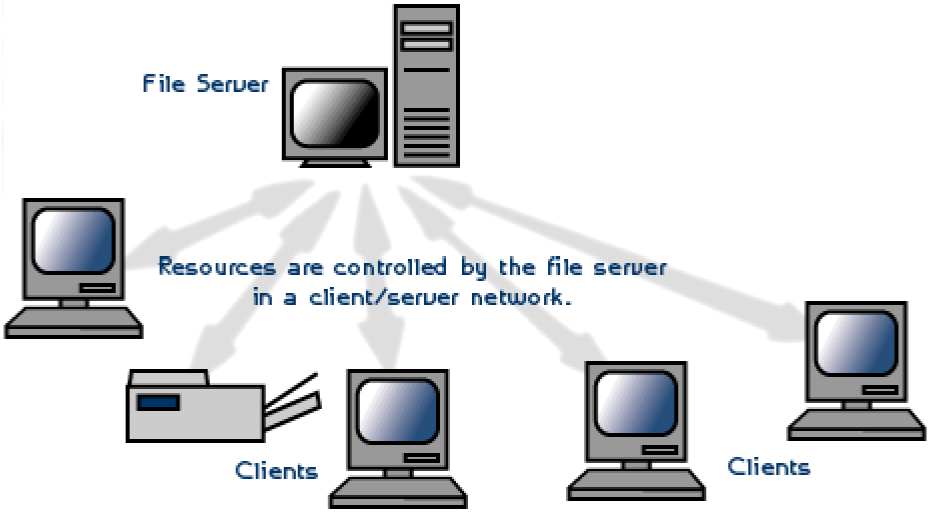

File Server
Resources are controlled by the file server
in a client/server network.
Clients
Clients

Fig.1.4. 2 Client/server network

Source: http://www.infinitygroup.com/images/internetworking.gif

Advantages of a client/server network:

- Centralized - Resources and data security are controlled through the server.
- Scalability - Any or all elements can be replaced individually as needs increase.
- Flexibility - New technology can be easily integrated into system.
- Interoperability - All components (client/network/server) work together.
- Accessibility - Server can be accessed remotely and across multiple platforms.

Disadvantages of a client/server network:

- Expense - Requires initial investment in dedicated server.
- Maintenance - Large networks will require a staff to ensure efficient operation.
- Dependence - When server goes down, operations will cease across the network.

Examples of network operating systems

Some examples of network operating systems include Novel Netware, Microsoft Windows NT, Microsoft Windows 2000, Microsoft Windows XP, Sun Solaris, Linux, AppleShare etc...

4.0 CONCLUSION

This unit has explained the meaning and importance of network operating system, It has highlighted the difference between peer-to-peer and client-server network operating systems

5.0 SUMMARY

In this unit we have been able to :

- Explain network operating system
- Describe the functions of network operating system
- Explain the difference between peer-to-peer network operating system and client-server network operating system.

6.0 TUTOR MARKED ASSIGNMENT

1. What is Network Operating System?
2. What are the functions of network operating system
3. Differentiate between peer-to-peer network operating system and client-server network operating system.

7.0 FURTHER READING

1. Stanford H. Rowe, Computer Networking, Prentice-Hall, Inc., Upper Saddle River, NJ, 2004

MODULE 2: NETWORK TOPOLOGIES, PROTOCOLS AND CONFIGURATION

Unit 1: Network topologies

1.0 Introduction 27

2.0 Objectives 27

3.0 Network topologies 27

3.1 Main types of physical topologies 28

3.1.1 Bus topology 28

3.1.2 Ring topology 29

3.1.3 Star topology 30

3.1.4 Tree topology 31

3.1.5 Mesh topology 33

3.1.6 Considerations when choosing topology 34

4.0 Conclusion 34

5.0 Summary 34

6.0 Tutor Marked Assignment 34

7.0 Further Reading and Other Resources 35

1.0 INTRODUCTION

A physical topology is the physical layout, or pattern, of the nodes on a network. It depicts a network in broad scope; that is, it does not specify device types, connectivity methods, or addressing schemes for the network. Physical topologies are divided into three fundamental geometric shapes: bus, ring, and star.

2.0 OBJECTIVES

At the end of this unit you will be able to

- Understand network topology concept
- Understand the geometric representation of computer network
- Explain the merits and demerits of various network topologies
- Know how to choose the right topology

3.0 NETWORK TOPOLOGIES

The term topology refers to the way a network is laid out, either physically or logically. The physical topology of a network refers to the configuration of cables, computers, and other peripherals while the logical topology is the method used to pass information between workstations. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to each other. There are five basic topologies possible: mesh, star, tree, bus, and ring.

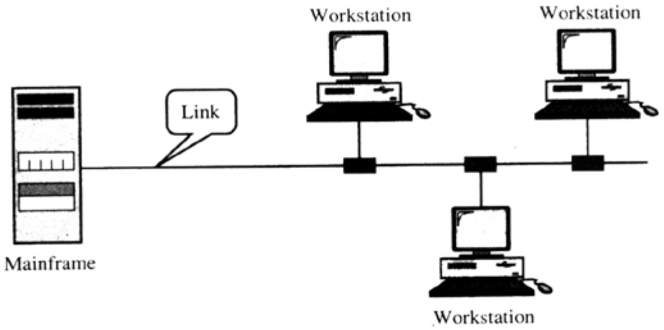


Fig. 2.1.1 - Multipoint Line Configuration

Source: http://en.wikipedia.org/wiki/Network_topology

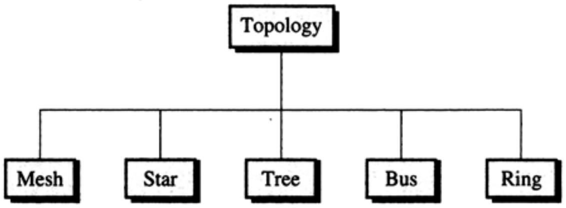


Fig. 2.1.2 - Categories of Topologies

Source: http://en.wikipedia.org/wiki/Network_topology

These five labels describe how the devices in a network are interconnected rather than their physical arrangement. For example, having a star topology does not mean that all of the computers in the network must be placed physically around a hub in a star shape. A consideration when choosing a topology is the relative status of the devices being linked. Two relationships are possible: peer-to-peer, where the devices share the link equally, and primary-secondary, where one device controls traffic and the others must transmit through it. Ring and mesh topologies are more convenient for peer-to-peer transmission, while star and tree are more convenient for primary-secondary, bus topology is equally convenient for either.

3.1 Main Types of Physical Topologies

The following sections discuss the physical topologies used in networks.

The most common topologies are:

- bus
- star
- ring
- mesh
- Tree.

Hybrid networks are the complex networks, which can be built of two or more above mentioned topologies.

3.1.1 Bus Topology

Bus topology uses a common backbone to connect all the network devices in a network in a linear shape. A single cable functions as the shared communication medium for all the devices attached with this cable with an interface connector. The device, which wants to communicate send the broadcast message to all the devices attached with the shared cable but only the intended recipient actually accepts and process that message.

A linear bus topology consists of a main run of cable with a terminator at each end (See fig.2.1.3). All nodes (file server, workstations, and peripherals) are connected to the linear cable. Eternet and Local Talk networks use a linear bus topology.

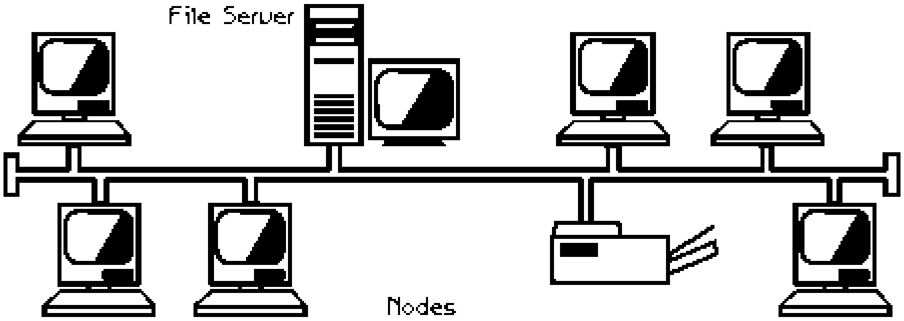


Fig. 2.1.3 Linear Bus topology

Source: http://en.wikipedia.org/wiki/Bus_network

Advantages of a Linear Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a Linear Bus Topology

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

3.1.2 Ring Topology

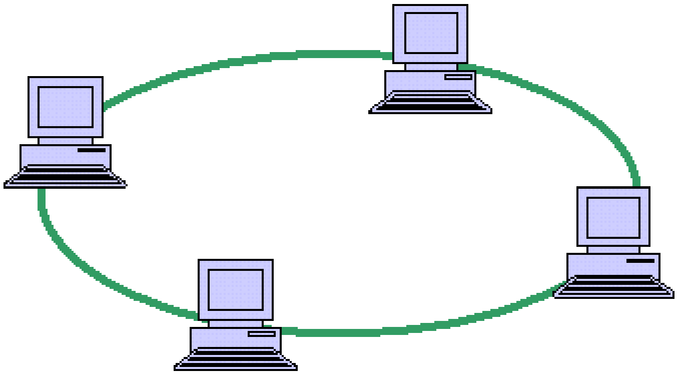


Fig. 2.1.4 Ring topology (Source: http://en.wikipedia.org/wiki/Ring_network)

A ring topology is a network topology or circuit arrangement in which each network device is attached along the same signal path to two other devices, forming a path in the shape of a ring. Each device in the network that is also referred to as node handles every message that flows through the ring. Each node in the ring has a unique address. Since in ring topology there is only one pathway between any two nodes, ring networks are generally disrupted by the failure of a single link.

The redundant topologies are used to eliminate network downtime caused by a single point of failure. All networks need redundancy for enhanced reliability. Network reliability is achieved through reliable equipment and network designs that are tolerant to failures and faults. The FDDI networks overcome the disrupt ion in the network by sending data on a clockwise and a counterclockwise ring. In case there is a break in data flow, the data is wrapped back onto the complementary ring before it reaches the end of the cable thereby maintaining a path to every node within the complementary ring. The most well known example of a ring topology is Token Ring.

Advantages

- An orderly network where every device has access to the token and the opportunity to transmit
- Under heavy network load performs better than a start topology.
- To manage the connectivity between the computers it doesn't need network server.

Disadvantages

- One malfunctioning workstation can throw away the entire network.
- Moves, adds and changes of devices can affect the entire network .
- It is slower than an Ethernet network.

3.1.3 Star Topology

In the computer networking world the most commonly used topology in LAN is the star topology. Star topologies can be implemented in home, offices or even in a building. All the computers in the star topologies are connected to central devices like hub, switch or router. The functionality of all these devices is different. As compared to the bus topology, a star network requires more devices & cables to complete a network. The failure of each node or cable in a star network, won't take down the entire network as compared to the Bus topology. However if the central connecting devices such as hub, switch or router fails due to any reason, then ultimately all the network can come down or collapse.

A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub or concentrator (See fig.2.1.5).

Data on a star network passes through the hub or concentrator before continuing to its destination. The hub or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted-pair cable; however, it can also be used with coaxial cable or fiber-optic cable.

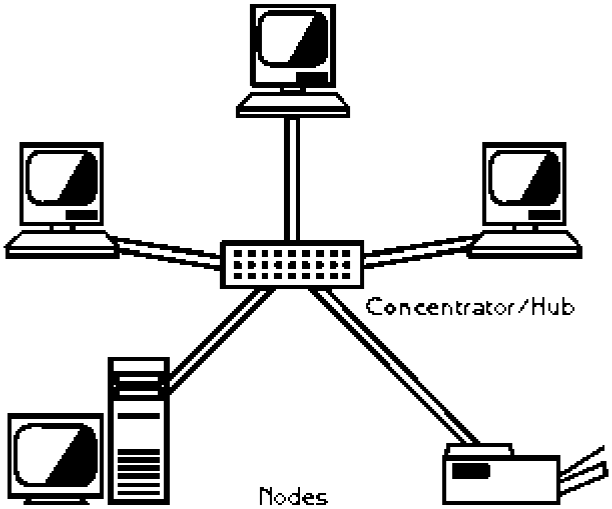


Fig.2.1.5 Star topology

Source: http://en.wikipedia.org/wiki/Star_network

Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network then connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators.

The protocols used with star configurations are usually Eternet or Local Talk.

3.1.4 Tree Topology

Tree topologies are comprised of the multiple star topologies on a bus. Tree topologies integrate multiple star topologies together onto a bus. Only the hub devices can connect directly with the tree bus and each Hub functions as a root of a tree of the network devices. This bus/star/hybrid combination supports future expandability of the computer networks, much better than a bus or star (See fig. 2.1.6).

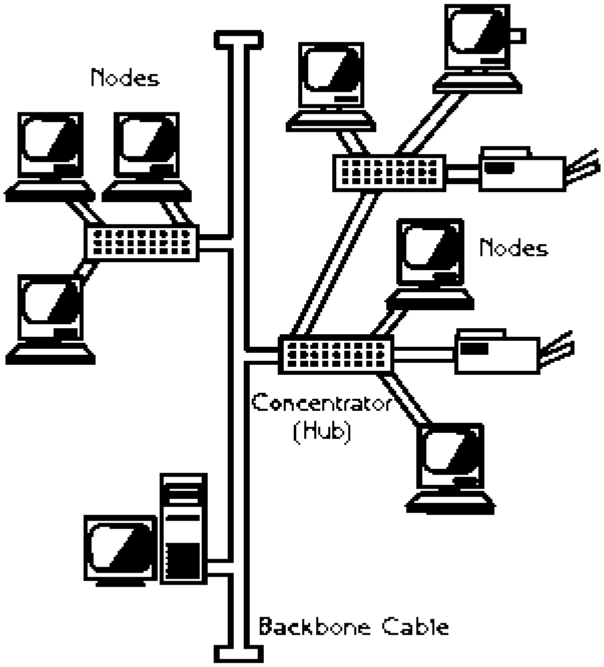


Fig. 2.1.6 Tree topology

Source: http://en.wikipedia.org/wiki/Tree_network

Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

5-4-3 Rule

A consideration in setting up a tree topology using Ethernet protocol is the 5-4-3 rule. One aspect of the Ethernet protocol requires that a signal sent out on the network cable reach every part of the network within a specified length of time. Each concentrator or repeater that a signal goes through adds a small amount of time. This leads to the rule that between any two nodes on the network there can only be a maximum of 5 segments, connected through 4 repeaters/concentrators. In addition, only 3 of the segments may be populated (trunk) segments if they are made of coaxial cable. A populated segment is one which has one or more nodes attached to it.

3.1.5 Mesh topology

In the topologies shown above, there is only one possible path from one node to another node. If any cable in that path is broken, the nodes cannot communicate.

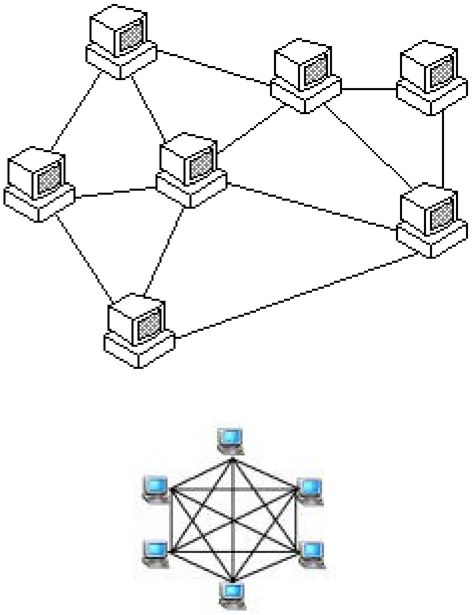


Fig. 2.1.7. Mesh topology

Source: http://en.wikipedia.org/wiki/Mesh_network

Mesh topology uses lots of cables to connect every node with every other node. It is very expensive to wire up, but if any cable fails, there are many other ways for two nodes to communicate. Some WANs, like the Internet, employ mesh routing. In fact the Internet was deliberately designed like this to allow sites to communicate even during a nuclear war.

Mesh topology work on the concept of routes. In Mesh topology, message sent to the destination can take any possible shortest, easiest route to reach its destination. In the previous topologies star and bus, messages are usually broadcasted to every computer, especially in bus topology. Similarly in the Ring topology message can travel in only one direction i.e clockwise or anticlockwise. Internet employs the Mesh topology and the message finds its route for its destination. Router works in finding the routes for the messages and in reaching them to their destinations. The topology in which every devices connects to every other device is called a full Mesh topology unlike in the partial mesh in which every device is indirectly connected to the other devices.

3.1.6 Considerations When Choosing a Topology:

It is important to choose the right topology for how the network will be used. Each topology has its own characteristic. To choose the right topology we must see the factors that influenced it. The factors are:

- **Length of cable needed**. The linear bus network uses shorter lengths of cable.
- **Future growth**. With a star topology, expanding a network is easily done by adding another concentrator.
- **Cable type**. The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

Exercise 2.1.1 What is the key disadvantage of a physically direct-wired LAN? Explain how a star-wired LAN remedies this disadvantage.

Answer: Fault detection and isolation are very difficult in a large (large span and large number of stations) direct-wired LAN. To find and isolate a fault one must literally "walk the wire". In a star wired LAN faults can be detected and isolated in a central location – the wiring closet. To detect and isolate a fault in a wiring closet, individual lobes of the LAN can be unplugged until the LAN returns to operation. This can be automated.

4.0 CONCLUSION

Topologies are the important part of the network design theory. A better network can be built if you have the knowledge of these topologies and if you know the difference between each topology. Similarly you should have the knowledge of each network device so that you can properly use them according to your network needs. A mis-configured network can result in a waste of time and energy as well as a lots of troubleshooting methods to resolve the issue. So the basic understanding of the network topologies and network devices is a must to build a good network.

5.0 SUMMARY

In this unit we have been able to:

- Discuss network topology concept
- Describe the geometric representation of computer network
- Explain the merits and demerits of various network topologies
- Show how to choose the right topology

6.0 TUTOR MARKED ASSIGNMENT

1. In networking, what does the term *topology* refer to?
2. Describe the geometric representations of computer network
3. Explain the merits and demerits of various network topologies
4. What are the considerations for choosing the right topology?

7.0 FURTHER READINGS

1. Ed, T. Theory and Problems of Computer Networking. USA: Schaum's Outline Series, McGRAW-HILL, 2002.

MODULE 2: NETWORK TOPOLOGIES, PROTOCOLS AND CONFIGURATION

Unit 2: Network protocols

1.0 Introduction 37

2.0 Objectives 37

3.0 Network protocol 37

3.1 Type of protocols 38

3.2 Protocols properties 48

4.0 Conclusion 48

5.0 Summary 48

6.0 Tutor Marked Assignment 48

7.0 Further Reading and Other Resources 49

1,0 INTRODUCTION

The word protocol is derived from the Greek word “protocollon” which means a leaf of paper glued to manuscript volume. In computer protocols means a set of rules, a communication language or set of standards between two or more computing devices. Protocols exist at the several levels of the OSI (open system interconnectivity) layers model. In the telecommunication system, there are one or more protocols at each layer of the telephone exchange. On the internet, there is a suite of the protocols known as TCP/IP protocols that are consisting of transmission control protocol, internet protocol, file transfer protocol, dynamic host configuration protocol, Border gateway protocol and a number of other protocols.

2.0 OBJECTIVES

* To assist students in understanding network protocols
* To assist students in analyzing networking requirements.

3.0 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. In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. Examples include application programs, file transfer packages, browsers, database management systems, and electronic mail software. A system, is a physical object that contains one or more entities, Examples include computers and terminals. But two entities cannot just send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communication. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

Syntax

Syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first eight bits of data to be the address of the sender, the second eight bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics

Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation. For example, does an address identify the route to be taken or the final destination of the message?

Timing

Timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

In data communication, a protocol is a set of rules that govern all aspects of information communication.

3.1 TYPE OF PROTOCOLS

There are a many standard protocols to choose from, standard protocols have their own advantage and disadvantage i.e., some are simpler than the others, some are more reliable, and some are faster. From a user's point of view, the only interesting aspect about protocols is that our computer or device must support the right ones if we want to communicate with other computers. The protocols can be implemented either in hardware or in software.

Some of the popular protocols are:

NetBIOS

Network basic input/output system is an application programming interface (API). Applications located on different computers; use NetBIOS to communicate each other over a local area network (LAN). NetBIOS is widely used in Ethernet, token ring, and Windows NT networks. NetBIOS provides services at the transport and session layer of the OSI model. NetBIOS supports three services;
* Name service for name registration and resolution.
* Session service for connection-oriented communication.
* Datagram services for connection less communication.

TCP/IP

Transmission control protocol/internet protocol (TCP/IP) is the communication protocol used by internet. It is used for communication in a private network such as internet or extranet. It performs various functions such as multiplexing, error recovery, flow control, connection establishment, termination and segmentation.

Address Resolution Protocols

The data packets travel through various physical networks to reach the destination. At the physical layer, routers and hosts are recognized by their physical address, which is a local address. It is usually implemented in hardware. To communicate within the same network, the physical address can solve the purpose. However, to communicate between different networks, both the physical (MAC) and logical (IP) address are required. The user should be able to map a logical address to its corresponding physical address and vice versa. There are two protocols used for this purpose. The ARP maps the logical address to a physical address and the RARP maps the physical address to a logical address.

* Address Resolution Protocol (ARP)

Address resolution protocol (ARP) associates an IP address with its physical address whenever a host or router want to determine the physical address of other host or router on the network it broadcast ARP query packet containing the physical and IP address of the receiver over the network. Every device and router on the network receives the packet checks for the IP address and processes it. The interred recipient identifies its IP address and responds with an ARP reply packet, which contains its IP and physical address. Now the sender can send all the packet intended for this receiver.

* Reverse Address Resolution Protocol (RARP)

In a network, each device and router is assigned a unique logical address, which is required while creating the IP datagram. This address is normally saved in a configuration file, which is stored on the hard disk. However, when a diskless machine is booted from ROM, it can’t discover its IP address. Reverse address resolution protocol (RARP) is used to determine the logical address when the physical address is known. A device booted for the first time gets it physical address from the NIC card. The device creates a RARP request packet and broadcast it over the network. Another device on the network working as the server and having all the IP address responds with a RARP reply packet. This packet includes the IP address of the sender.

Internet Control Message protocol (ICMP)

Internet control message protocol message (ICMP) is an extension to internet protocol, which support packets containing error, control and information messages. It provides a method for communicating error messages and other transmission information. Two types of ICMP messages are error-reporting message and query messages.

a. Error Reporting Message: Error messages report any problem that a router or host may come across while processing the IP datagram. The messages are following below.

* Destination unreachable: If a router is unable to deliver a datagram to the destination, it sends a ‘destination unreachable’ message back to the source that transmitted the datagram.
* Source Quench: This message is used for flow control at the network layer. The router sends a ‘source quench’ message to the sender to slow down the transmission rate as congestion has occurred in the network.
* Time exceeded: When the TTL value zero, the router discards the datagram and sends a ‘time exceeded’ message back to the sender.
* Parameter Problem: If there is an ambiguity in the header of the datagram, them the ‘parameter problem’ message is send back to the sender by the host or router.
* Redirection: If the host forwards a datagram to a wrong router the router will forward it to the correct router and send a ‘redirection message’ to the host to update its routing table.

b. ICMP Query Message: ICMP query messages are used to identify network problems. The messages are following below:

* Echo request and reply: A device can also check whether another device is reachable or unreachable. One device sends an ‘echo-request’ message to another device, which replies with an ‘echo-reply’ message.
* Timestamp Request and Reply: This message is used to determine the round-trip time requested for a datagram to travel between two machines.
* Address mark Request and Reply: A host may have its full IP address but may not know the corresponding mask. To know its mask, a host sends the address mask request message to a router, which replies with the address mask reply message. This message contains the required mask for the host.
* Router solicitation and advertisement: This message is used to determine whether the routers in a network are working properly. All the routers that receive router solicitation message from a host broadcast their routing information through the ‘router advertisement message’.
* Internet Group Message Protocol (IGMP): Internet group message protocol (IGMP) allows hosts to participate in multicasting. A message can forwarded to a large number of recipients simultaneously using multicasting. Multicast routers are used for forwarding the multicast packets to hosts or other routers. There are three type of IGMP messages. The query, the membership report and the leave report.

* Query: Query messages are used to determine multicast groups of hosts or devices. They are of two types;

i. General query: This message discovers which groups have member on the attached network. This message is intended for all groups and not a specific one.
ii. Special Query: This message help to determine if a specific group has any members of the attached network.

* Membership Report: When a host joins a multicast group, it sends a multicast report. Some time the IGMP router can function as queries, which can send a query message to the host. In such a condition, the host replies with a membership report message.
• Leave Report: When a host leaves a multicast group, it sends this message to all the members.

User Datagram Protocol (UDP)

User datagram protocol (UDP) is a transport layer connection less protocol that uses port numbers to provide process-to-process communication. The protocol accepts smaller data units from the processes and delivers them to the receiver. If the UDP detects any kind of error in the data unit, it drops that unit. UDP sends each datagram independently. The individual datagram are not related to each other even if they cone from the same source application and reach same destination application program. There are three stages; encapsulation, encapsulation, and queuing. In UDP, data is passed in the form of packets are called as user datagram’s. User datagram’s consists of 8-bytes header and data.

Inter-network packet exchange/sequenced packet exchange
IPX/SPX is a communication protocol of the Novell Netware operating system used by the clients and server to transfer data within the networks. IPX is a network layer protocol used for connectionless communication where as SPX is a transport layer protocol used for connection-oriented communication.

Data Link control (DLC)
Data link control (DLC) protocols are setup transmission protocols used at the data link layer. DLC protocols are two types. Asynchronous and synchronous. Asynchronous protocols have no synchronization between the sender and receiver during data transfer. In synchronous transmission, data packet contains the control information for synchronization. Two synchronous protocol used ate high level data link control (HDLC) protocol and synchronous data link control (SDLC) protocol. These are bit-oriented protocol in which data frame are interpreted as series of bits. HDLC provides a data transmission mechanism at the data link layer. Data is encapsulated in to the lower layers. HDLC is used both half-duplex and full-duplex communication. It ensures that the data is received error free without loss and in the correct order. SDLC protocol is a bit-oriented protocol invented by IBM and similar to HDLC. SDLC frame format is exactly same as that of HDLC. Earlier this protocol was used to link PCs to mainframe computers. Later on Hewlett Packard (HP) adopted the DLC protocol for use by network printers. All version of windows including windows XP still support DLC but it is only required while you install an older printer.

HTTP (Hyper Text Transfer Protocol)

Hypertext transfer protocol is a method of transmitting the information on the web. HTTP basically publishes and retrieves the HTTP pages on the World Wide Web. HTTP is a language that is used to communicate between the browser and web server. The information that is transferred using HTTP can be plain text, audio, video, images, and hypertext. HTTP ``11qssis a request/response protocol between the client and server. Many proxies, tunnels, and gateways can be existing between the web browser (client) and server (web server). An HTTP client initializes a request by establishing a TCP connection to a particular port on the remote host (typically 80 or 8080). An HTTP server listens to that port and receives a request message from the client. Upon receiving the request, server sends back 200 OK messages, its own message, an error message or other message.

POP3 (Post Office Protocol)

In computing, e-mail clients such as (MS outlook, outlook express and thunderbird) use Post office Protocol to retrieve emails from the remote server over the TCP/IP connection. Nearly all the users of the Internet service providers use POP 3 in the email clients to retrieve the emails from the email servers. Most email applications use POP protocol.

SMTP (Simple Mail Transfer Protocol)

Simple Mail Transfer Protocol is a protocol that is used to send the email messages between the servers. Most email systems and email clients use the SMTP protocol to send messages to one server to another. In configuring an email application, you need to configure POP, SMTP and IMAP protocols in your email software. SMTP is a simple, text based protocol and one or more recipient of the message is specified and then the message is transferred. SMTP connection is easily tested by the Telnet utility. SMTP uses the by default TCP port number 25.

FTP (File Transfer Protocol)

FTP or file transfer protocol is used to transfer (upload/download) data from one computer to another over the internet or through or computer network. FTP is a most commonly communication protocol for transferring the files over the internet. Typically, there are two computers are involved in the transferring the files a server and a client. The client computer that is running FTP client software such as Cuteftp and AceFTP etc initiates a connection with the remote computer (server). After successfully connected with the server, the client computer can perform a number of the operations like downloading the files, uploading, renaming and deleting the files, creating the new folders etc. Virtually operating system supports FTP protocols.

IP (Internet Protocol)

An Internet protocol (IP) is a unique address or identifier of each computer or communication devices on the network and internet. Any participating computer networking device such as routers, computers, printers, internet fax machines and switches may have their own unique IP address. Personal information about someone can be found by the IP address. Every domain on the internet must have a unique or shared IP address.

DHCP (Dynamic Host Configuration Protocol)

The DHCP or Dynamic Host Configuration Protocol is a set of rules used by a communication device such as router, computer or network adapter to allow the device to request and obtain and IP address from a server which has a list of the larger number of addresses. DHCP is a protocol that is used by the network computers to obtain the IP addresses and other settings such as gateway, DNS, subnet mask from the DHCP server. DHCP ensures that all the IP addresses are unique and the IP address management is done by the server and not by the human. The assignment of the IP addresses is expires after the predetermined period of time. DHCP works in four phases known as DORA such as Discover, Observe, Request and Authorize

IMAP (Internet Message Access Protocol)

The Internet Message Access Protocol known as IMAP is an application layer protocol that is used to access to access the emails on the remote servers. POP3 and IMAP are the two most commonly used email retrieval protocols. Most of the email clients such as outlook express, thunderbird and MS outlooks support POP3 and IMAP. The email messages are generally stored on the email server and the users generally retrieve these messages whether by the web browser or email clients. IMAP is generally used in the large networks. IMAP allows users to access their messages instantly on their systems.

ARCNET

ARCNET is a local area network technology that uses token bus scheme for managing line sharing among the workstations. When a device on a network wants to send a message, it inserts a token that is set to 1 and when a destination device reads the message it resets the token to 0 so that the frame can be used by another device.

FDDI

Fiber distributed data interface (FDDI) provides a standard for data transmission in a local area network that can extend a range of 200 kilometers. The FDDI uses token ring protocol as its basis. FDDI local area network can support a large number of users and can cover a large geographical area. FDDI uses fiber optic as a standard communication medium. FDDI uses dual attached token ring topology. A FDDI network contains two token rings and the primary ring offers the capacity of 100 Mbits/s. FDDI is an ANSI standard network and it can support 500 stations in 2 kilometers.

UDP

The user datagram protocol is a most important protocol of the TCP/IP suite and is used to send the short messages known as datagram. Common network applications that uses UDP are DNS, online games, IPTV, TFTP and VOIP. UDP is very fast and light weight. UDP is an unreliable connectionless protocol that operates on the transport layer and it is sometimes called Universal Datagram Protocol.

X.25

X.25 is a standard protocol suite for wide area networks using a phone line or ISDN system. The X.25 standard was approved by CCITT now ITU in 1976.

TFTP

Trivial File Transfer Protocol (TFTP) is a very simple file transfer protocol with the very basic features of the FTP. TFTP can be implemented in a very small amount of memory. TFTP is useful for booting computers such as routers. TFTP is also used to transfer the files over the network. TFPT uses UDP and provides no security features.

SNMP

The simple network management protocol (SNMP) forms the TCP/IP suite. SNMP is used to manage the network attached devices of the complex network.

PPTP

The point to point tunneling protocol is used in the virtual private networks. PPP works by sending regular PPP session. PPTP is a method of implementing VPN networks.

LocalTalk

LocalTalk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers. The method used by LocalTalk 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. LocalTalk 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 LocalTalk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of LocalTalk 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.

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.

ETHERNET

History of the Ethernet

Ethernet is a well-known and widely used network technology that employs bus topology. Ethernet was invented at Xerox Corporation's Palo Alto Research Center in the early 1970s. Digital Equipment Corporation, Intel Corporation, and Xerox later cooperated to devise a production standard, which is informally called DIX Ethernet for the initials of the three companies. IEEE now controls Ethernet standards. In its original version, an Ethernet LAN consisted of a single coaxial cable, called the ether, to that multiple computers connect. Engineers use the term segment to refer to the Ethernet coaxial cable. A given Ethernet segment is limited to 500 meters in length, and the standard requires a minimum separation of 3 meters between each pair of connections. The original Ethernet hardware operated al a bandwidth of 10 Megabits per second (Mbps); a later version known as Fast Ethernet operates at IUU Mbps. and the most recent version, which is known as Gigabit Ethernet operates at 1000 Mbps or 1 Gigabit per second (Gbps).

Sharing on an Ethernet

The Ethernet standard specifies all details, including the format of frames that computers send across the ether, the voltage to be used, and the method used to modulate a signal. Because it uses a bus topology, Ethernet requires multiple computers to share access to a single medium. A sender transmits a signal, which propagates from the sender toward both ends of the cable.

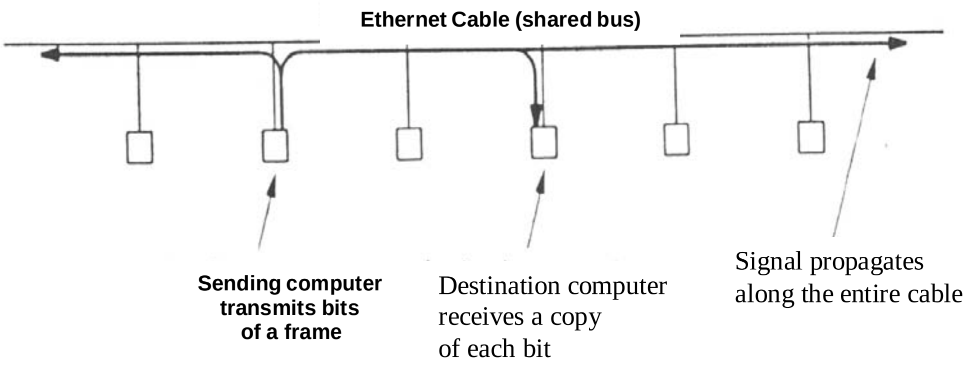

Ethernet Cable (shared bus)
Sending computer transmits bits of a frame
Destination computer receives a copy of each bit
Signal propagates along the entire cable

Fig. 2.2.1 - Conceptual flow of bits across an Ethernet

Source: http://en.wikipedia.org/wiki/Ethernet_hub

A signal propagates from the sending computer to both end of the shared cable. It is important to understand that sharing in local area network technologies does not mean that multiple frames are being sent at the same time. In stead, the sending computer has exclusive use of the entire cable during the transmission of a given frame- other computers must wait. After one-computer finishers transmitting one frame, the shared cable becomes available for another computer to use.

Carrier Sense on Multi-Access Networks (CSMA)

The most interesting aspect of Ethernet is the mechanism used to coordinate transmission. An Ethernet network does not have a centralized controller that tells each computer how to take turns using the shard cable. Instead, all computers attached to an Ethernet participate in a distributed coordination scheme called Carrier Sense Multiple Access (CSMA). The scheme uses electrical activity on the cable to determine status. When no computer is sending a frame, the ether does not contain electrical signals. During frame transmission, however, a sender transmits electrical signals used to encode bits. Although the signals differ slightly from the carrier waves, they are informally called a carrier. Thus, to determine whether the cable is currently being used, a computer can check for a carrier. If no carrier is present, the computer can transmit a frame. If a carrier is present, the computer must wait for the sender to finish before proceeding. Technically, checking for a carrier wave is called carrier sense, and the idea of using the presence of a signal to determine when to transmit is called Carrier Sense Multiple Access (CSMA).

Carrier Sense Multiple Access with Collision Detect (CSMA/CD)

Because CSMA allows each computer to determine whether a shared cable is already in use by another computer, it prevents a computer from interrupting an ongoing transmission. However, CSMA cannot prevent all possible conflicts. To understand why, imagine what happens if two computers at opposite ends of an idle cable both have a frame ready to send at the same time. When they check for a carrier, both stations find the cable idle, and both start to send frames simultaneously. The signals travel at approximately 70% of the speed of light, and when the signals transmitted by two computers reach the same point on the cable, they interfere with each other.

The interference between two signals is called a collision. Although a collision does not harm the hardware, it produces a garbled transmission that prevents either of the two frames from being received correctly. To ensure that no other computer transmits simultaneously, the Ethernet standard requires a sending station to monitor signals on the cable. If the signal on the cable differs from the signal that the station is sending, it means that a collision has occurred. Whenever a collision is detected, a sending station immediately stops transmitting. Technically, monitoring a cable during transmission is known as Collision Detect {CD), and the Ethernet mechanism is known as Carrier Sense Multiple Access with Collision Detect (CSMA/CD).

CSMA/CD does more than merely detect collisions - it also recovers from them. After a collision occurs, a computer must wait for the cable to become idle again before transmitting a frame. However, if the computers begin to transmit as soon as the ether becomes idle another collision will occur. To avoid multiple collisions, Ethernet requires each computer to delay after a collision before attempting to retransmit. The standard specifies a maximum delay, d, and forces each computer to choose a random delay less than d. In most cases, when a computer chooses a delay at random, it will select a value that differs from any of the values chosen by the other computers – the computer that chooses the smallest delay will proceed to send a frame and the network will return to normal operation.

If two or more computers happen to choose nearly the same amount of delay after a collision, they will both begin to transmit at nearly the same time, producing a second collision. To avoid a sequence of collisions, Ethernet requires each computer to double the range from which a delay is chosen after each collision. Thus, a computer chooses a random delay from 0 to d after one collision, a random delay between 0 and 2d after a second collision, between 0 and 4d after a third, and soon after a few collisions, the range from which a random value is chosen becomes large, and the probability is high that some computer will choose a short delay and transmit without a collision.

Technically, doubling the range of the random delay after each collision is known as binary exponential back off. In essence, exponential back off means that an Ethernet can recover quickly after a collision because each computer agrees to wait longer times between attempts when the cable becomes busy. In the unlikely event that two or more computers choose delays that are approximately equal, exponential back off guarantees that contention for the cable will be reduced after a few collisions.

Computers attached to an Ethernet use CSMA/CD in which a computer waits for the ether lo be idle before transmitting a frame. If two computers transmit simultaneously, a collision occurs: the computers use exponential back off to choose which computer will proceed. Each computer' delays a random time before trying to transmit again, and then doubles the delay for each successive collision.

Basis and Working

Ethernet is a very popular local area network architecture based on the CSMA/CD access method. The original Ethernet specification was the basis for the IEEE 802.3 specifications. In present usage, the term "Ethernet" refers to original Ethernet (or Ethernet II, the latest version) as well as the IEEE 802.3 standards. The different varieties of Ethernet networks are commonly referred to as Ethernet topologies. Typically, Ethernet networks can use a bus physical topology, although, as mentioned earlier, many varieties of Ethernet such as 10BASE-T use a star physical topology and a bus logical topology. (Microsoft uses the term "star bus topology" to describe 10BASE-T.)

Ethernet networks, depending on the specification, operate at 10 or 100Mbps using base band transmission. Each IEEE 802.3 specification prescribes its own cable types.

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.

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.

3.2 PROTOCOLS PROPERTIES

Different protocols perform different functions so it is difficult to generalize the properties of the protocols. There are some basic properties of most of the protocols.

- Detection of the physical (wired or wireless connection)
- Handshaking
- How to format a message.
- How to send and receive a message.
- Negotiation of the various connections
- Correction of the corrupted or improperly formatted messages.
- Termination of the session.

4.0 CONCLUSION

Network protocols is a predefined setup rule, which govern the transfer of data and communication between the computers connected in a network. Protocols regulate the type of network access method, compression techniques while transmitting data, the topologies, the cabling methods and even the speed of data transfer.

5.0 SUMMARY

The widespread use of the communication protocols is a prerequisite to the internet. The term TCP/IP refers to the protocols suite and a pair of the TCP and IP protocols are the most important internet communication protocols. Most protocols in communication are layered together where the various tasks listed above are divided. Protocols stacks refer to the combination of the different protocols.

6.0 TUTOR MARKED ASSIGNMENT

1. Define Protocol.

2. Explain in brief the key elements of a protocol.

3. Compare and contrast the functions of Carrier Sense on Multi-Access Networks (CSMA) and Carrier Sense Multiple Access with Collision Detect (CSMA/CD).

7.0 FURTHER READINGS

1. TCP/IP Illustrated Volume 1 by R.W. Stevens, 1994[4],
2. TCP/IP Network Administration by C. Hunt, 2002[5].

MODULE 2: NETWORK TOPOLOGIES, PROTOCOLS AND CONFIGURATION

Unit 3: Network Configuration

1.0	**Introduction**	**51**
2.0	**Objectives**	**51**
3.0	**How to configure a network**	**51**
3.1	**Peer to Peer network model**	**51**
3.2	**Client/Server Network Model**	**52**
3.3	**Configuration steps**	**52**
4.0	**Conclusion**	**53**
5.0	**Summary**	**53**

1.0 INTRODUCTION

In this unit you will learn how to configure a network, peer to peer, client server, workstation, server, basic data communication.

2.0 OBJECTIVES

The main objective of this unit is to give a brief explanation on how to configure a network.

3.0 How to Configure a Network

3.1 Peer to Peer network model

Before configuring a computer network, you have to decide that, which networking model you require. There are two main types of network models. Peer to peer and client-server network model. In the peer to peer network model you simply use the same Workgroup for all the computers and a unique name for each computer.

Additionally, you will have to give a unique IP address of the same class A, B, or C for all the computers in your network and its related subnet mask e.g if you decide to use class A IP address for your three computers in your Peer to Peer network then your IP address/Subnet mask settings can be as follows.

Computer Name	IP Address	Subnet Mask	Workgroup
PC1	100.100.100.1	255.0.0.0	Office-network
PC2	100.100.100.2	255.0.0.0	Office-network
PC3	100.100.100.3	255.0.0.0	Office-network

Please note that the above example is for only illustration purpose so you can choose any IP address, computer name and workgroup name of your interest.

For doing this right click on My Computer and then click Properties then go to the Network Identification section and set these.

In a peer to peer network all computers acts as a client because there is not centralized server. Peer to peer network is used where not security is required in the network. If a computer fails to work then all other computers work normally in peer to peer network.

3.2 Client/Server Network Model

In the client/server network model a computer plays a centralized role and is known as a server all other computers in the network are known as clients. All client computers access the server simultaneously for files, database, docs, spreadsheets, web pages and resources like hard diver, printer, fax modem, CD/DVD ROM and others. In other words, all the client computes depends on the server and if server fails to respond or crash then networking/communication between the server and the client computes stops.

If you want to configure a client-server network model then first prepare the server. Install Windows 2000 or Windows 2003 Server from the CD on the server computer and make a domain. You can create a domain by this command on the Run “DCPROMO”. You can give this command once you install the server successfully. After you give the DCPROMO command you will be asked for a unique domain name. All the client computers will use the same unique domain name for becoming the part of this domain. This command will install the active directory on the server, DNS and other required things. A step by step wizard will run and will guide you for the rest of the steps. Make sure that a network cable is plugged in the LAN card of the server when you run the DCPROMO.exe command.

When the Active directory is properly installed on the server, restart the server. You can create network users on the server computer and also name/label the network resources like computers/printers etc.

Once you install the server successfully now come to the client computers. Install Windows 2000 professional on your all client computers. Once you install the Windows 2000 professional on the clients the next step is to make this computer (client computer) a part of the network.

3.3 Configuration Steps

1. Choose a unique name for each client computer
2. Choose unique IP address for each computer and relevant.
3. Use the same domain name for all client PCs.

Network/System administrators are required to do these administrative tasks on the server and client computers. Any shared resources on the network either on the server or the clients can be access through the My Network Places in the Windows 2000 platform. There is another way to connect to the shared resources by giving this command in the run \\ComputerName\SharedDriverLetter. Network configurations steps can be implemented by right clicking the My Computer>Properties>

For giving the IP address you will have to right click on the My Network places>properties>Local Area Connection>Properties>Internet Protocols (TCP/IP)>Properties and then give the IP address and subnet mask of the same range and class for all the computers in the network.

4.0 CONCLUSION

In this unit we have discussed how to configure both the peer to peer network model and client server network model. In addition we described briefly the steps to be followed while configuring a network.

5.0 SUMMARY

Basic network configuration techniques are considered in this unit

MODULE 3: OSI AND TCP/IP MODELS

Unit 1: Open Systems Interconnection Reference Model (OSI Model)

1.0	Introduction	55
2.0	Objectives	55
3.0	OSI model	55
3.1	Characteristics of the OSI 7 layers model	60
4.0	Conclusion	60
5.0	Summary	61
6.0	Tutor Marked Assignment	61
7.0	Further Readings	61

1.0 INTRODUCTION

The Open Systems Interconnection (OSI) reference model has been an essential element of computer network design since its ratification in 1984. The OSI is an abstract model of how network protocols and equipment should communicate and work together (interoperate). The OSI model is a technology standard maintained by the International Standards Organization (ISO). Although today's technologies do not fully conform to the standard, it remains a useful introduction to the study of network architecture.

2.0 OBJECTIVES

It expected that at the end of this unit students should be able to:

- Understand the seven layers of the OSI model.
- Describe the functions of each of the models

3.0 OSI MODEL

This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers. The model is called the ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems. We will usually just call it the OSI model for short.

The OSI model has seven layers. The principles that were applied to arrive at the seven layers are as follows

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

Below we will discuss each layer of the model in turn, starting at the bottom layer. Note that the OSI model itself is not network architecture because it does not specify the exact services and protocols to be used in each layer. It just tells what each layer should do. However, ISO has also produced standards for all the layers, although these are not part of the reference model itself. Each one has been published as a separate international standard.

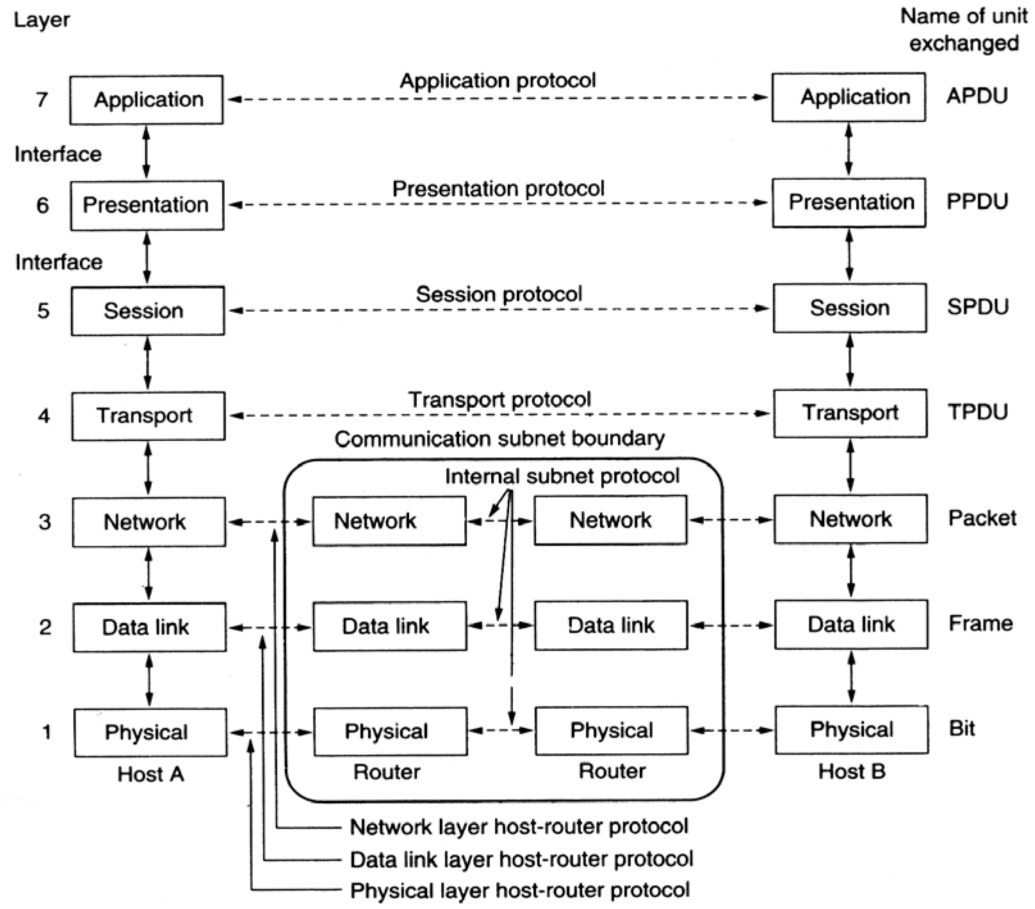


Fig. 3.1.1 - The OSI Reference Model

Source: http://ezinearticles.com/?Seven-Layers-of-ISO-OSI-Model&id=349951

The Physical Layer

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. Typical questions here are how many volts should be used to represent a 1 and how many for a 0, how many microseconds a bit lasts, whether transmission may proceed simultaneously in both directions, how the initial connection is established and how it is torn down when both sides are finished, and how many pins the network connector has and what each pin is used for. The design issues here largely deal with mechanical, electrical, and procedural interfaces, and the physical transmission medium, which lies below the physical layer.

The Data Link Layer

The main task of the data link layer is to take a raw transmission facility and transform it into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break the input data up into data frames (typically a few hundred or a few thousand bytes), transmit the frames sequentially, and process the acknowledgement frames sent back by the receiver. Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning or structure, it is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If these bit patterns can accidentally occur in the data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame delimiters.

A noise burst on the line can destroy a frame completely. In this case, the data link layer software on the source machine can retransmit the frame. However, multiple transmissions of the same frame introduce the possibility of duplicate frames. A duplicate frame could be sent if the acknowledgement frame from the receiver back to the sender were lost. It is up to this layer to solve the problems caused by damaged, lost, and duplicate frames. The data link layer may offer several different service classes to the network layer, each of a different quality and with a different price.

Another issue that arises in the data link layer (and most of the higher layers is well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism must be employed to let the transmitter know how much buffer space the receiver has at the moment. Frequently, this flow regulation and the error handling are integrated. If the line can be used to transmit data in both directions, this introduces a new complication that the data link layer software must deal with. The problem is that the acknowledgement frames for A to B traffic compete for the use of the line with data frames for the B to A traffic. Broadcast networks have an additional issue in the data link layer to control access to the shared channel. A special, sub layer of the data link layer, the medium access sub layer, deals with this problem.

The Network Layer

The network layer is concerned with controlling the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are "wired into" the network and rarely changed. They can also be determined at the start of each conversation, for example a terminal session. Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load. If too many packets are present in the subnet at the same time, they will get in each other's way, forming bottlenecks. The control of such congestion also belongs to the network layer. Since the operators of the subnet may well expect remuneration for their efforts, there is often some accounting function built into the network layer. At the very least, the software must count how many packets or each customer sends characters or bits, to produce billing information. When a packet crosses a national border, with different rates on each side, the accounting can become complicated.

When a packet has to travel from one network to another to get to its destination, many problems can arise. The addressing used by the second network may be different from the first one. The second one may not accept the packet at all because it is too large. The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected. In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

The Transport Layer

The basic function of the transport layer is to accept data from the session layer, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently, and in a way that isolates the upper layers from the inevitable changes in the hardware technology. Under normal conditions, the transport layer creates a distinct network connection for each transport connection required by the session layer. If the transport connection requires a high throughput, however, the transport layer might create multiple network connections, dividing the data among the network connections to improve throughput. On the other hand, if creating or maintaining a network connection is expensive, the transport layer might multiplex several transport connections onto the same network connection to reduce the cost. In all cases, the transport layer is required to make the multiplexing transparent to the session layer.

The transport layer also determines what type of service to provide the session layer, and ultimately, the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent. However, other possible kinds of transport service are transport of isolated messages with no guarantee about the order of delivery, and broadcasting of messages to multiple destinations. The type of service is determined when the connection is established. The transport layer is a true end-to-end layer, from source to destination, in other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages. In the lower layers, the protocols are between each machine and its immediate neighbors, and not by the ultimate source and destination machines, which may be separated by many routers. There is a difference between layers 1 through 3, which are chained, and layers 4 through 7, which are end-to-end. Many hosts are multi-programmed, which implies that multiple connections will be entering and leaving each host. Their needs to be some way to tell which message belong to which connection. The transport header is one place this information can be put.

In addition to multiplexing several message streams onto one channel, the transport layer must take care of establishing and deleting connections across the network. This requires some kind of naming mechanism, so that a process on one machine has a way of describing with whom it wishes to converse. There must also be a mechanism to regulate the flow of information, so that a fast host cannot overrun a slow one. Such a mechanism is called flow control and plays a key role in the transport layer (also in other layers). Flow control between hosts is distinct from flow control between routers, although we will later see that similar principles apply to both.

The Session Layer

The session layer allows users on different machines to establish sessions between them. A session allows ordinary data transport, as does the transport layer, but it also provides enhanced services useful in some applications. A session might be used to allow a user to log into a remote timesharing system or to transfer a file between two machines. One of the services of the session layer is to manage dialogue control. Sessions can allow traffic to go in both directions at the same time, or in only one direction at a time. If traffic can only go one way at a time (analogous to a single railroad track), the session layer can help keep track of whose turn it is.

A related session service is token management. For some protocols, it is essential that both sides do not attempt the same operation at the same time. To manage these activities, the session layer provides tokens that can be exchanged. Only the side holding the token may perform the critical operation. Another session service is synchronization. Consider the problems that might occur when trying to do a 2-hour file transfer between two machines with a 1-hour mean time between crashes. After each transfer was aborted, the whole transfer would have to start over again and would probably fail again the next time as well. To eliminate this problem, the session layer provides a way to insert checkpoints into the data stream, so that after a crash, only the data transferred after the last checkpoint have to be repeated.

The Presentation Layer

The presentation layer performs certain functions that are requested sufficiently often to warrant finding a general solution for them, rather than letting each user solve the problems. In particular, unlike all the lower layers, which are just interested in moving bits reliably from here to there, the presentation layer is concerned with the syntax and semantics of the information transmitted. A typical example of a presentation service is encoding data in a standard agreed upon way. Most user programs do not exchange random binary bit strings. They exchange things such as people's names, dates, amounts of money, and invoices. These items are represented as character strings, integers, floating-point numbers, and data structures composed of several simpler items. Different computers have different codes for representing character strings, integers, and so on. In order to make it possible for computers with different representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and converts from the representation used inside the computer to the network standard representation and back.

The Application Layer

The application layer contains a variety of protocols that are commonly needed. For example, there are hundreds of incompatible terminal types in the world. Consider, the plight of a full screen editor that is supposed to work over a network with many different terminal types, each with different screen layouts, escape sequences for inserting and deleting text, involving the cursor, etc. One way to solve this problem is to define an abstract network virtual terminal that editors and other programs can be written to deal with. To handle each terminal type, a piece of software must be written to map the functions of the network virtual terminal onto the real terminal. For example, when the editor moves the virtual terminal's cursor to the upper left-hand corner of the screen, this software must issue the proper command sequence to the real terminal to get its cursor there too. All the virtual terminal software is in the application layer.

Another application layer function is file transfer. Different file systems have different file naming conventions, different ways of representing text lines, and so on. Transferring a file between two different systems requires handling these and other incompatibilities. This work, too, belongs to the application layer, as do electronic mail, remote job entry, directory lookup, and various other general purpose and special-purpose facilities.

3.1 CHARACTERISTICS OF THE OSI 7 LAYERS MODEL

Layers 7 through 4 deal with end to end communications between data source and destinations. Layers 3 to 1 deal with communications between network devices.

On the other hand, the seven layers of the OSI model can be divided into two groups: upper layers (layers 7, 6 & 5) and lower layers (layers 4, 3, 2, 1). The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the wires, for example) and is responsible for placing data on the medium.

Exercise 3.1.1 Sketch the OSI model and describe the function of the layers with one sentence for each layer.

Answer: OSI is Applications, Presentation, Session, Transport, Network, Data Link, and Physical (top to bottom).
Application – provides access to user applications
Presentation – provides data independence
Session – manages end-to-end connections
Transport – provides reliable end-to-end data transport
Network – maintains point-to-point connections
Data Link – provide reliable point-to-point data transport
Physical – transmission of bit stream

4.0 CONCLUSION

By separating the network communications into logical smaller pieces, the OSI model simplifies how network protocols are designed. The OSI model was designed to ensure different types of equipment (such as network adapters, hubs, and routers) would all be compatible even if built by different manufacturers. A product from one network equipment vendor that implements OSI Layer 2 functionality, for example, will be much more likely to interoperate with another vendor's OSI Layer 3 product because both vendors are following the same model.

5.0 SUMMARY

The OSI model divides the complex task of computer-to-computer communications, traditionally called *internetworking*, into a series of stages known as *layers*. Layers in the OSI model are ordered from lowest level to highest. Together, these layers comprise the OSI stack. The stack contains seven layers in two groups:

Upper layers -

4. transport
3. network
2. data link
1. physical

Lower layers -

7. application
6. presentation
5. session

6.0 TUTOR MARKED ASSIGNMENT

1. Discuss the main characteristics of OSI reference model

2. ___________ are documented agreements containing technical specifications or other precise criteria that stipulate how a particular product or service should be designed or performed.

3. The _________ goals are to promote development and education in the electrical engineering and computer science fields.

4. Addresses used to identify computers on the Internet and other TCP/IP-based networks are known as ___________.

5. The Application layer separates data into ___________, or discreet amounts of data.

6. ___________are added to data at the source and verified at the destination.

7.0 FURTHER READINGS

1. MLA Style Citation:
Yadla, Vijayanand "Seven Layers of ISO OSI Model." Seven Layers of ISO OSI Model. 7 Nov. 2006. *EzineArticles.com*. 14 Aug 2009 <http://ezinearticles.com/?Seven-Layers-of-ISO-OSI-Model&id=349951>.

2. APA Style Citation:
Yadla, V. (2006, November 7). *Seven Layers of ISO OSI Model*. Retrieved August 14, 2009, from http://ezinearticles.com/?Seven-Layers-of-ISO-OSI-Model&id=349951

3. Chicago Style Citation:
Yadla, Vijayanand "Seven Layers of ISO OSI Model." *Seven Layers of ISO OSI Model EzineArticles.com*. http://ezinearticles.com/?Seven-Layers-of-ISO-OSI-Model&id=349951

MODULE 3: OSI AND TCP/IP MODELS

Unit 2: Interaction between OSI model layers protocols

Page

1.0 Introduction 63

2.0 Objectives 63

3.0 Interaction between OSI model layers 63

3.1 Communication between two systems 65

3.2 Benefits of the OSI model 66

4.0 Conclusion 66

5.0 Summary 66

6.0 Tutor Marked Assignment 67

7.0 Further Reading and Other Resources 67

1.0 INTRODUCTION

OSI model, contains seven layers which build on one another. In OSI model, each layer provides specific services and makes the results available to the next layer. Theoretically each layer should be independent of all others, but this is a simplistic notion.

2.0 OBJECTIVE

The main objectives of this unit are to :

- Describe the interaction between OSI model layers protocols
- Explain communications among the OSI layers
- Discuss the benefits of the OSI model

3.0 INTERACTION BETWEEN OSI MODEL LAYERS PROTOCOLS

To picture the physical path that data takes from one computer to another, consider that a user or device first initiates a data exchange through the Application layer The application layer separates data into protocol data units (PDUs), or discreet amounts of data.

Application Layer

The top, or seventh, layer or the OSI Model is the Application layer. Application layer services communicate between software programs and lower-layer network services so that the network can properly interpret an application's request and, in turn, the application can interpret data sent from the network. For example, when you choose to open a Web page in Netscape, an Application layer protocol called HTTP (Hypertext Transfer Protocol) formats and sends your request, then formats and sends the Web server's response.

Presentation Layer

Protocols at the Presentation layer accept Application layer data and format it so that one type of application and host can understand data from another type of application and host. Presentation layer services also manage data encryption (such as the scrambling of passwords) and decryption.

Session Layer

Protocols in the Session layer coordinate and maintain communications between two nodes on the network. The term **session** refers to a connection for ongoing data exchange between two parties; it is most often used in the context of terminal and mainframe communications, in which the terminal is a device with little (if any) of its own processing or disk capacity that depends on a host to supply it with software and processing services. Among the Session layer's functions are establishing and keeping alive the communications link for the duration of the session, keeping the communication secure, synchronizing the dialog between the two nodes, determining whether communications have been cut off, and, if so, figuring out where to restart transmission, and terminating communications.

Transport Layer

Protocols in the Transport layer accept data from the Session layer and manage end-to-end delivery of data. That means they can ensure that the data is transferred from point A to point B reliably, in the correct sequence, and without errors. Without Transport layer services, data could not be verified or interpreted by its recipient. Transport layer protocols also handle flow control, which is the process of gauging the appropriate rate of transmission based on how fast the recipient can accept data.

Some Transport layer protocols take steps to ensure that data arrives exactly as it was sent. Such protocols are known as connection-oriented, because they establish a connection with another node before they begin transmitting data. The Web server responds with an acknowledgement (ACK), or a confirmation, to indicate that it's willing to make a connection. To ensure data integrity further, connection-oriented protocols such as TCP use a checksum, or a method of error checking that determines if the contents of an arriving data unit match the contents of the data unit sent by the source.

Not all Transport layer protocols are concerned with reliability. Those that do not establish a connection before transmitting and make no effort to ensure that data is delivered error-free are called connectionless protocols. A connectionless protocol's lack of sophistication makes it more efficient than a connection-oriented protocol and renders it useful in situations where data must be transferred quickly, such as live audio or video transmissions over the Internet.

In addition to ensuring reliable data delivery, Transport layer protocols break large data units received from the Session layer into multiple smaller units, called segments. This process is known as segmentation. On certain types of networks, segmentation increases data transmission efficiency. In some cases segmentation is necessary for data units to match a network's maximum transmission unit (MTU), the largest data unit it will carry.

Segmentation is similar to the process of breaking down words into recognizable syllables that a child uses when learning to read. Reassembly is the process of reconstructing the segmented data units.

Network Layer

The primary function of protocols at the Network layer is to translate network addresses into their physical counterparts and decide how to route data from the sender to the receiver. One type of address that nodes use is called a network layer address. Network layer addresses follow a hierarchical addressing scheme and can be assigned through operating system software. Network layer addresses are also called logical addresses or virtual addresses.

On TCP/IP-based networks, Network layer protocols can perform an additional function called fragmentation. In fragmentation a Network layer protocol (such as IP) subdivides the segments it receives from the Transport layer into smaller packets.

Data Link Layer

The primary function of protocols in the second layer of the OSI Model, the Data Link layer**,** is to divide data they receive from the Network layer into distinct frames that can then be transmitted by the Physical layer. A frame is a structured package for moving data that includes not only the raw data, or "payload," but also the sender's and receiver's network addresses, and error checking and control information.

Error checking is accomplished by a 4-byte Frame Check Sequence (FCS) field, whose purpose is to ensure that the data at the destination exactly matches the data issued from the source. When the source node transmits the data, it performs an algorithm called a Cyclic Redundancy Check (CRC)**.**

The upper sublayer of the Data Link layer, called the Logical Link Control (LLC) sublayer, provides an interface to the Network layer protocols, manages flow control, and issues requests for transmission for data that has suffered errors. The Media Access Control (MAC) sublayer, the lower sublayer of the Data Link layer, manages access to the physical medium. It appends the physical address of the destination computer onto the data frame. The physical address is a fixed number associated with a device's NIC; it is initially assigned at the factory and stored in the NIC's on-board memory. Because this address is appended by the MAC sublayer of the Data Link layer, it also is known as a MAC address. Sometimes it's also called a hardware address**.** MAC addresses contain two parts: a Block ID and a Device ID. The Block ID is a six-character sequence unique to each vendor.

Physical Layer

The Physical layer is the lowest, or first, layer of the OSI Model. Protocols at the Physical layer accept frames from the Data Link layer and generate voltage so as to transmit signals. When receiving data, Physical layer protocols detect voltage and accept signals, which they pass on to the Data Link layer.

3.1 COMMUNICATION BETWEEN TWO SYSTEMS

At each layer of the OSI Model, some information—for example, a format specification or a network address—is added to the original data. After it has followed the path from the Application layer to the Physical layer, data is significantly transformed.

Frame Specifications

The two major categories of frame types, Ethernet and Token Ring, correspond to the two most commonly used network technologies. Ethernet is a networking technology originally developed at Xerox in the early 1970s and improved by Digital Equipment Corporation, Intel, and Xerox. There are four different types of Ethernet frames. The most popular form of Ethernet is characterized by the unique way in which devices share a common transmission channel, described in the IEEE 802.3 standard.

Token Ring is a networking technology developed by IBM in the 1980s. It relies upon direct links between nodes and a ring topology. Nodes pass around tokens, special control frames that indicate to the network when a particular node is about to transmit data. The IEEE has defined Token Ring technology in its 802.5 standard.

IEEE Networking Specifications

In addition to frame types and addressing, IEEE networking specifications apply to connectivity, networking media, error checking algorithms, encryption, emerging technologies, and more.

3.2 BENEFITS OF THE OSI MODEL

By separating the network communications into logical smaller pieces, the OSI model simplifies how network protocols are designed. The OSI model was designed to ensure different types of equipment (such as network adapters, hubs, and routers) would all be compatible even if built by different manufacturers. A product from one network equipment vendor that implements OSI Layer 2 functionality, for example, will be much more likely to interoperate with another vendor's OSI Layer 3 product because both vendors are following the same model.

The OSI model also makes network designs more extensible as new protocols and other network services are generally easier to add to a layered architecture than to a monolithic one.

4.0 CONCLUSION

In the Open Systems Interconnection (OSI) communications model, each layer knows the address of the neighboring nodes in the network, packages output with the correct network address information, selects routes and quality of service, and recognizes and forwards to the next layer.

5.0 SUMMARY

In this unit we have been able to :

- Describe the interaction between OSI model layers protocols
- Explain communications among the OSI layers
- Discuss the benefits of the OSI model

6.0 TUTOR MARKED ASSIGNMENT

1 Explain the interaction among the various layers of the OSI model

7.0 FURTHER READINGS

[Kurose, Ross] “Computer Networking”, J.F. Kurose and K.W. Ross, Addison Wesley, 2000

MODULE 3: OSI AND TCP/IP MODELS

Unit 3: Transmission Control Protocol/ Internet Protocol (TCP/IP) model

Page

1.0 Introduction 69

2.0 Objectives 69

3.0 TCP/IP model 69

3.1 Comparison between TCP/IP and OSI models 72

4.0 Conclusion 74

5.0 Summary 74

6.0 Tutor Marked Assignment 75

7.0 Further Reading and Other Resources 75

1.0 INTRODUCTION

TCP/IP is an industry standard set of protocols developed by the U.S. Department of Defense Advanced Research Projects Agency (DARPA) in 1969. It maps TCP/IP protocols to a four-layer conceptual model known as the *DARPA model*. It is often compared to the still born OSI Protocol Layers. The four layers of the DARPA model are: Internet, Transport, Application and, *Host-to-Network* .

2.0 OBJECTIVES

At the end of this unit student should be able to:

- Understand the workings of TCP/IP model
- Distinguish between the OSI model and TCP/IP model
- Explain the functions of the four layers of TCP/IP model

3.0 TCP/IP MODEL

Let us now turn from the OSI reference model to the reference model used in the grandparent of all computer networks, the ARPANET, and its successor, the worldwide Internet. The ARPANET was a research network sponsored by the DOD (U.S Department of Defense). It eventually connected hundreds of universities and government installations using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble inter-working with them, so new reference architecture was needed. Thus the ability to connect multiple networks together in a seamless way was one of the major design goals from the very beginning. This architecture later became known as the TCP/IP Reference Model, after its two primary protocols.

Given the DOD's worry that some of its precious hosts, routers, and internet work gateways might get blown to pieces at a moment's notice, another major goal was that the network be able to survive loss of subnet hardware, with existing conversations not being broken off. In other words, DOD wanted connections to remain intact as long as the source and destination machines were functioning, even if some of the machines or transmission lines in between were suddenly put out of operation. Furthermore, a flexible architecture was needed, since applications with divergent requirements were envisioned, ranging from transferring files to real-time speech transmission.

The Internet Layer

All these requirements led to the choice of a packet-switching network based on a connectionless Internet work layer. This layer, called the Internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.

Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The analogy here is with the mail system. A person can drop a sequence of international letters into a mailbox in one country, and with a little luck, most of them will be delivered to the correct address in the destination country. Probably the letters will travel through one or more international mail gateways along the way, but this is transparent to the users. Furthermore, that each country has its own stamps, preferred envelope sizes, and delivery rules is hidden from the users. The Internet layer defines an official packet format and protocol called IP (Internet Protocol). The job of the Internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP Internet layer is very similar in functionality to the OSI network layer. Figure 3.3.1 shows this correspondence.

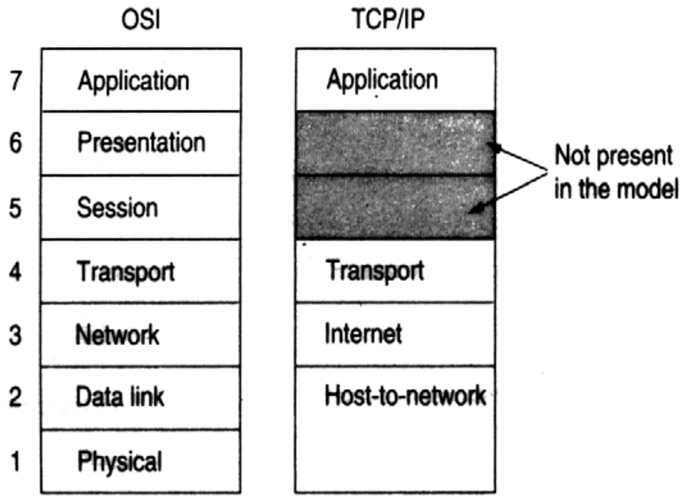


Fig. 3.3.1 - The TCP/IP Reference Model

Source: http://www.ietf.org/rfc.html

T*ransport Layer*

The layer above the Internet layer in the TCP/IP model is now usually called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, the same as in the OSI transport layer. Two end-to-end protocols have been defined here. The first one, TCP (Transmission Control Protocol) is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the Internet. It fragments the incoming byte stream into discrete messages and passes each one onto the Internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

The second protocol in this layer, UDP (User Data gram Protocol), is an unreliable, connectionless protocol for. Applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP . Since the model was developed, IP has been implemented on many other networks.

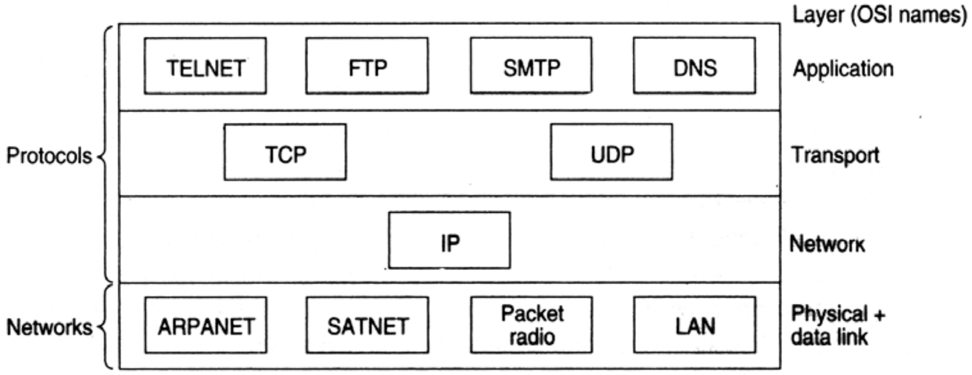


Fig. 3.3.2 - Protocols and Networks in the TCP/IP Model Initially

Source: http://www.faqs.com

The Application Layer

The TCP/IP model does not have session or presentation layers. No need for them was 'perceived, so they were not included. Experience with the OSI model has proven this view correct: they are of little use to most applications.

On top of the transport layer is the application layer. It contains all the Higher Level Protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP). The virtual terminal protocol allows a user on one machine to log into a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol was developed for it. Many other proto- cols have been added to these over the years, such as the Domain Name Service (DNS) for mapping host names onto their network addresses, NNTP, the protocol used for moving news articles around, and HTTP, the protocol used for fetching pages on the World Wide, and many others.

The Host-to-Network Layer

Below the Internet layer is a great void. The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets over it. This protocol is not defined and varies from host to host and network to network. Books and papers about the TCP/IP model rarely discuss it.

3.1 COMPARISON BETWEEN TCP/IP AND OSI

Like OSI network model, TCP/IP also has a network model. TCP/IP was on the path of development when the OSI standard was published and there was interaction between the designers of OSI and TCP/IP standards. The TCP/IP model is not same as OSI model. OSI is a seven-layered standard, but TCP/IP is a four layered standard. The OSI model has been very As we can see from the above figure, presentation and session layers are not there in OSI model. Also note that the Network Access Layer combines the functions of Datalink Layer and Physical Layer.

influential in the growth and development of TCP/IP standard, and that is why much OSI terminology is applied to TCP/IP. The following figure compares the TCP/IP and OSI network models.

Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Datalink Layer	Network Access Layer
Physical Layer	

Fig. 3.3.3 Comparison between seven layer OSI and four layer TCP/IP Models

Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation.

Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protoco).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport Layer. Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as internet layer, is the linchpin that holds the whole design together. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Exercise 3.3.1 What are the four causes, or components, of delay in a packet switched network? What can be done to reduce each of these components?

Answer: The delay components are Processing, queueing, transmission, and propagation. Processing delay can be reduced by
faster CPUs, queueing and transmission delay by faster links, and propagation delay only by moving content closer to its
user.

Exercise 3.3.2 What is the purpose of hierarchical address in the Internet (i.e., why are IP addresses hierarchical)? Explain how the hierarchical address is used in IP routing.

Answer: By having an IP address hierarchical as network-host, we can reduce the size of routing tables by having routing tables only handle forwarding from network to network. Only at the destination network is the host address portion used for delivering the packet to the destination host.

4.0 CONCLUSION

In this lesson, you have learned about the four layers of TCP/IP model and the comparison between four layered TCP/IP model and seven layered OSI model. TCP/IP model is a four-layered structure resting on a common hardware platform. It was initially developed for DARPA and sometimes called DARPA model. TCP/IP model has standards that are defined and described in Request for Comment (RFC) documents.

5.0 SUMMARY

In this unit we have been able to:

- Distinguish between the OSI model and TCP/IP model
- Discuss the workings of TCP/IP model
- Explain the functions of the four layers of TCP/IP model

6.0 TUTOR MARKED ASSIGNMENT

1. Distinguish between the OSI model and TCP/IP model.

2. What are the functions of the four layers of TCP/IP model.

7.0 FURTHER READINGS

1. TCP/IP Illustrated Volume 1 by R.W. Stevens, 1994[4],
2. TCP/IP Network Administration by C. Hunt, 2002[5].

MODULE 4: TYPES OF NETWORK, TRANSMISSION MEDIA, ADDRESSING AND TROBLESHOOTING

Unit 1: Local Area Network (LAN)

		Page
1.0	Introduction	77
2.0	Objectives	77
3.0	Local Area Network	77
3.1	Major characteristics of LAN	77
3.2	Components of LAN	78
3.3	LAN topologies	81
3.3.1	Bus topology	81
3.3.2	Tree topology	82
3.3.3	Star topology	83
3.3.4	Ring topology	83
4.0	Conclusion	84
5.0	Summary	84
6.0	Tutor Marked Assignment	84
7.0	Further Reading and Other Resources	84

1.0 INTRODUCTION

Today when we speak of networks, we are generally referring to three primary categories: local area networks, metropolitan area networks, and wide area networks. A network consists of two or more computers that are linked in order to share resources (such as printers and CD-ROMs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

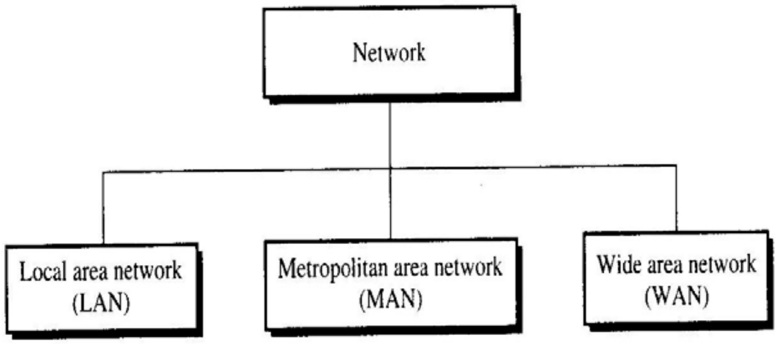


Fig. 4.1.1 - Categories of networks

2.0 OBJECTIVES

The purpose of this unit are as follows:

- to assist students understanding the concept of local area network
- to discuss the major characteristics of LANs
- to describe various components of LANs
- to deepen students understating of LAN topologies

3.0 LOCAL AREA NETWORK

The Local Area Network (LAN) is by far the most common type of data network. As the name suggests, a LAN serves a local area (typically the area of a floor of a building, but in some cases spanning a distance of several kilometers). Typical installations are in industrial plants, office buildings, college or university campuses, or similar locations. In these locations, it is feasible for the owning Organisation to install high quality, high-speed communication links interconnecting nodes. Typical data transmission speeds are one to 100 megabits per second.

3.1 MAJOR CHARACTERISTICS OF LANs

Major characteristics of LANs are**:**

- The network operates within a building or floor of a building. The geographic scope for ever more powerful LAN desktop devices running more powerful applications is for less area per LAN.

- LANs provide multiple connected desktop devices (usually PCs) with access to high-bandwidth media.

- An enterprise purchases the media and connections used in the LAN; the enterprise can privately control the LAN as it chooses.

- LANs rarely shut down or restrict access to connected workstations; local services are usually always available.

- By definition, the LAN connects physically adjacent devices on the media.

3. 2 COMPONENTS OF LAN

- Network operating system(NOS)

In order for computers to be able to communicate with each other, they must first have the networking software that tells them how to do so. Without the software, the system will function simply as a "standalone," unable to utilize any of the resources on the network. Network operating software may by installed by the factory, eliminating the need for you to purchase it, (for example AppleTalk), or you may install it yourself.

- Network interface card(NIC)

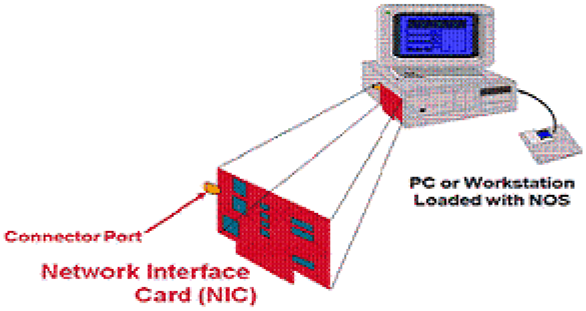


Fig. 4.1.2 Network interface card

In addition to network operating software, each network device must also have a network interface card. These cards today are also referred to as adapters, as in "Ethernet adapter card" or "Token Ring adapter card." The NIC card amplifies electronic signals which are generally very weak within the computer system itself. The NIC is also responsible for packaging data for transmission, and for controlling access to the network cable. When the data is packaged properly, and the timing is right, the NIC will push the data stream onto the cable. The NIC also provides the physical connection between the computer and the transmission cable (also called "media"). This connection is made through the connector port. Examples of transmission media are Ethernet, Token Ring, and FDDI.

Wiring Hub

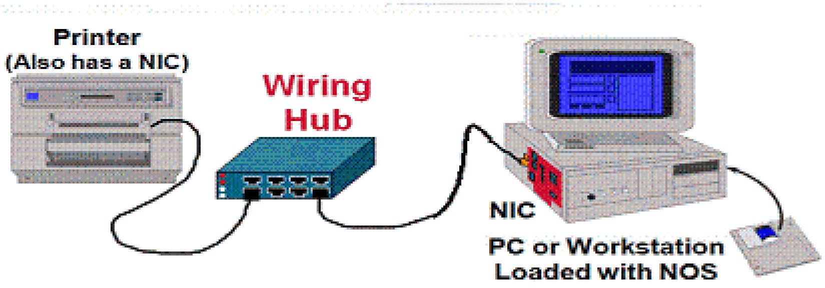


Fig. 4.1.3 Wiring Hub

In order to have a network, you must have at least two devices that communicate with each other. In this simple model, it is a computer and a printer. The printer also has an NIC installed (for example, an HP Jet Direct card), which in turn is plugged into a wiring hub. The computer system is also plugged into the hub, which facilitates communication between the two devices. Additional components (such as a server, a few more PCs, and a scanner) may be connected to the hub. With this connection, all network components would have access to all other network components. The benefit of building this network is that by sharing resources a company can afford higher quality components. For example, instead of providing an inkjet printer for every PC, a company may purchase a laser printer (which is faster, higher capacity, and higher quality than the inkjet) to attach to a network. Then, all computers on that network have access to the higher quality printer.

- Cables or Transmission Media

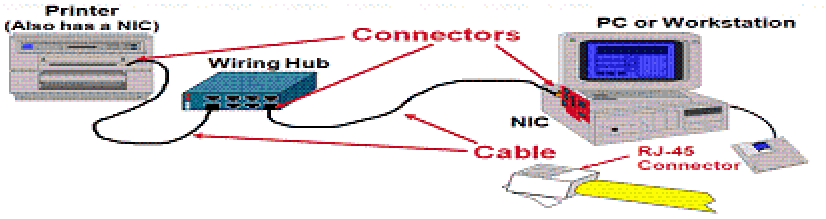


Fig. 4.1.4 Cable Or Transmission Media

The wires connecting the various devices together are referred to as cables.

- Cable prices range from inexpensive to very costly and can comprise of a significant cost of the network itself.

- Cables are one example of transmission media. Media are various physical environments through which transmission signals pass. Common network media include twisted-pair, coaxial cable, fiber-optic cable, and the atmosphere (through which microwave, laser, and infrared transmission occurs). Another term for this is "physical media." *Note that not all wiring hubs support all medium types.

The other component shown in this figure is the connector.

- As their name implies, the connector is the physical location where the NIC card and the cabling connect.

- Registered jack (RJ) connectors were originally used to connect telephone lines. RJ connectors are now used for telephone connections and for 10BaseT and other types of network connections. Different connectors are able support different speeds of transmission because of their design and the materials used in their manufacture.

- RJ-11 connectors are used for telephones, faxes, and modems. RJ-45 connectors are used for NIC cards, 10BaseT cabling, and ISDN lines.

Throughput Needs....!!

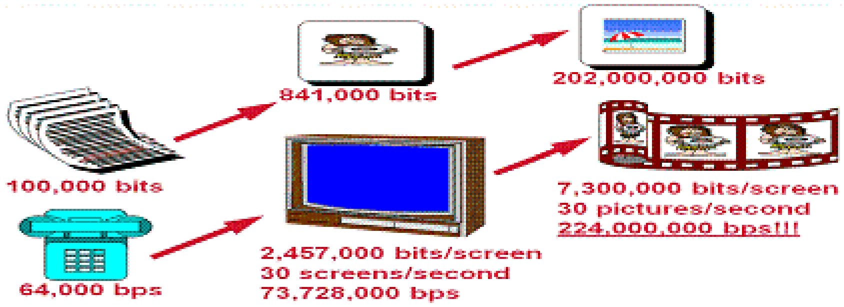


Fig. 4.1.5 Throughput Needs

Super servers, high-capacity workstations, and multimedia applications have also fueled the need for higher capacity bandwidths. The examples on above image shows that the need for throughput capacity grows as a result of a desire to transmit more voice, video, and graphics. The rate at which this information may be sent (transmission speed) is dependent how data is transmitted and the medium used for transmission. The "how" of this equation is satisfied by a transmission protocol. Each protocol runs at a different speed. Two terms are used to describe this speed: throughput rate and bandwidth. The throughput rate is the rate of information arriving at, and possibly passing through, a particular point in a network. In this unit, the term bandwidth means the total capacity of a given network medium (twisted pair, coaxial, or fiber-optic cable) or protocol.

- Bandwidth is also used to describe the difference between the highest and the lowest frequencies available for network signals. This quantity is measured in Megahertz (MHz).

- The bandwidth of a given network medium or protocol is measured in bits per second (bps). Some of the available bandwidth specified for a given medium or protocol is used up in overhead, including control characters. This overhead reduces the capacity available for transmitting data.

Table 4.1.1: Table showing the tremendous variation in transmission time with different throughput rates

Speed		Transmit Time
9.6000 bps	=	12.27 hrs
24.000 bps	=	4.91 hrs
56 Kbps	=	2.1 hrs
1 Mbps	=	7.1 min
10 Mbps	=	42.4 sec
100 Mbps	=	4.24 sec
1 Gbps	=	0.42 sec

This table shows the tremendous variation in transmission time with different throughput rates. In years past, megabit (Mb) rates were considered fast. In today's modern networks, gigabit (Gb) rates are possible. Nevertheless, there continues to be a focus on greater throughput rates.

3.3 LAN TOPOLOGIES

You may hear the word topology used with respect to networks. "Topology" refers to the physical arrangement of network components and media within an enterprise networking structure. There are four primary kinds of LAN topologies: bus, tree, star, and ring.

3.3.1 Bus topology

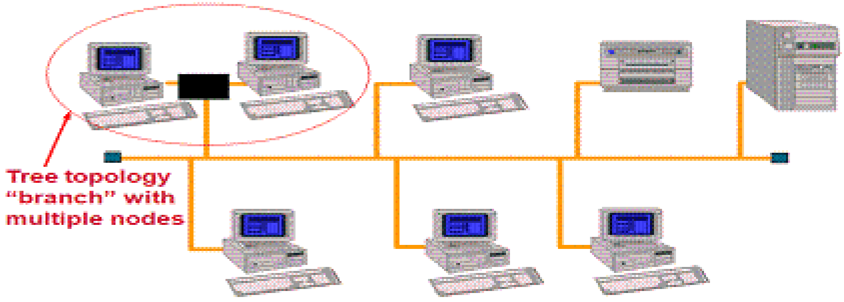


FIG. 4.1.6 Bus topology

Bus topology is

- A linear LAN architecture in which transmissions from network components propagate the length of the medium and are received by all other components.
- The bus portion is the common physical signal path composed of wires or other media across which signals can be sent from one part of a network to another. Sometimes called a highway.

- Ethernet/IEEE 802.3 networks commonly implement a bus topology

The disadvantage of bus topology is that if the connection to any one user is broken, the entire network goes down, disrupting communication between all users. Because of this problem, bus topology is rarely used today. The advantage of bus topology is that it requires less cabling (therefore, lower cost) than star topology.

3.3.2 Tree topology

Tree topology is

- Similar to bus topology, except that tree networks can contain branches with multiple nodes. As in bus topology, transmissions from one component propagate the length of the medium and are received by all other components.

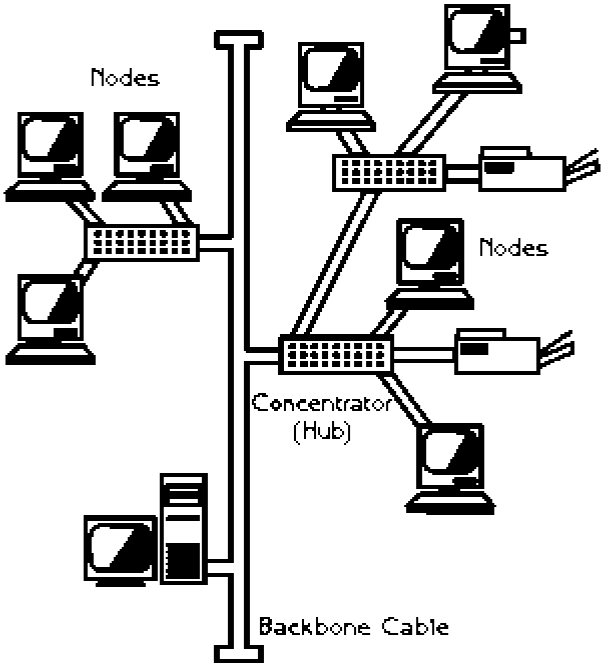


Fig. 4.1.7 Tree topology

3.3.3 Star topology

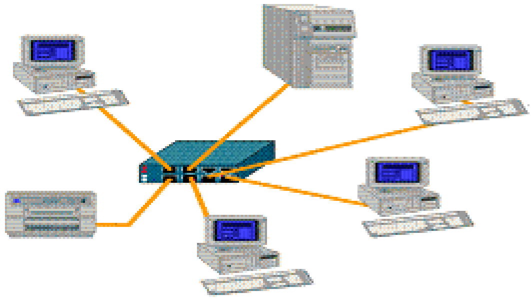


Fig. 4.1.8 Star topology

Star topology is a LAN topology in which endpoints on a network are connected to a common central switch or hub by point-to-point links. Logical bus and ring topologies re often implemented physically in a star topology.

- The benefit of star topology is that even if the connection to any one user is broken, the network stays functioning, and communication between the remaining users is not disrupted.
- The disadvantage of star topology is that it requires more cabling (therefore, higher cost) than bus topology.

3.3.4 Ring topology

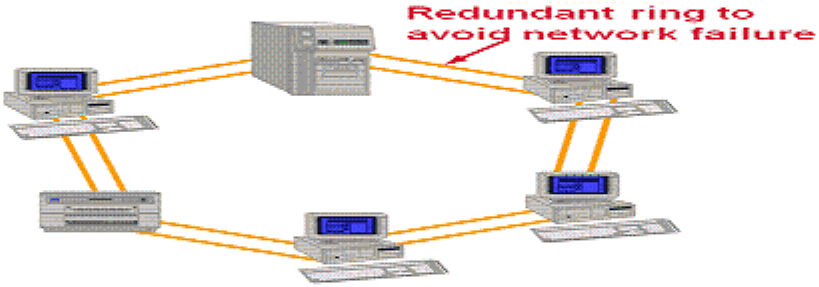


Fig. 4.1.9 Ring topology

Ring topology consists of a series of repeaters connected to one another by unidirectional transmission links to form a single closed loop.

- Each station on the network connects to the network at a repeater.
- While logically a ring, ring topologies are most often organized in a closed-loop star. A ring topology that is organized as a star implements a unidirectional closed-loop star, instead of point-to-point links.

-One example of a ring topology is Token Ring.

-Redundancy is used to avoid collapse of the entire ring in the event that a connection between two components fails.

Exercise 4.1.1 What is a Local Area Network (LAN)?

Answer: Very precisely, a LAN is a data network optimized for a medium-sized area with 10’s to 100’s of stations and 100’s to 1000’s of meter span. A LAN is owned, operated, and used by a single organization.

4.0 CONCLUSION

The term local-area network, or LAN, describes of all the devices that communicate together—printers, file server, computers, and perhaps even a host computer. However, the LAN is constrained by distance. The transmission technologies used in LAN applications do not operate at speed over long distances. LAN distances are in the range of 100 meters (m) to 3 kilometers (km). This range can change as new technologies emerge. For systems from different manufacturers to interoperate—be it a printer, PC, and file server—they must be developed and manufactured according to industry-wide protocols and standards.

5.0 SUMMARY

In this unit we have been able to establish the facts that:

- LANs are designed to operate within a limited geographic area
- Key LAN components are computers, NOS, NICs, hubs, and cables
- Common LAN topologies include bus, tree, star, and ring
- Common LAN devices are hubs, bridges, switches, and routers

6.0 TUTOR MARKED ASSIGNMENT

1. Describe what a Local Area Network is.
2. Describe the different types of LANs.
3. Describe some of the key components of a network system.
4. State some of the benefits LAN technology offers to system users.

7.0 FURTHER READINGS

1. Computer Networks by A.S. Tanenbaum, 2003[2],
2. Computer Networks by P.J. Irving, 2003[3],
3. Ed, T. Theory and Problems of Computer Networking. USA: Schaum's Outline Series, McGRAW-HILL, 2002.

Source of diagrams used in this unit: Computer Networks by A.S. Tanenbaum, 2003[2], and . Computer Networks by P.J. Irving, 2003[3],

MODULE 4: TYPES OF NETWORK, TRANSMISSION MEDIA, ADDRESSING AND TROBLESHOOTING

Unit 2: Metropolitan Area Network(MAN) and Wide Area Network(WAN)

		Page
1.0	**Introduction**	**86**
2.0	**Objectives**	**86**
3.0	**Metropolitan Area Network**	**86**
3.1	**MAN Protocols and Topology**	**87**
3.2	**Wide Area Network**	**88**
3.3	**WAN topologies**	**89**
4.0	**Conclusion**	**92**
5.0	**Summary**	**92**
6.0	**Tutor Marked Assignment**	**92**
7.0	**Further Reading and Other Resources**	**92**

1.0 INTRODUCTION

Metropolitan Area network is a combination of two or more individual Local Area Networks but with a small criterion of the boundary of the network not exceeding the city limits, thus integrating the network as a single unit within a city. Wide Area Network is basically an extension of the Local Area Network except for the fact that the size of the network extends to a very large area. The major functionality of the WAN networks take place at the 3 lower layers of the OSI model namely network layer, data link layer and the physical layer.

2.0 OBJECTIVES

The purpose of this unit are as follows:

- to assist students understanding the concepts of metropolitan area network(MAN) and wide area network (WAN)
- to discuss the major characteristics of MAN and WAN
- to deepen students understating of MAN and WAN topologies

3.0 METROPOLITAN AREA NETWORK AND MAN PROTOCOLS

Metropolitan Area Network(MAN) is a computer networks usually spanning a campus or a city, which typically connect a few local area networks using high speed backbone technologies. A MAN often provides efficient connections to a wide area network (WAN). There are three important features which discriminate MANs from LANs or WANs:

1. The network size falls intermediate between LANs and WANs. A MAN typically covers an area of between 5 and 50 km range. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings.
2. A MAN (like a WAN) is not generally owned by a single organisation. The MAN, its communications links and equipment are generally owned by either a consortium of users or by a network service provider who sells the service to the users.
3. A MAN often acts as a high speed network to allow sharing of regional resources. It is also frequently used to provide a shared connection to other networks using a link to a WAN.

MAN adopted technologies from both LAN and WAN to serve its purpose. Some legacy technologies used for MAN are ATM, FDDI, DQDB and SMDS. These older technologies are in the process of being displaced by Gigabit Ethernet and 10 Gigabit Ethernet. At the physical level, MAN links between LANs have been built on fiber optical cables or using wireless technologies such as microwave or radio.

A typical use of MANs to provide shared access to a wide area network is shown in the figure below:

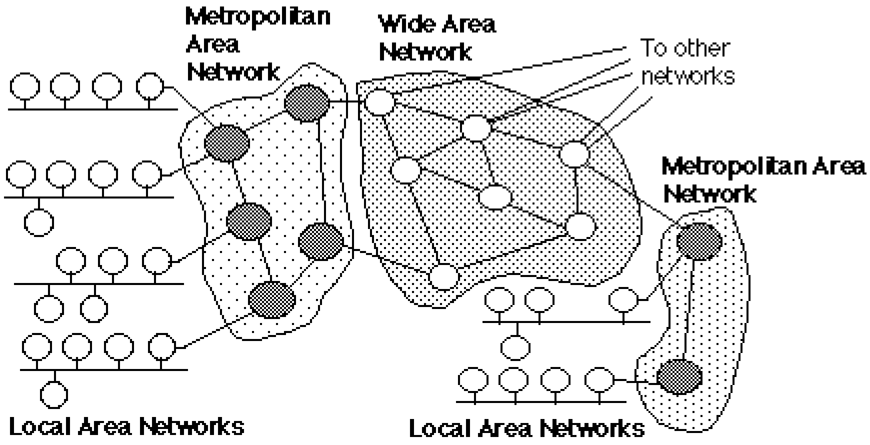


Fig. 4.2.1 Use of MANs to provide regional networks which share the cost of access to a WAN

3.1 MAN PROTOCOLS AND TECHNOLOGY

The key MAN protocols and technologies are listed as follows:

ATM: Asynchronous Transfer Mode Protocol

The Asynchronous Transfer Mode (ATM) composes a protocol suite which establishes a mechanism to carry all traffic on a stream of fixed 53-byte packets (cells). A fixed-size packet can ensure that the switching and multiplexing function could be carried out quickly and easily. ATM is a connection-oriented technology, i.e.; two systems on the network should inform all intermediate switches about their service requirements and traffic parameters in order to establish communication.

The ATM reference model, which has two forms - one for the user-to-network interface (UNI) and the other for the network-to-node interface (NNI), is divided into three layers: the ATM adaptation layer (AAL), the ATM layer, and the physical layer. The AAL interfaces the higher layer protocols to the ATM Layer, which relays ATM cells both from the upper layers to the ATM Layer and vice versa. When relaying information received from the higher layers, the AAL segments the data into ATM cells. When relaying information received from the ATM Layer, the AAL must reassemble the payloads into a format the higher layers can understand. This is called Segmentation and Reassembly (SAR). Different AALs are defined in supporting different types of traffic or service expected to be used on ATM networks.

The ATM layer is responsible for relaying cells from the AAL to the physical layer for transmission and from the physical layer to the AAL for use at the end systems, it determines where the incoming cells should be forwarded to, resets the corresponding connection identifiers and forwards the cells to the next link, as well as buffers cells, and handles various traffic management functions such as cell loss priority marking, congestion indication, and generic flow control access. It also monitors the transmission rate and conformance to the service contract (traffic policing).

The physical layer of ATM defines the bit timing and other characteristics for encoding and decoding the data into suitable electrical/optical waveforms for transmission and reception on the specific physical media used. In addition, it also provides frame adaptation function, which includes cell delineation, header error check (HEC) generation and processing, performance monitoring, and payload rate matching of the different transport formats used at this layer. SONET , DS3, Fiber, twisted-pair are few media often used at the physical layer.

DQDB: Distributed Queue Dual Bus Defined in IEEE 802.6

Data Over Cable Service Interface Distributed Queue Dual Bus (DQDB) is a Data-link layer communication protocol for Metropolitan Area Networks (MANs), specified in the IEEE 802.6 standard, designed for use in MANs. DQDB is designed for data as well as voice and video transmission based on cell switching technology (similar to ATM). DQDB, which permits multiple systems to interconnect using two unidirectional logical buses, is an open standard that is designed for compatibility with carrier transmission standards such as SMDS, which is based on the DQDB standards.

For a MAN to be effective it requires a system that can function across long, city-wide distances of several miles, have a low susceptibility to error, adapt to the number of nodes attached and have variable bandwidth distribution. Using DQDB, networks can be thirty miles long and function in the range of 34 Mbps to 155 Mbps. The data rate fluctuates due to many hosts sharing a dual bus as well as the location of a single host in relation to the frame generator, but there are schemes to compensate for this problem making DQDB function reliably and fairly for all hosts.

The DQDB is composed of a two bus lines with stations attached to both and a frame generator at the end of each bus. The buses run in parallel in such a fashion as to allow the frames generated to travel across the stations in opposite directions.

3.2 WIDE AREA NETWORK (WAN)

A WAN is a network that traverses some distance and usually connects LANs, whether across the city or across the nation. Most WANs arise from the simple need to connect one building to another. WANs and LANs are similar in some fundamental ways. They both are designed to enable communication between clients and hosts for resource sharing. However, LANs and WANs often differ at Layers 1 and 2 of the OSI Model, in access methods, topologies, and sometimes, media. They also differ in the extent to which the organization that uses the network is responsible for the network. The individual geographic locations connected by a WAN are known as WAN sites. A WAN link is a connection between one WAN site (or point) and another site (or point).

In a WAN the machines (usually called hosts) are connected by a communication subnet or simply a subnet. The job of the subnet is to carry messages from one host to another and consists of two main components: transmission lines (also called channels, circuits or trunks) to move bits from one location to another and switching elements (also called packet switching nodes or routers) which switch packets from one transmission channel to another. A router is a special computer dedicated to switching packets. If it is required to send a packet between to routers for which there is no direct link, then the packet is routed via intermediate routers. As the packet is received at an intermediate router it is stored until the packet has arrived in its entirety and then forwarded to the next router as soon as a transmission channel becomes free. Such systems are thus often called store and forward or packet-switched subnets.

Of course in most WANs rather than a single host being connected to a router on the subnet, a whole LAN is connected to the subnet at this point as shown in the diagram overleaf. Also on some WANs the distinction between hosts and routers is blurred as some hosts can also act as routers. However technically the term subnet is reserved for the case where no hosts are present.

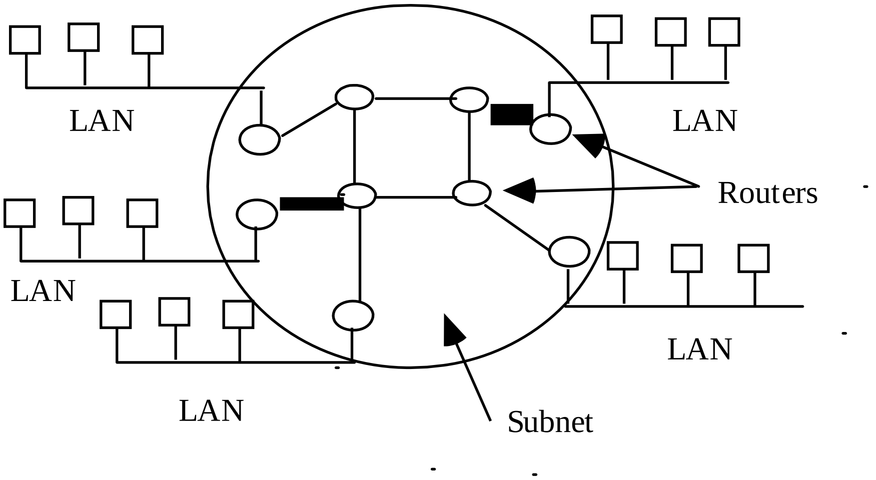


Fig. 4.2.2 Wide Area Network

3.4 WAN TOPOLOGIES

WAN topologies resemble LAN topologies, but their details differ because of the distance they must cover, the larger number of users they serve, and the heavy traffic they often handle.

Bus

A WAN in which each site is directly connected to no more than two other sites in a serial fashion is known as a bus topology WAN**.** A bus topology WAN is similar to a bus topology LAN in that each site depends on every other site in the network to transmit and receive its traffic. However, bus topology LANs use computers with shared access to one cable.

Ring

In a ring topology WAN**,** each site is connected to two other sites so that the entire WAN forms a ring pattern. This architecture is similar to the simple ring topology used on a LAN, except that a WAN ring topology connects locations rather than local nodes and in most WANs, a ring topology uses two parallel paths for data.

Star

The star topology WAN mimics the arrangement of a star topology LAN. A single site acts as the central connection point for several other points. This arrangement provides separate routes for data between any two sites. That means that if a single connection fails, only one location loses WAN access. As with star LAN topologies, the greatest drawback of a star WAN is that a failure at the central connection point can bring down the entire WAN.

Mesh

A mesh topology WAN incorporates many directly interconnected sites. Because every site is interconnected, data can travel directly from its origin to its destination. The type of mesh topology in which every WAN site is directly connected to every other site is called a full mesh WAN**.** One drawback to a full mesh WAN is the cost. To reduce costs, a network administrator might choose to implement a partial mesh WAN, in which only critical WAN sites are directly interconnected and secondary sites are connected through star or ring topologies.

Tiered

In a **tiered topology WAN,** sites connected in star or ring formations are interconnected at different levels, with the interconnection points being organized into layers to form hierarchical groupings.

PSTN

PSTN, which standard for Public Switched Telephone Network, refers to the network of typical telephone lines and carrier equipment that service most homes. PSTN may also be called plain old telephone service (POTS). The PSTN comprises the entire telephone system, from the lines that connect homes and businesses to the network centers that connect different regions of a country. A dial-up connection is one in which a user connects, via a modem, to a distant network from a computer and stays connected for a finite period of time. Most of the time, the term dial-up refers to a connection that uses a PSTN line.

The portion of the PSTN that connects your house to the nearest central office is known as the local loop**,** or the last mile. The advantages to using the PSTN are is ubiquity, ease of use, and low cost. However, the PSTN comes with significant disadvantages. Most limiting is its low throughput. Currently, manufacturers of PSTN modems advertise a connection speed of 56 Kbps. However, the 56-Kbs maximum is only a *theoretical* threshold that assumes that the connection between the initiator and the receiver is pristine.

X.25 and Frame Relay

X.25 is an analog, packet-switched technology designed for long-distance data transmission and standardized by the ITU in the mid-1970s. The original standard for X.25 specified a maximum of 64-Kbps throughput, but by 1992 the standard was updated to include maximum throughput of 2.048 Mbps.

Frame Relay is an updated, digital version of X.25 that also relies on packet switching. ITU and ANSI standardized Frame Relay in 1984. An important difference between Frame Relay and X.25 is the Frame Relay does not guarantee reliable delivery of data. X.25 checks for errors and, in the case of an error, either corrects the damaged data or retransmits the original data.

Both X. 25 and Frame Relay may be configured as switched virtual circuits (SVCs) or permanent virtual circuits (PVCs). **SVCs** are connections that are established when parties need to transmit, then terminated once the transmission is complete. PVCs are connections that are established before data needs to be transmitted and maintained after the transmission is complete.

When you lease an X.25 or Frame Relay circuit from your local carrier, your contract reflects the endpoints you specify and the amount of bandwidth you require between those endpoints. The service provider guarantees a minimum amount of bandwidth, called the committed information rate (CIR)**.** The advantage to leasing a Frame Relay circuit over leasing a dedicated service is that you pay for only the amount of bandwidth required.

ISDN

ISDN (Integrated Services Digital Network) is an international standard, originally established by the ITU in 1984, for transmitting digital data over the PSTN. ISDN specifies protocols at the Physical, Data Link and Transport layers of the OSI Model. These protocols handle signaling, framing, connection setup and termination, routing, flow control, and error detection and correction. ISDN relies on the PSTN for its transmission medium.

All ISDN connections are based on two types of channels: B channels and D channels. The B channel is the “bearer” channel, employing circuit-switching techniques to carry voice, video, audio, and other types of data over the ISDN connection. The D channel is the “data” channel, employing packet-switching techniques to carry information about the call, such as session initiation and termination signals, caller identity, call forwarding, and conference calling signals.

In North America, two types of ISDN connections are commonly used: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI (Basic Rate Interface) uses two B channels and one D channel, as indicated by the notation 2B+D. The two B channels are treated as separate connections by the network and can carry voice and data or two data stream simultaneously and separate from each other. In a process called bonding, these two 64-Kbps B channels can be combined to achieve an effective throughput of 128 Kbps—the maximum amount of data traffic that a BRI connection can accommodate.

4.0 CONCLUSION

MANs (Metropolitan Area Networks) are larger versions of LANs. Typically they link several distinct sites dispersed around a city. They may be privately owned or they may be implemented using network capacity rented from a telecommunications service provider. Early MANs used technologies similar to LANs, but now they often use technologies more akin to WANs. WANs (Wide Area Networks) span a wide geographical area, typically a country or continent. They are almost invariably operated by a telecommunications service provider rather than being owned by an end user. Rather, an end user's individual machine, or more likely his LAN or MAN, will have a connection to the WAN. The backbone of the familiar Internet is basically a collection of linked WANs. WANs are usually point-to-point networks.

5.0 SUMMARY

In this unit we have been able to:

- to assist students in understanding the concepts of metropolitan area network(MAN) and wide area network (WAN)
- discuss the major characteristics of MAN and WAN
- deepen students understating of MAN and WAN topologies

TUTOR MARKED ASSIGNMENT

1. Explain the main characteristics of both MAN and WAN.

7.0 FURTHER READINGS

1. Computer Networks by A.S. Tanenbaum, 2003[2],
2. Computer Networks by P.J. Irving, 2003[3],
3. Ed, T. Theory and Problems of Computer Networking. USA: Schaum's Outline Series, McGRAW-HILL, 2002.

MODULE 4: TYPES OF NETWORK, TRANSMISSION MEDIA,ADDRESSING AND TROBLESHOOTING

Unit 3: Transmission media

		Page
1.0	**Introduction**	**94**
2.0	**Objectives**	**94**
3.0	**Network cabling**	**94**
3.1	**Installing cable – some guidelines**	**100**
3.2	**Wireless Network**	**102**
4.0	**Conclusion**	**102**
5.0	**Summary**	**102**
6.0	**Tutor Marked Assignment**	**102**
7.0	**Further Reading and Other Resources**	**102**

1.0 INTRODUCTION

This unit covers various transmission media available for transferring information, the characteristics and the ways to carry data during its transmission are also included.

2.0 OBJECTIVES

The main objective of this unit is to explain different transmission media including Unshielded Twisted Pair (UTP) cable, Shielded Twisted Pair (STP) cable, Coaxial Cable, Fiber Optic Cable, Wireless LANs.

3.0 NETWORK CABLING

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) cable
- Shielded Twisted Pair (STP) cable
- Coaxial Cable
- Fiber Optic Cable
- Wireless LANs
- Cable Installation Guides

Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 4.3.1).

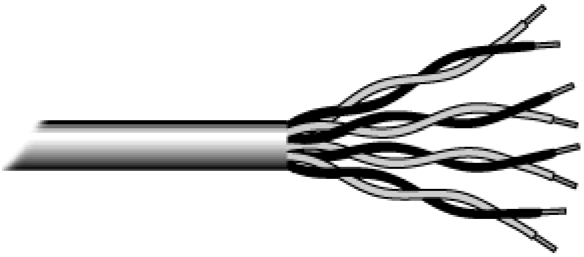
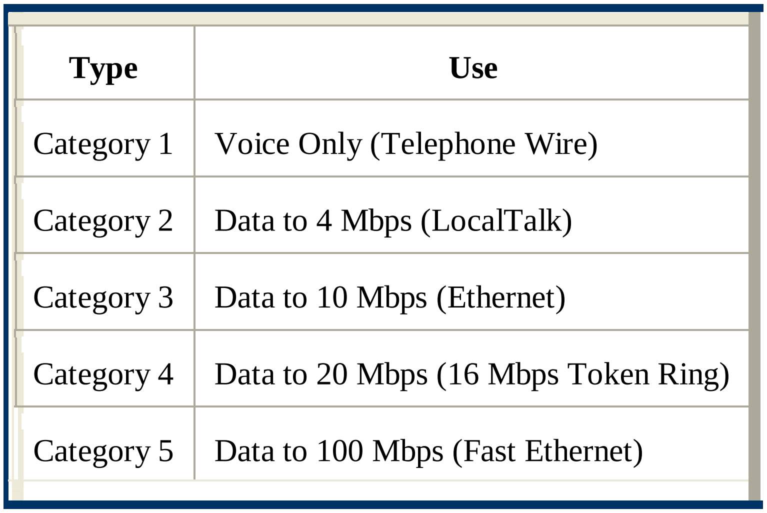


Fig.4.3.1: Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated five categories of wire.

Categories of Unshielded Twisted Pair



Type	Use
Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

Buy the best cable you can afford; most schools purchase Category 3 or Category 5. If you are designing a 10 Mbps Ethernet network and are considering the cost savings of buying Category 3 wire instead of Category 5, remember that the Category 5 cable will provide more "room to grow" as transmission technologies increase. Both Category 3 and Category 5 UTP have a maximum segment length of 100 meters. In Florida, Category 5 cable is required for retrofit grants. 10BaseT refers to the specifications for unshielded twisted pair cable (Category 3, 4, or 5) carrying Ethernet signals. Category 6 is relatively new and is used for gigabit connections.

Unshielded Twisted Pair Connector

table shows the tremendous variation in transmission time with different throughput rates

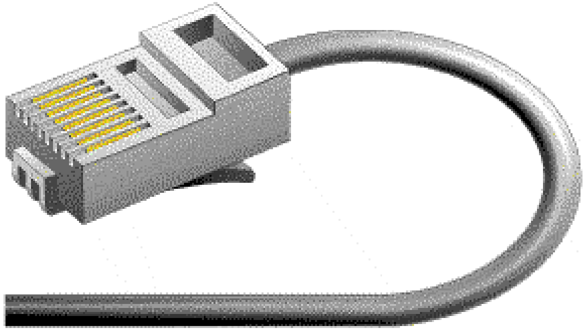


Fig. 4.3.2 RJ-45 connector

Shielded Twisted Pair (STP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 4.3.3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

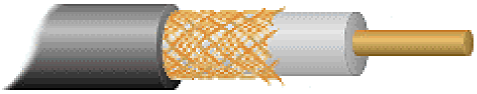


Fig. 4.3.3 Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable is popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4.3.4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.

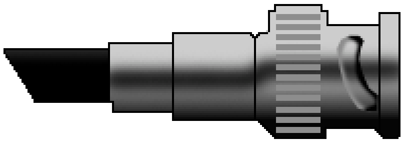


Fig. 4.3.4 BNC connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 4.3.5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

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

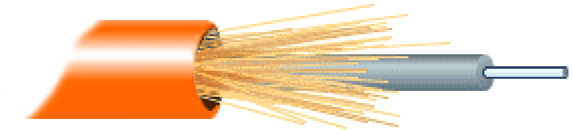


Fig. 4.3.5 Fiber optic cable

Facts about fiber optic cables:

- Outer insulating jacket is made of Teflon or PVC.
- Kevlar fiber helps to strengthen the cable and prevent breakage.
- A plastic coating is used to cushion the fiber center.

- Center (core) is made of glass or plastic fibers.

Fiber Optic Connector

The most common connector used with fiber optic cable is an ST connector. It is barrel shaped, similar to a BNC connector. A newer connector, the SC, is becoming more popular. It has a squared face and is easier to connect in a confined space.

Ethernet Cabling

The types of Ethernet cables available are

1. Straight-through cable
2. Crossover cable
3. Rolled cable

Straight-through cable

Four wires are used in straight-through cable to connect Ethernet devices. It is relatively simple to create this type. Only pins1, 2, 3 and 6 are used. Just connect 1 to1, 2 to 2, 3 to 3 and 6 to 6 and you will be up and networking in no time while practically we connect all 4 pairs straighten of CAT-5. However, this would be an Ethernet only cable and would not work with Voice, Token Ring, ISDN, etc. This type of cable is used to connect

1. Host to switch or hub
2. Router to switch or hub

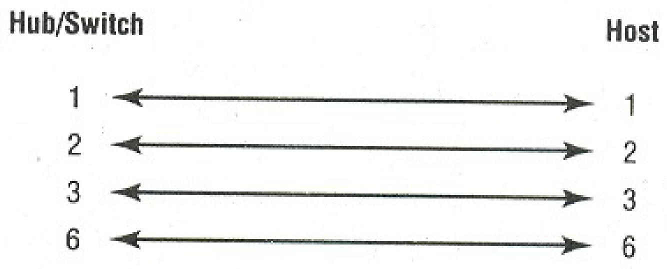


Fig. 4.3.6 Straight-through cable

Crossover Cable

Four wires are used in straight-through cable to connect Ethernet devices. Only four pins are used in this type of cabling. In crossover cable we connect 1 to3 and 2 to 6 on each side of cable. This type of cable is used to connect

1. Switch to switch
2. Hub to hub
3. Host to host
4. Hub to switch
5. Router direct to host

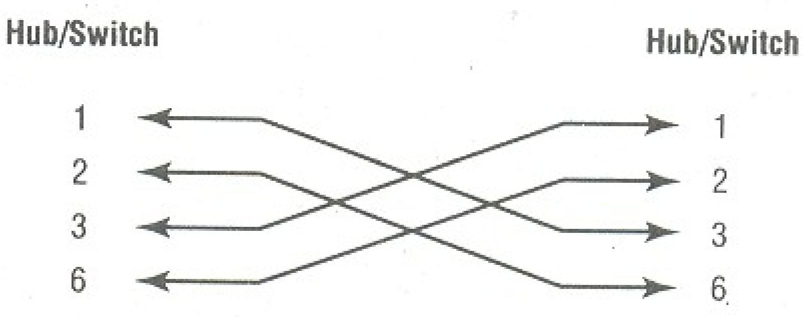


Fig. 4.3.7 Cross over cable

Rolled Cable

Although rolled cable is not used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a host to a router console serial communication (com) port. If you have a Cisco router of switch, you would use this cable to connect your PC running Hyper Terminal to the Cisco hardware. Eight wires are used in this cable to connect serial devices, although not all eight are used to send information, just as in Ethernet networking

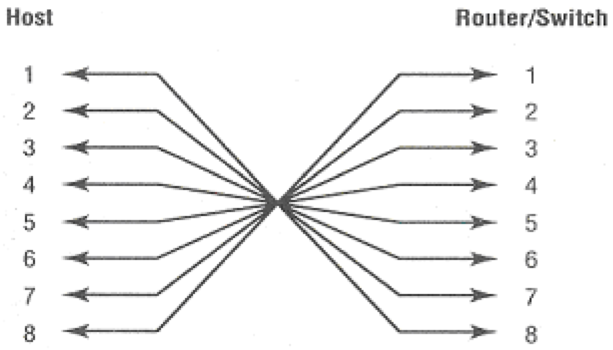


Fig. 4.3.8 Rolled cable

Table 4.3.1 Ethernet Cable Summary

Specification	Cable Type	Maximum length
10BaseT	Unshielded Twisted Pair	100meters
10Base2	Thin Coaxial	185Meters
10Base5	Thick Coaxial	500Meters
10BaseF	Fiber Optic	2000Meters
100BaseT	Unshielded Twisted pair	100Meters
100BaseTX	Unshielded Twisted Pair	220Meters

3.1 INSTALLING CABLE - SOME GUIDELINES

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

3.2 WIRELESS LANs

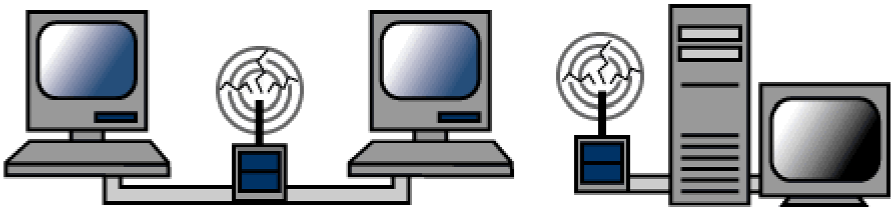


Fig. 4.3.9 Wireless LAN

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network.

Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless LANs have several disadvantages. They provide poor security, and are susceptible to interference from lights and electronic devices. They are also slower than LANs using cabling.

Exercise 4.3.1 What are the types of media used in LANs?

Answer: The types of media are coax, unshielded twisted pair (two categories – voice grade (3) and data grade (5)), fiber, and wireless. There was also shielded twisted pair (from IBM). Coax comes in two flavors – thick and thin.

4.0 CONCLUSION

This unit has discussed various transmission media available for transferring information, the characteristics and the ways to carry data during its transmission are also discussed

5.0 SUMMARY

In summary we have explained different transmission media such as Unshielded Twisted Pair (UTP) cable, Shielded Twisted Pair (STP) cable, Coaxial Cable, Fiber Optic Cable, and Wireless LANs.

6.0 TUTOR'S MARKED ASSIGNMENT

1. Explain the characteristics of some of the transmission media mentioned in this unit.

7.0 FURTHER READINGS

1. Keshav . "An Engineering Approach to Computer Networking", S. Keshav, Addison Wesley, 1998
2. Kurose, Ross. "Computer Networking", J.F. Kurose and K.W. Ross, Addison Wesley, 2000

Source of diagrams: http://www.commscope.com/ images/hybrids.jpg hybrid cable

MODULE 4: TYPES OF NETWORK, TRANSMISSION MEDIA,ADDRESSING AND TROBLESHOOTING

Unit 4: Addressing

Page

1.0 Introduction 104

2.0 Objectives 104

3.0 Addressing 104

3.1 Ethernet Addressing 104

3.2 Internet Protocols (IP) Addressing 105

3.2.1 Hierarchical IP addressing 105

3.2.2 Private IP addressing 106

3.3 Network Addressing 106

4.0 Conclusion 108

5.0 Summary 108

6.0 Tutor Marked Assignment 108

7.0 Further Reading and Other Resources 108

1.0 INTRODUCTION

This unit offers an introduction to network addressing. An address is a numeric identifier assigned to each machine on a network. It designates the specific location of a device on the network. An address is a software address, not a hardware address- the latter is hard-coded on a Network Interface Card (NIC) and used for finding hosts on a local network. Addressing was designed to allow a host on one network to communicate with a host on a different network, regardless of the type of LANs the hosts are participating in.

2.0 OBJECTIVES

At the end of this unit, students should be able to:

- Explain the basics of a network addressing
- Describe the standard networking addresses
- Explain the variations on standard networking addresses
- Describe the role of address in a network.

3.0 ADDRESSING

3.1 Ethernet Addressing

Ethernet addressing uses Media Access Control (MAC) Address burned into each and every Ethernet Network Interface Card (NIC). The MAC or hardware address, is a 48-bit (6-byte) address written in a hexadecimal format.

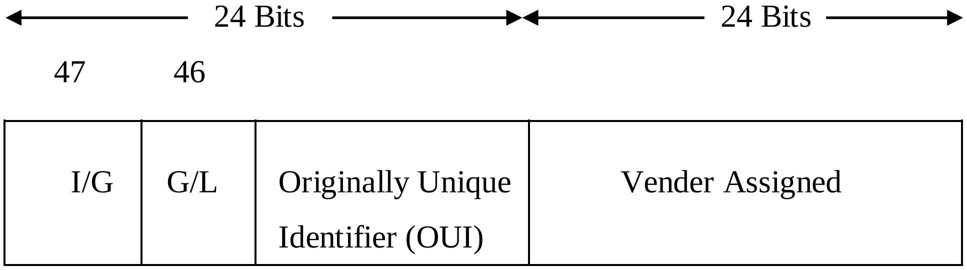


Fig. 4.4.1 – Ethernet addressing using MAC addresses

The organizationally unique identifier (OUI) is assigned by the IEEE to an organization. It’s composed of 24 bits, or 3 bytes. The organization, in turn, assigns a globally administered address (24 bits, or 3 bytes) that is unique (supposedly, again-no guarantees) to each and every adapter they manufacture. The high-order bit is the individual/Group (I/G) bit. When it has a value of 0, we can assume that the address is MAC address of a device and may well appear in the source portion of the MAC header. When it is a 1, we can assume that the address represents either a broadcast or multicast address in Ethernet, or a broadcast .The next bit is the G/L bit (also known as U/L, where U means universal). When set to 0, this bit represents a globally administered address (as by IEEE). When the bit is 1, it represents a locally governed and administered address (as in DECnet). The low-order 24 bits of an Ethernet address represent a locally administered or manufacturer-assigned code. This portion commonly starts with 24 0s for the first card made and continues in order until there are 24 1s for the last card made. You will find that many manufacturers use these same six hex digits as the last six characters of their serial number on the same card.

3.2 IP ADDRESSING

An IP address is a numeric identifier assigned to each machine on an IP network. It designates the specific location of a device on the network. An IP address is a software address, not a hardware address- the latter is hard-coded on a Network Interface Card (NIC) and used for finding hosts on a local network. IP addressing was designed to allow a host on one network to communicate with a host on a different network, regardless of the type of LANs the hosts are participating in.

There are two IP addressing schemes:

1. Hierarchical IP addressing
2. Private IP Addressing

3.2.1 Hierarchical IP addressing

An IP address consists of 32 bits of information. These bits are divided into four sections, referred to as octets or bytes, each containing 1 byte (8 bits).You can depict an IP address using one of three methods:

1. Dotted-decimal, as in 172.16.30.56
2. Binary, as in 10101100.00010000.00011110.00111000
3. Hexadecimal, as in AC.10.1E.38

All these examples represent same IP address. The 32-bit IP address is a structured or hierarchical address, as opposed to a flat or nonhierarchical address. Although either type of addressing scheme could have been used, hierarchical addressing was chosen for a good reason. The advantage of this scheme is that it can handle a large number of addresses, namely 4.3 billion. The disadvantage of the flat addressing scheme, and the reason it’s not used for IP addressing, relates to routing. If every address were unique, all routers on the Internet would need to store the address of each and every machine on the Internet. This would make efficient routing impossible, even if only a fraction of the possible addresses were used.

The solution to this problem is to use a two or three-level, hierarchical addressing scheme that is structured by network and host, or network, subnet, and host. This two- or three-level scheme is comparable to a telephone number. The first section, the area code, designates a very large area. The second section, the prefix, narrows the scope to a local calling area. The final segment, the customer number, zooms in on the specific connection. IP address uses the same type of layered structure. Rather than all 32 bits being treated as a unique identifier, as in flat addressing, a part of the address is designated as the network address, and the other part is designated as either the subnet and host or just the node address.

3.2.2 Private IP Addresses

These addresses can be used on a private network, but they are not routable through the Internet. This is designed for the purpose of creating a measure of well-needed security, but it also conveniently saves valuable IP address space. If every host on every network had to have real routable IP address, we would have run out of IP address to hand out years ago. But by using private IP address, ISPs, corporation, and home users only need a relatively tiny group of bona fide IP addresses to connect

their networks to the Internet. This is economical because they can use private IP addresses on their inside networks and get along just fine.

To accomplish this task, the ISP and the corporation-the end user, no matter who they are-need to use something called a Network Address Translation (NAT), which basically takes a private and converts it for use on the Internet. Many people can use the same real IP address to transmit out onto the Internet.

3.3 NETWORK ADDRESSING

The network address (which can also be called the network number) uniquely identifies each network. Every machine on the same network shares that network address as part of its IP address. In the IP address 172.16.30.56, for example, 172.16 is the network address.

The nodes address is assigned to, and uniquely identifies, each machine on a network. This part of the address must be unique because it identifies a particular machine-an individual as opposed to a network, which is a group. This number can also be referred to as a host address. In the sample IP address 172.16.30.56 is the node address.

The designers of the Internet decided to create classes of networks based on network size. For the small number of networks possessing a very large number of nodes, they created the rank *Class 'A' network.* At the other extreme is the *Class 'C' network*, which is reserved for the numerous networks with a small, is predictably called the *Class 'B' network.*

Subdividing an IP address into a network and node address is determined by the class designation of one's network

	8 Bits	8 Bits	8 Bits	8 Bits
Class ‘A’ :	Network	Host	Host	Host

	8 Bits	8 Bits	8 Bits	8 Bits
Class ‘B’ :	Network	Network	Host	Host

	8 Bits	8 Bits	8 Bits	8 Bits
Class ‘C’ :	Network	Network	Network	Host

Class ‘D’ : Multicast

Class ‘E’ : Research

Fig. 4.4.2 - Summary of the three classes of Networks

To ensure efficient routing, Internet designers defined a mandate for the leading-bits section of the address for each different network class. For example, since a router knows that a Class ‘A’ network address always starts with a 0, the router might be able to speed a packet on its way after reading only the first bit of its address. This is where the address schemes define the difference between a Class ‘A’, a Class ‘B’, and a Class ‘C’ address. In the next section, I will discuss the differences between these three classes, followed by a discussion of the Class ‘D’ and Class ‘E’ address.

Network Address Range - Class ‘A’

The designers of the IP address scheme said that the first bit of the first byte in a Class ‘A’ network address must always be off, or 0. This means a Class ‘A’ address must be between 0 and 127. So a Class ‘A’ network is defined in the first octet between 0 and 127, and it can’t be less or more.

Network Address Range - Class ‘B’

In a Class ‘B’ network, the RFCs state that the first bit of the first byte must always be turned on, but the second bit must always be turned off. If you turn the other 6 bits all off and then all on, you will find the range for a Class ‘B’ network, thus a Class ‘B’ network is defined when the first byte is configured from 128 to191.

Network Address range - Class ‘C’

The first three bytes of a Class ‘C’ network address are dedicated to the network portion of the address, with only one measly byte remaining for the node address. Thus a class ‘C’ network is defined when first byte is configured from192 to 223.

Exercise 4.4.1 Assume that hosts A and B have a TCP connection established. Assume that the two hosts are separate by one router (i.e., they are one hop apart). Why does host A not directly use the MAC (LAN) address of host B when constructing its packets to send to host B?

Answer: Host A has no way of knowing the MAC address of host B on the other side of a router. A router does not pass broadcasr ARP frames. In any case, the MAC address of the router port connecting host A's LAN to host B's LAN must be used to forward an A-to-B packet through the router. If some other MAC address (e.g., that of host B) were used, routing would not take place.

Exercise 4.4.2. An Ethernet frame has 8 bytes of 10101010b in the preamble. What is the purpose of this preamble?

Answer: This preamble serves to delimit the frame for the receiving adapter. Specifically, the purpose of the preamble is to synchronize the receiver's clock with the sender's clock for the receipt of the frame

4.0 CONCLUSION

In this unit we have presented the fact that an address is a numeric identifier assigned to each machine on a network. It designates the specific location of a device on the network. An address is a software address, not a hardware address- the latter is hard-coded on a Network Interface Card (NIC) and used for finding hosts on a local network. Addressing was designed to allow a host on one network to communicate with a host on a different network, regardless of the type of LANs the hosts are participating in.

5.0 SUMMARY

At the end of this unit we have been able to:

- Explain the basics of addressing
- Describe different types of addressing
- Explain the variations on standard networking addresses
- Describe the role of address in a network.

6.0 TUTOR MARKED ASSIGNMENT

1. Enumerate on the functions of various addressing techniques.

7.0 FURTHER READINGS

1. Communication Networks: Fundamental Concepts and Key Architectures, Albert Leon- Garcia & Indra Widjaja, McGraw Hill
2. Data and Computer Communications, William Stallings, Prentice-Hall,

MODULE 4: TYPES OF NETWORK, TRANSMISSION MEDIA, ADDRESSING, AND TROBLESHOOTING

Unit 5: Basic Network Troubleshooting

Page

1.0 Introduction 110

2.0 Objectives 110

3.0 Basic Network Troubleshooting 110

4.0 Conclusion 113

5.0 Summary 113

6.0 Tutor Marked Assignment 113

1.0 INTRODUCTION

We discuss the basic methods of network troubleshooting in this unit.

2.0 OBJECTIVES

The main objective of this unit is to explain how basic network troubleshooting can be performed/

3.0 Basic network troubleshooting.

Cause:

If a computer is unable to connect to a network or see other computers on a network, it may be necessary to troubleshoot the network. A network may not work because of any of the below reasons.

1. Network card not connected properly.
2. Bad network card drivers or software settings.
3. Firewall preventing computers from seeing each other.
4. Connection related issues.
5. Bad network hardware.

Solution:

Because of the large variety of network configurations, operating systems, setup, etc... not all of the below information may apply to your network or operating system. If your computer is connected to a company or large network, or you are not the administrator of the network, it is recommended that if you are unable to resolve your issues after following the below recommendations that you contact the network administrator or company representative.

Note: If you are being prompted for a Network password and do not know the password, Computer Hope is unable to assist users with obtaining a new or finding out the old password.

Verify connections / LEDs

Verify that the network cable is properly connected to the back of the computer. In addition, when checking the connection of the network cable, ensure that the LEDs on the network are properly illuminated. For example, a network card with a **solid** green LED or light usually indicates that the card is either connected or receiving a signal.

Note: generally, when the green light is flashing, this is an indication of data being sent or received. If, however, the card does not have any lights or has orange or red lights, it is possible that either the card is bad, the card is not connected properly, or that the card is not receiving a signal from the network. If you are on a small or local network and have the capability of checking a hub or switch, verify that the cables are properly connected and that the hub or switch has power.

Adapter resources

Ensure that if this is a new network card being installed into the computer that the card's resources are properly set and/or are not conflicting with any hardware in the computer. Users who are using Windows 95, 98, ME, 2000 or XP, verify that Device Manager has no conflicts or errors. Additional help and information about Device Manager and resources can be found on our Device Manger page.

Adapter functionality

Verify that the network card is capable of pinging or seeing itself by using the ping command. Windows / MS-DOS users ping the computer from a MS-DOS prompt. Unix / Linux variant users ping the computer from the shell.

To ping the card or the local-host, type either

```
ping 127.0.0.1
```

or

```
ping local-host
```

This should show a listing of replies from the network card. If you receive an error or if the transmission failed, it is likely that either the network card is not physically installed into the computer correctly, or that the card is bad.

Protocol

Verify that the correct protocols are installed on the computer. Most networks today will utilize TCP/IP, but may also utilize or require IPX/SPX and NetBEUI.

Additional information and help with installing and reinstalling a network protocol can be found on document CH000470.

When the TCP/IP protocol is installed, unless a DNS server or other computer assigns the IPX address, the user must specify an IP address as well as a Subnet Mask. To do this, follow the below instructions.

1. Click Start / Settings / Control Panel
2. Double-click the Network icon

3. Within the configuration tab double-click the TCP/IP protocol icon. Note: Do not click on the PPP or Dial-Up adapter, click on the network card adapter.
4. In the TCP/IP properties click the IP address tab
5. Select the option to specify an IP address
6. Enter the IP address and Subnet Mask address, an example of such an address could be:

   IP Address: 102.55.92.1
   Subnet Mask: 255.255.255.192

7. When specifying these values, the computers on the network must all have the same Subnet Mask and have a different IP Address. For example, when using the above values on one computer you would want to use an IP address of 102.55.92.2 on another computer and then specify the same Subnet Mask.

Firewall

If your computer network utilizes a firewall, ensure that all ports required are open. If possible, close the firewall software program or disconnect the computer from the firewall to ensure it is not causing the problem.

Additional time

In some cases it may take a computer some additional time to detect or see the network. If after booting the computer you are unable to see the network, give the computer 2-3 minutes to detect the network. Windows users may also want to try pressing the F5 (refresh) key when in Network Neighborhood to refresh the network connections and possibly detect the network.

Additional troubleshooting

If after following or verifying the above recommendations you are still unable to connect or see the network, attempt one or more of the below recommendations.

If you have installed or are using TCP/IP as your protocol you can attempt to ping another computer's IP address to verify if the computer is able to send and receive data. To do this, Windows or MS-DOS users must be at a prompt and Linux / Unix variant users must open or be at a shell.

Once at the prompt assuming, that the address of the computer you wish to attempt to ping is 102.55.92.2, you would type:

```
ping 102.55.92.2
```

If you receive a response back from this address (and it is a different computer), this demonstrates that the computer is communicating over the network. If you are still unable to connect or see the network, it is possible that other issues may be present.

Another method of determining network issues is to use the tracert command if you are a MS-DOS or Windows user or the traceroute command if you are a Linux / Unix variant user. To use this command you must be at the command prompt or shell.

Once at the prompt, assuming that the address is again 102.55.92.2, type:

```
tracert 102.55.92.2
```

or

```
traceroute 102.55.92.2
```

This should begin listing the hops between the computer and network devices. When the connection fails, determine which device is causing the issue by reviewing the traceroute listing.

4.0 CONCLUSION

This unit has highlighted the basic network troubleshooting techniques.

5.0 SUMMARY

In this unit, various ways of how to troubleshoot a network have been discussed

6.0 TUTOR MARKED ASSIGNMENT

1. What are the likely causes of network connection failure and how can they be resolved?