NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

NETWORK ROUTING AND OPTIMIZATION

Graduation Project
COM-400

Student: Adham Habboub(20021932)

Supervisor: Ass.Prof.Dr.Rahib Abiyev

Nicosia- 2006

ACKNOWLEDGMENT

First of all I am happy to complete the mission which I had been given with blessing of God and also I am grateful to all the people who assisted , supported , guided , taught and who have always encouraged me during performing my project.

I wish to thank my supervisor, ***Assoc.Prof.Dr. Rahib Abiyev****, for supporting, encouragement, and enthusiasm and his patience for correcting both my stylistic and scientific errors.*

All my warm wishes for long life for my parents who tried their best to develop my abilities to be educational person which make the ease via my life.

My sincerest thanks must go to my friends Hazem Aboshaaban, Khaled A'amar, Osama Alkurd, Muath Ismael,Musab Soutari ,Ahmed Mesleh, who shared their suggestions and evaluations throughout the completion of my project. The comments from these friends enabled me to present this project successfully.

And above, I thank God for giving me stamina and courage to achieve my objectives.

ADHAM HABBOUB

ABSTRACT

Now-a-days Networking is getting very famous. Specially in the big organizations such like universities, Banks, Multinational companies. Networking to reduce the cost, to reduce the distances, to access the data in the blink of eye. Now the best idea of network's knowledge, standards of networks, protocols such like TCP/IP is provided. And the idea about networks types and network topologies suck like star, tree, mesh, bus and ring and as well merits and demerits of every type of topology. It is considered that some knowledge about the cables, which have to be understood very carefully because we have different types of cabling connections.

Some information about the networks connection such like Peer-to-peer, Client-to –peer. And also some useful information about the networking hardware such like Routers, hubs, repeater, etc is provided.

Idea about routing speacially its history and some information about how the router works. Also provide some information algorithm routing. And solved some examples regarding to this. Some best algorithm to find the routing path, also algorithm types, and some useful information about the routing information protocol. Some example of routing and routing tables.

The knowledge is considered about the network Optimization and some analysis regarding to this is explained. And also give some concentration to Topological Optimization of Network using Integer Programming and solved example related with this by using winqsb program.

TABLE OF CONTENT

ITRODUCTION

This project is about Network routing and optimization. We commonly use the word "networking" in our daily life. But a basic understanding of computer networks is requisite in order to understand the principles of network, security, and as the internet is growing, the community has changed from a small tight group of academic users to a loose gathering of people on a global network, so that the moving of information between the groups by the network sharing became a popular way, then, the need to find the optimal paths to rout the information has come to be one of the important topics all over the world of information transportation.

This Project includes *four chapters* covering the main topics:

Chapter 1 discuss the network structures as whole**:** What is Networking, The OSI model, protocols, Network operating system.

*Chapter 2 d*escribes the underlying concepts widely used in network topologies: What Is network topologies, Types of networks, its geographical coverage, Types of cables, networking hardware, networking architecture.

Chapter 3 discuss the network routing problem: How Routers Work, Algorithm routing types, Routing Information Protocol, Distance Vector, Counting to Infinity, Open Shortest Path First, Dijkstra's Algorithm, Flooding Algorithm, OSPF Protocol.

Chapter 4 discuss network optimization and solve the network optimization problem: What Is Network Optimization, Network Modification Analysis, Measuring Network Application Efficiency Problem, Network Linear Program.

Finally in conclusion the important results for the project are described.

CHAPTER ONE

INTRODUCTION TO NETWORKING

1.1 Overview

In this chapter we will discuss the network structures as whole: What is Networking, explain some protocols just like OSI model , TCP/IP protocol and the difference between them and Network operating system .

1.2 Introduction to Networking

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this section, we will cover some of the foundations of computer networking. Following that, we will take a more in-depth look at Routing`s concepts,the problem of routing in computer network.

1.3 What is a Network?

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.

The three basic types of networks include:

- Local Area Network (LAN)
- Wide Area Network (WAN)

.

1.4 Network Essentials

Network essentials are the things we must have to take care of to establish a good network between two or more networks. It include the OSI reference model which help in complete establishment of the network then we have protocols then we have WAN hardware all these things are very essential for a network .

1.4.1 The OSI Model

- OSI is a layer model Developed by ISO it is a seven layer architecture help in communication between two computers.
- International Standards Organization (ISO) specifications for network architecture. Called the Open Systems Interconnect or OSI model.
- Seven layered model, higher layers have more complex tasks. Each layer provides services for the next higher layer. Each layer communicates logically with its associated layer on the other computer.
- Packets are sent from one layer to another in the order of the layers, from top to bottom on the sending computer and then in reverse order on the receiving computer.

OSI Layers Names and a precise description is as follows:

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

1.4.1.1 Application Layer.

- Serves as a window for applications to access network services.
- Handles general network access, flow control and error recovery.

1.4.1.2 Presentation Layer

- Determines the format used to exchange data among the networked computers.
- Translates data from a format from the Application layer into an intermediate format.

- Responsible for protocol conversion, data translation, data encryption, data compression, character conversion, and graphics expansion.
- Redirector operates at this level.

1.4.1.3 Session Layer

- Allows two applications running on different computers to establish use and end a connection called a Session.
- Performs name recognition and security.
- Provides synchronization by placing checkpoints in the data stream.
- Implements dialog control between communicating processes.

1.4.1.4 Transport Layer

- Responsible for packet creation.
- Provides an additional connection level beneath the Session layer.
- Ensures that packets are delivered error free, in sequence with no losses or duplications.
- Unpacks, reassembles and sends receipt of messages at the receiving end.
- Provides flow control, error handling, and solves transmission problems.

1.4.1.5 Network Layer

- Responsible for addressing messages and translating logical addresses and names into physical addresses.
- Determines the route from the source to the destination computer.
- Manages traffic such as packet switching, routing and controlling the congestion of data.

1.4.1.6 Data Link Layer

- Sends data frames from the Network layer to the Physical layer.
- Packages raw bits into frames for the Network layer at the receiving end.
- Responsible for providing error free transmission of frames through the Physical layer.

1.4.1.7 Physical Layer

- Transmits the unstructured raw bit stream over a physical medium.
- Relates the electrical, optical mechanical and functional interfaces to the cable.
- Defines how the cable is attached to the network adapter card.
- Defines data encoding and bit synchronization. .

1.5 Protocols

- Protocols are rules and procedures for communication.

1.5.1 How Protocols Work?

The Sending Computer does the following jobs

- Breaks data into packets.
- Adds addressing information to the packet
- Prepares the data for transmission.

The Receiving Computer does the following jobs

- Takes the packet off the cable.
- Strips the data from the packet.
- Copies the data to a buffer for reassembly.
- Passes the reassembled data to the application.

1.5.2 Protocol Stacks (or Suites)

- A combination of protocols, each layer performing a function of the communication process.
- Ensure that data is prepared, transferred, received and acted upon.

1.5.3 The Binding Process

- Allows more than one protocol to function on a single network adapter card. (e.g. both TCP/IP and IPX/SPX can be bound to the came card

- Binding order dictates which protocol the operating systems uses first.
- Binding also happens with the Operating System architecture: for example, TCP/IP may be bound to the NetBIOS session layer above and network card driver below it. The NIC device driver is in turn bound to the NIC.

1.5.4 Standard Stacks

- ISO/OSI
- IBM SNA (Systems Network Architecture)
- Digital DECnet
- Novell NetWare
- Apple AppleTalk
- TCP/IP

1.6 Protocol types map roughly to the OSI Model into three layers:

Application Level Service Users

- Application Layer
- Presentation Layer
- Session Layer

Transport Services

- Transport Layer

Network Services

- Network Layer
- Data Link Layer
- Physical Layer

1.7 The IEEE protocols at the Physical Layer

1.7.1 802.3 (CSMA /CD - Ethernet)

- logical bus network
- can transmit at 10 Mbps
- data is transmitted on the wire to every computer but only those meant to receive respond
- CSMA /CD protocol listens and allows transmission when the wire is clear

1.7.2 802.4 (Token Passing)

- bus layout that used token passing
- every computer receives all of the data but only the addressed computers respond
- token determines which computer can send

1.7.3 802.5 (Token Ring)

- logical ring network; physical set up as star network
- transmits at 4 Mbps or 16 Mbps
- token determines which computer can send

1.8 Important Protocols

1.8.1 TCP/IP

- Provides communications in a heterogeneous environment.
- Routable, defacto standard for internetworking.
- SMTP, FTP, SNMP are protocols written for TCP/IP
- Disadvantages are size and speed.

1.8.2 NetBEUI

- NetBIOS extended user interface.
- Originally, NetBIOS and NetBEUI were tightly tied together but, NetBIOS has been separated out to be used with other routable protocols. NetBIOS acts as a

tool to allow applications to interface with the network; by establishing a session with another program over the network

- NetBIOS operates at the Session layer.
- Small, fast and efficient.
- Compatible with most Microsoft networks.
- Not routable and compatible only with Microsoft networks.

1.8.3 X.25

- Protocols incorporated in a packet switching network of switching services.
- Originally established to connect remote terminals to mainframe hosts.

1.8.4 XNS

- Xerox Network System.
- Developed for Ethernet LANs but has been replaced by TCP/IP.
- Large, slow and produces a lot of broadcasts.

1.8.5 IPX/SPX and NWLink

- Used for Novell networks.
- Small and fast.
- Routable.

1.8.6 APPC

- Advanced Program to Program Communication
- Developed by IBM to support SNA.
- Designed to enable application programs running on different computers to communicate and exchange data directly.

1.8.7 AppleTalk

- Apple's proprietary protocol stack for Macintosh networks.

1.8.8 OSI Protocol Suite

- each protocol maps directly to a single layer of the OSI model

1.8.9 DECnet

- Digital Equipment's proprietary protocol stack
- Defines communications over Ethernet, FDDI MAN's and WAN's.
- DECnet can also use TCP/IP and OSI protocols as well as its own protocols
- Routable.

1.9 How does encapsulation allow computer to communicate data

To understand how networks are structured and how they function, you should remember that all communications on a network originate at a source and are being sent to a destination.

The information that is sent on a network is referred to as data or data packets. If one computer (host A) wants to send data to another computer (host B), the data must first be packaged in a process called encapsulation.

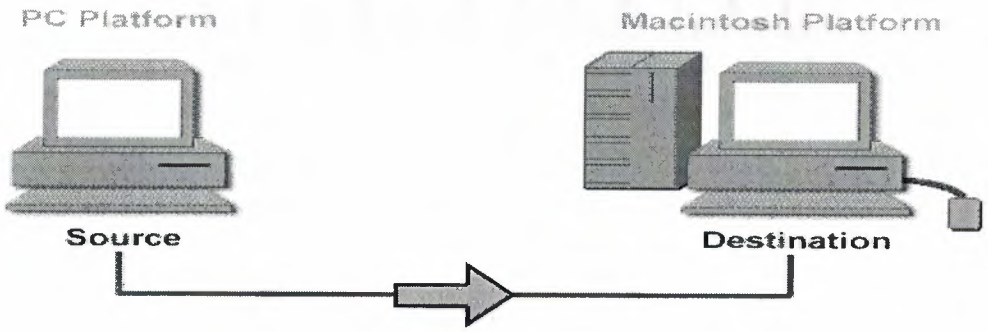


Figure 1.1 Data packet

1.10 Storing the Information in the computers

Information in computers is stored using the binary number system, in which the only possible symbols, or binary digits, or "bits", are 1 and 0. These bits - many of which are called data - are used to represent information, like text, pictures, and sounds.

In the physical layer, a 1 bit is often represented by the presence of voltage (electrical pressure) on a copper conducting cable or light in an optical fiber.

To help you picture these bits, imagine measuring the voltage at one point on the cable as time goes on (for a fiber, imagine measuring the light intensity versus time).

Your measurements would allow you to create a graph of voltage versus time (for a fiber, light intensity versus time).

How the bits (1s and 0s) might be represented on the cable is shown in the graphic.

There are many ways bits can be represented with voltages.

This process is called encoding.

Many of the LANs use "Manchester Encoding."

In this type of encoding bits are represented by different voltage patterns than the ones shown in the graphic.

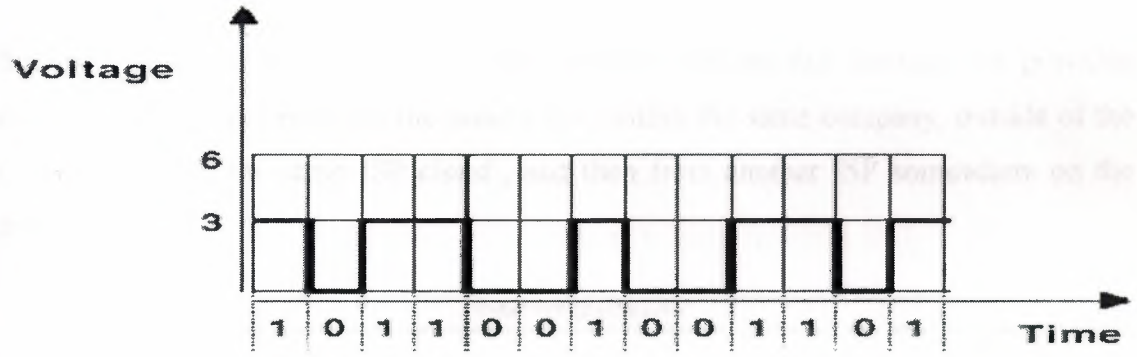


Figure 1.2 Digital signal

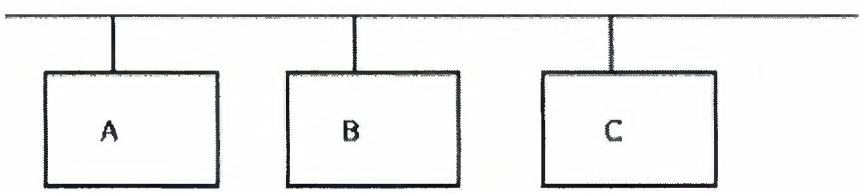


Figure 1.3 A Simple Local Area Network

I might be allowed to put one of my hosts on one of my employer's networks. We have a number of networks, which are all connected together on a backbone , that is a network of our networks. Our backbone is then connected to other networks, one of

which is to an Internet Service Provider (ISP) whose backbone is connected to other networks, one of which is the Internet backbone.

If you have a connection "to the Internet" through a local ISP, you are actually connecting your computer to one of their networks, which is connected to another, and so on. To use a service from my host, such as a web server, you would tell your web browser to connect to my host. Underlying services and protocols would send *packets* (small datagrams) with your query to your ISP's network, and then a network they are connected to, and so on, until it found a path to my employer's backbone, and to the exact network my host is on. My host would then respond appropriately, and the same would happen in reverse: packets would traverse all of the connections until they found their way back to your computer, and you were looking at my web page.

In Figure 1.4, the network shown in is designated "LAN 1" and shown in the bottom-right of the picture. This shows how the hosts on that network are provided connectivity to other hosts on the same LAN, within the same company, outside of the company, but in the same ISP *cloud* , and then from another ISP somewhere on the Internet.

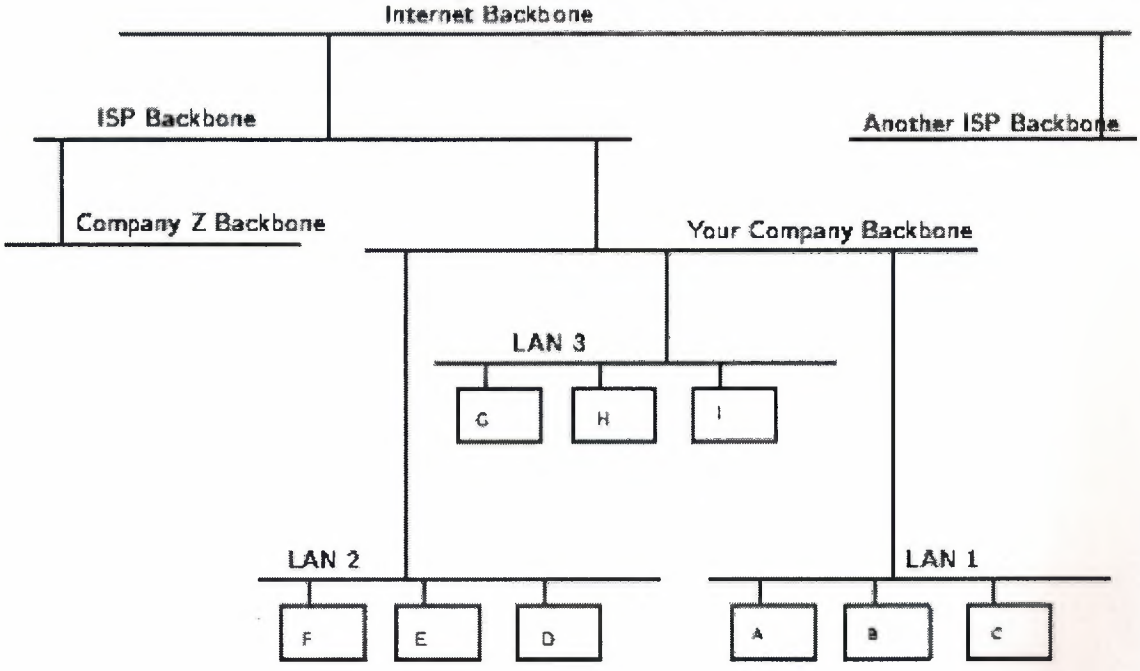


Figure 1.4 A Wider View of Internet-connected Network

The Internet is made up of a wide variety of hosts, from supercomputers to personal computers, including every imaginable type of hardware and software. How do all of these computers understand each other and work together?

1.11 Overview of TCP/IP

TCP/IP (Transport Control Protocol/Internet Protocol) is the language of the Internet. Anything that can learn to speak TCP/IP can play on the Internet. This is functionality that occurs at the Network (IP) and Transport (TCP) layers in the ISO/OSI Reference Model. Consequently, a host that has TCP/IP functionality (such as Unix, OS/2, MacOS, or Windows NT) can easily support applications (such as Netscape's Navigator) that uses the network.

TCP/IP protocols are not used only on the Internet. They are also widely used to build private networks, called internets, that may or may not be connected to the global Internet. An internet that is used exclusively by one organization is sometimes called an intranet

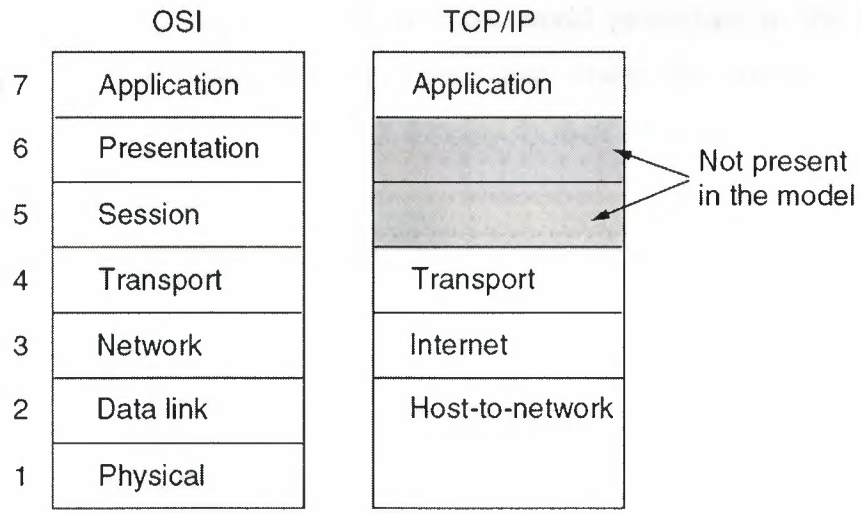


Figure1.5 The OSI and TCP/IP diagram

1.11.1 layers of TCP/IP

Session and presentation Layer not presented in TCP/IP model. Host-to-Network layer is equivalent of Physical and Data link layers in the OSI model.

1.11.2 Comparison of the OSI and TCP/IP Reference Model:

- There are 3 concepts control to the OSI model services, interface, protocol.
- The OSI model was devised before protocols were created.
- With TCP/IP, the protocols came first and the model was just a description of the existing protocols.
- TCP/IP has 4 layers, where as the OSI model has 7 layers.
- The OSI model has both connectionless and connection oriented communication in the network layer, but only connection oriented in the transport layer.
- The TCP/IP model has connectionless only in the network layer, but support both modes in the transport layer.

1.12 Open Design

One of the most important features of TCP/IP isn't a technological one: The protocol is an open protocol, and anyone who wishes to implement it may do so freely. Engineers and scientists from all over the world participate in the IETF (Internet Engineering Task Force) working groups that design the protocols that make the Internet work. Their time is typically donated by their companies, and the result is work that benefits everyone.

1.12.1 IP

IP is a "network layer" protocol. This is the layer that allows the hosts to actually talk to each other. Such things as carrying datagrams, mapping the Internet address to a physical network address , and routing, which takes care of making sure that all of the devices that have Internet connectivity can find the way to each other.

1.12.2 IP Address

IP addresses are analogous to telephone numbers – when you want to call someone on the telephone, you must first know their telephone number. Similarly, when a computer on the Internet needs to send data to another computer, it must first know its

IP address. IP addresses are typically shown as four numbers separated by decimal points, or "dots". For example, 10.24.254.3 and 192.168.62.231 are IP addresses.

If you need to make a telephone call but you only know the person's name, you can look them up in the telephone directory (or call directory services) to get their telephone number. On the Internet, that directory is called the Domain Name System or DNS for short. If you know the name of a server, say www.cert.org, and you type this into your web browser, your computer will then go ask its DNS server what the numeric IP address is that is associated with that name.

1.12.2.1 Static And Dynamic Addressing

Static IP addressing occurs when an ISP permanently assigns one or more IP addresses for each user. These addresses do not change over time. However, if a static address is assigned but not in use, it is effectively wasted. Since ISPs have a limited number of addresses allocated to them, they sometimes need to make more efficient use of their addresses.

Dynamic IP addressing allows the ISP to efficiently utilize their address space. Using dynamic IP addressing, the IP addresses of individual user computers may change over time. If a dynamic address is not in use, it can be automatically reassigned to another computer as needed.

1.12.2.2 Attacks Against IP

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

1.12.2.3 IP Spoofing

This is where one host claims to have the IP address of another. Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address, this is a useful technique to an attacker: he can send packets to a host, perhaps causing it to take some sort of action.

1.12.3 TCP and UDP Ports

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both protocols that use IP. Whereas IP allows two computers to talk to each other across the Internet, TCP and UDP allow individual applications (also known as "services") on those computers to talk to each other.

In the same way that a telephone number or physical mail box might be associated with more than one person, a computer might have multiple applications (e.g. email, file services, web services) running on the same IP address. Ports allow a computer to differentiate services such as email data from web data. A port is simply a number associated with each application that uniquely identifies that service on that computer. Both TCP and UDP use ports to identify services. Some common port numbers are 80 for web (HTTP), 25 for email (SMTP), and 53 for Dmain Name System (DNS).

1.12.4 TCP

TCP is a transport-layer protocol. It needs to sit on top of a network-layer protocol, and was designed to ride atop IP. (Just as IP was designed to carry, among other things, TCP packets.) Because TCP and IP were designed together and wherever you have one, you typically have the other, the entire suite of Internet protocols are known collectively as TCP/IP. TCP itself has a number of important features that we'll cover briefly.

1.12.4.1 Guaranteed Packet Delivery

Probably the most important is guaranteed packet delivery. Host A sending packets to host B expects to get acknowledgments back for each packet. If B does not send an acknowledgment within a specified amount of time, A will resend the packet.

Applications on host B will expect a data stream from a TCP session to be complete, and in order. As noted, if a packet is missing, it will be resent by A, and if packets arrive out of order, B will arrange them in proper order before passing the data to the requesting application.

This is suited well toward a number of applications, such as a telnet session. A user wants to be sure every keystroke is received by the remote host, and that it gets every packet sent back, even if this means occasional slight delays in responsiveness while a lost packet is resent, or while out-of-order packets are rearranged.

It is not suited well toward other applications, such as streaming audio or video, however. In these, it doesn't really matter if a packet is lost (a lost packet in a stream of 100 won't be distinguishable) but it does matter if they arrive late (i.e., because of a host resending a packet presumed lost), since the data stream will be paused while the lost packet is being resent. Once the lost packet is received, it will be put in the proper slot in the data stream, and then passed up to the application.

1.12.5 UDP

UDP (User Datagram Protocol) is a simple transport-layer protocol. It does not provide the same features as TCP, and is thus considered "unreliable". Again, although this is unsuitable for some applications, it does have much more applicability in other applications than the more reliable and robust TCP.

1.12.5.1 Lower Overhead than TCP

One of the things that makes UDP nice is its simplicity. Because it does not need to keep track of the sequence of packets, whether they ever made it to their destination, etc., it has lower overhead than TCP. This is another reason why it's more suited to

streaming-data applications: there's less screwing around that needs to be done with making sure all the packets are there, in the right order, and that sort of thing.

1.12.6 Domain Name System (DNS)

DNS is a distributed database system used to match host names with IP addresses. A host normally requests the IP address of a given domain name by sending a UDP message to the DNS server which responds with the IP address or with information about another DNS server.

1.12.7 Telnet

Telnet provides simple terminal access to a host computer. The user is normally authenticated based on user name and password. Both of these are transmitted in plain text over the network however, and is therefore susceptible to capture.

1.12.8 File Transfer Protocols

FTP - The file transfer protocol is one of the most widely and heavily used Internet applications . FTP can be used to transfer both ASCII and binary files. Separate channels are used for commands and data transfer. Anonymous FTP allows external users to retrieve files from a restricted area without prior arrangement or authorisation. By convention users log in with the userid "anonymous" to use this service. Some sites request that the user's electronic mail address be used as the password.

1.13 What is a Network Operating System?

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

1.13.1 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 figure. 1.6). 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.

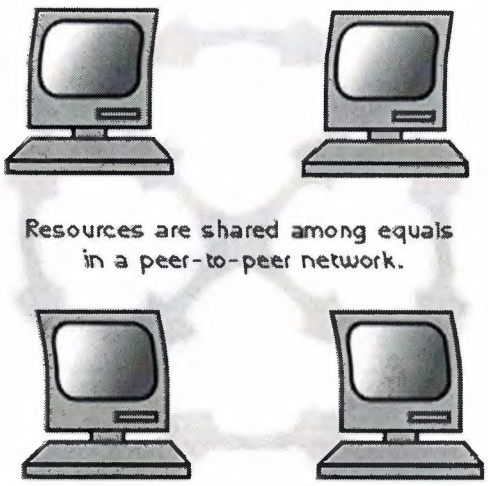


Figure. 1.6 Peer-to-peer network

1.13.1.1 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.

1.13.1.2 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.

1.13.2 Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers (See figure. 1.7). The

CHAPTER 2

NETWORK TOPOLOGY

2.1 overview

In this chapter we will explain types of networks LAN ,MAN ,WAN and explain the network topologies Bus, Star, Ring, Tree, and Mesh , the advantages , disadvantages for every topology , discuss the types of cables used in networks and other related topics.

.2.2 Types of Networks

In this section some useful categorizations of networks are introduced:

1- Categorization by geographical coverage.

2- Categorization by topology.

2.2.1 Categorization By Geographical Coverage

Depending on the distances signals have to travel different technologies are used to run the connections. That's why it makes sense to distinguish computer networks by the area they cover.

2.2.1.1 Local Area Network (LAN)

A LAN is a network that covers a small area only: a house, a factory site, or a small number of near buildings. It has most often only one owner. However, the size restriction is by area only, and not by number! Large companies can easily have hundreds of workstations in a single LAN.

Hence all the computers are nearby, many different ways of designing the cable connection can be applied, and some methods of cabelling can be used, that would be too expensive for long distances. Local Area Networks usually have *a* symmetric

topology. That's why there are many standards (namely those on symmetric topologies as star, ring, bus, etc.) that refer to LANs only.

2.2.1.2 Metropolitan Area Network

A Metropolitan Area Network (MAN) covers larger geographic areas, such as cities or school districts. By interconnecting smaller networks within a large geographic area, information is easily disseminated throughout the network. Local libraries and government agencies often use a MAN to connect to citizens and private industries.

2.2.1.3 Wide Area Network (WAN)

A WAN is a network that covers la large area; typically countries or continents. WANs are used to interconnect LANs over long distances. They usually have an irregular topology.

When examining a WAN the main interest is put on transmission *lines* and the switching elements, but not on the local "ends" of the WAN. Lines and switches together are called the communication subnet (short: subnet); it performs the data exchange in the network.

Besides data exchange in WANs application programs can be run. The machines that do that are referred to as hosts; Hosts perform applications in the network.

2.2.2 Categorization By Topology

Topology: The physical and/or electrical configuration of cabling and

connections comprising a network -- the shape of the system.

Every network has a "shape" which is normally refered to as its topology. There are five major topologies in use today: Bus, Star, Ring, Tree, and Mesh. Each is used for specific network types, although some network types can use more than one topology. For example, Ethernet networks can be laid out in a Bus, Star, or Tree topology, or any combination of the three. Token ring is physically laid out in a Star,

but electrically behaves like a Ring. To properly understand each network type requires first understanding the basic topologies.

2.2.2.1 Bus Topology

A bus topology, shown in Figure 2.1, features all networked nodes interconnected peer-to-peer using a single, open-ended cable. These ends must be terminated with a resistive load--that is, *terminating resistors*. This singe cable can support only a single channel. The cable is called the *bus*.

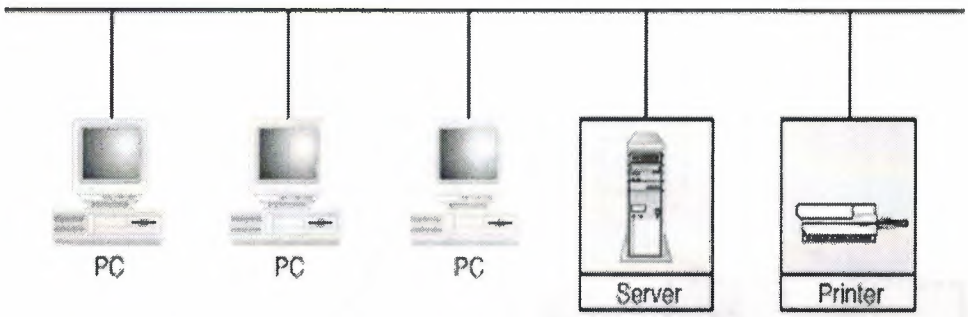


Figure 2.1 Typical bus topology.

The typical bus topology features a single cable, supported by no external electronics, that interconnects all networked nodes peer to peer. All connected devices listen to the bussed transmissions and accept those packets addressed to them. The lack of any external electronics, such as repeaters, makes bus LANs simple and inexpensive. The downside is that it also imposes severe limitations on distances, functionality, and scaleability.

2.2.2.1 .1 Benefits of Bus topology

Bus topology has the following advantage:

- Cabling costs are minimized because of the *common trunk.*

2.2.2.1 .2 Disadvantages of Bus topology

Disadvantages of bus topology are as follows:

- Difficult to trouble shoot because no central distribution points exist.

- Cable breaks can disable the entire segment because they remove the required termination from each of the two cable fragments

2.2.2.2 Star Topology

Star topology LANs have connections to networked devices that radiate out from a common point--that is, the *hub*, as shown in Figure 2.2 Unlike ring topologies, physical or virtual, each networked device in a star topology can access the media independently. These devices have to share the hub's available bandwidth. An example of a LAN with a star topology is Ethernet.

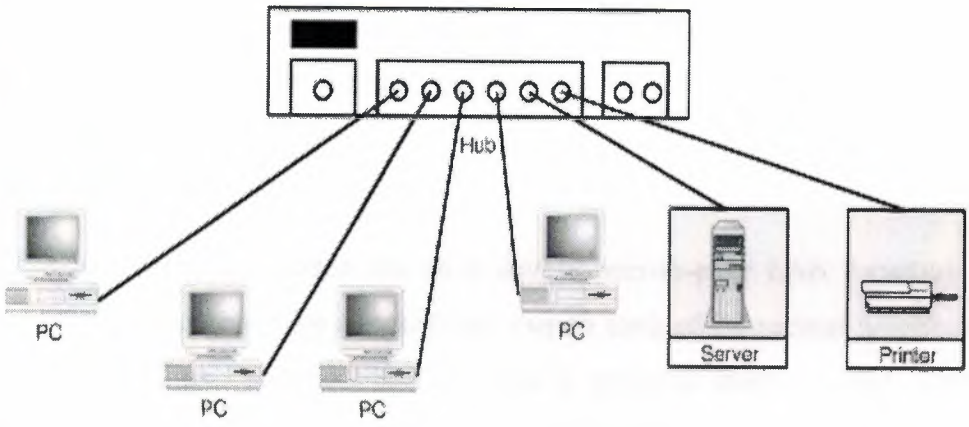


Figure 2.2 Star topology.

A small LAN with a star topology features connections that radiate out from a common point. Each connected device can initiate media access independent of the other connected devices.

2.2.2.2.1 Benefits of Stars

Most modern cabling systems are designed in a star physical topology. The benefits of the star topology are many, including the following:

Each device is isolated on its own cable. This makes it easy to isolate individual devices from the network by disconnecting them from the wiring hub.

All data goes through the central point, which can be equipped with diagnostic devices that make it easy to trouble shoot and manage the network.

- Hierarchical organization allows isolation of traffic on the channel. This is beneficial when several, but not all, computers place a heavy load on the network. Traffic from those heavily used computers can be separated from the rest or dispersed throughout for a more even flow of traffic.

2.2.2.2.2 Disadvantages of Star topology

Star topology has the following disadvantages:

- Because point-to-point wiring is utilized for each node, more cable is required.
- Hub failures can disable large segments of the network.

2.2.2.3 Ring Topology

The ring topology started out as a simple peer-to-peer LAN topology. Each networked workstation had two connections: one to each of its nearest neighbors (see Figure 2.3). The interconnection had to form a physical loop, or ring. Data was transmitted unidirectionally around the ring. Each workstation acted as a repeater, accepting and responding to packets addressed to it, and forwarding on the other packets to the next workstation "downstream."

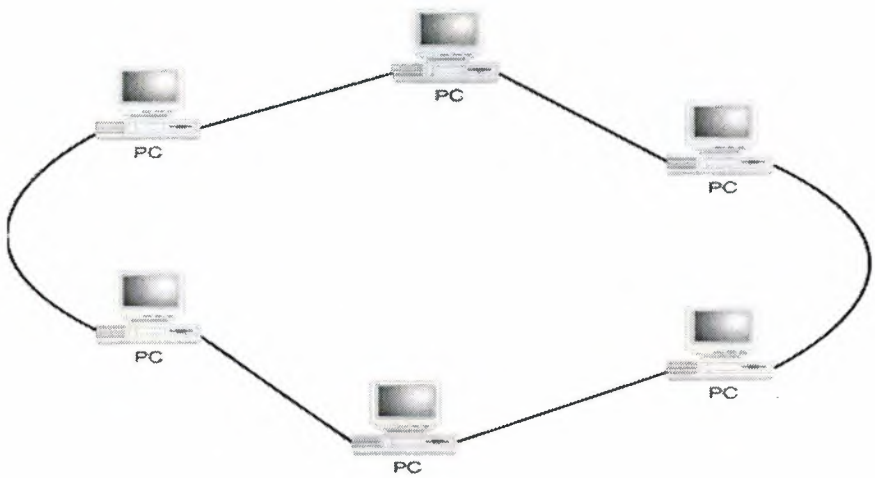


Figure 2.3. Peer-to-peer ring topology.

2.2.2.3.1 Benefits of Ring topology

Ring topology has the following advantage:

- Each repeater duplicates the data signals so that very little signal degradation occurs.

2.2.2.3.2 Disadvantages of Ring topology

Ring topology has the following disadvantages:

- A break in the ring can disable the entire network. Many ring designs incorporate extra cabling that can be switched in if a primary cable fails.
- Because each node must have the capability of functioning as a repeater, the networking devices tend to be more expensive.

2.2.2.4 Tree

A tree topology can be thought of as being a "Star of Stars" network. In a Tree network, each device is connected to its own port on a concentrator in the same manner as in a Star. However, concentrators are connected together in a heirarchial manner a hub will connect to a port on another hub. Look to the Tree network In figure 2.4

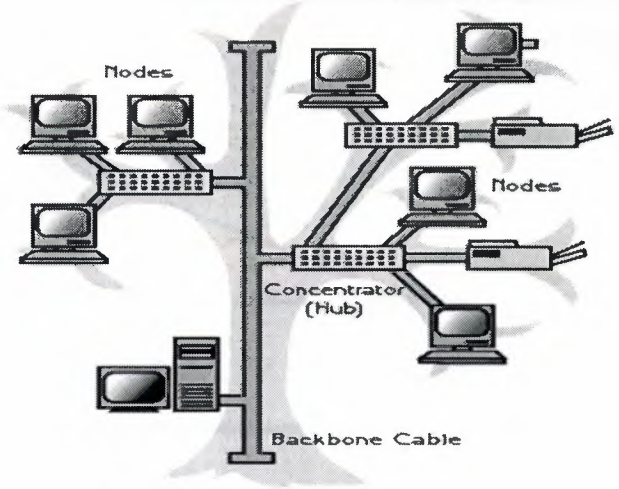


Figure 2.4 A tree topology

2.2.2.4.1 Advantages of a Tree Topology

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

2.2.2.4.2 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.

2.2.2.5 Mesh

A Mesh topology consists of a network where every device on the network is physically connected to every other device on the network. This provides a great deal of performance and reliability, however the complexity and difficulty of creating one increases geometrically as the number of nodes on the network increases. For example, a three or four node mesh network is relatively easy to create, whereas it is impractical to set up a mesh network of 100 nodes -- the number of interconnections would be so ungainly and expensive that it would not be worth the effort. Mesh networks are not used much in local area networks (LANs) but are used in Wide Area Networks (WANs) where reliability is important and the number of sites being connected together is fairly small. The next figure shows an example of a four-node Mesh network. Look to the figure 2.5

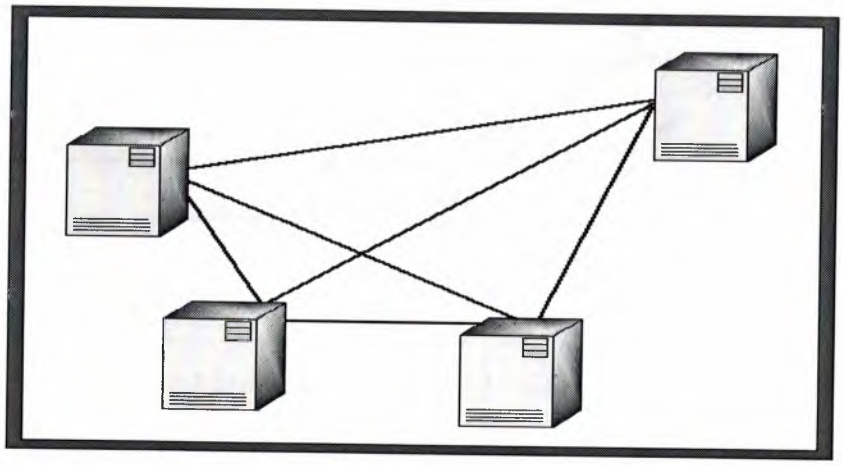


Figure 2.5 A Mesh topology

2.3 What is 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

2.3.1 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 figure. 2.6).

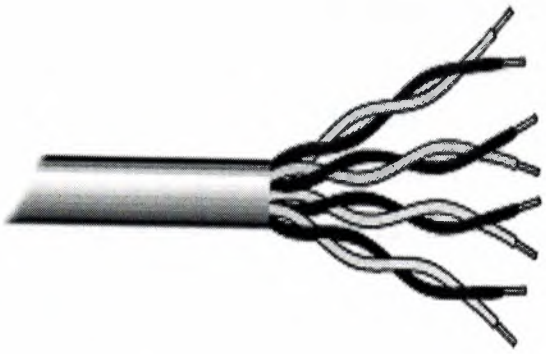


Figure.2.6. Unshielded twisted pair

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.

2.3.1.1Categories of Unshielded Twisted Pair

Table 2.1 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.

2.3.1.2Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See figure. 2.7). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

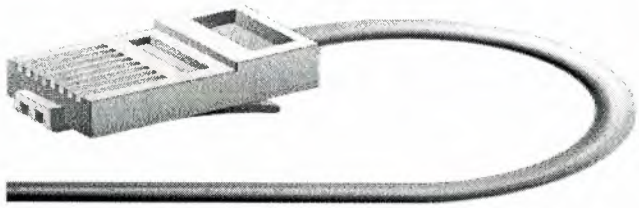


Figure. 2.7 RJ-45 connector

2.3.2 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. See figure 2.8

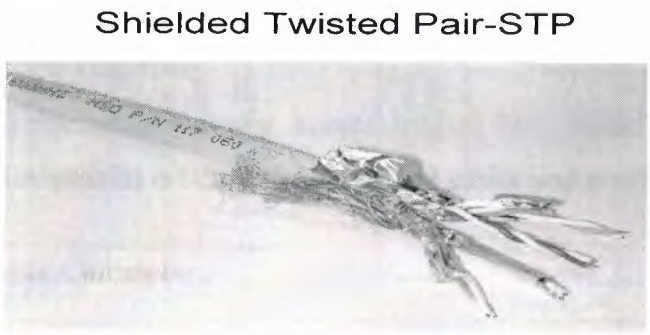


Figure. 2.8

2.3.3 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 figure. 2.9). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

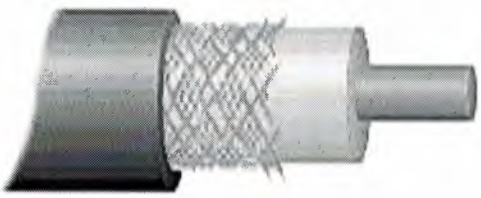


Figure. 2.9. Coaxial cable

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.

2.3.3.1Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See figure. 2.10). 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.

Figure. 2.10 BNC connector

2.3.4 Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See figure. 2.11). 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.

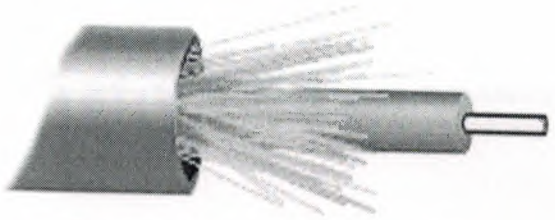


Figure.2.11. Fiber optic cable

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.

2.3.4.1 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.

2.3.5 Ethernet Cable Summary

Table 2.2 Ethernet Cable Summary

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

2.3.6 Wireless LANs

Figure 2.12 Wireless lans

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.

2.3.7 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.

2.4 What is Networking Hardware?

Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network. CLICK on the terms below to learn more about those pieces of networking hardware.

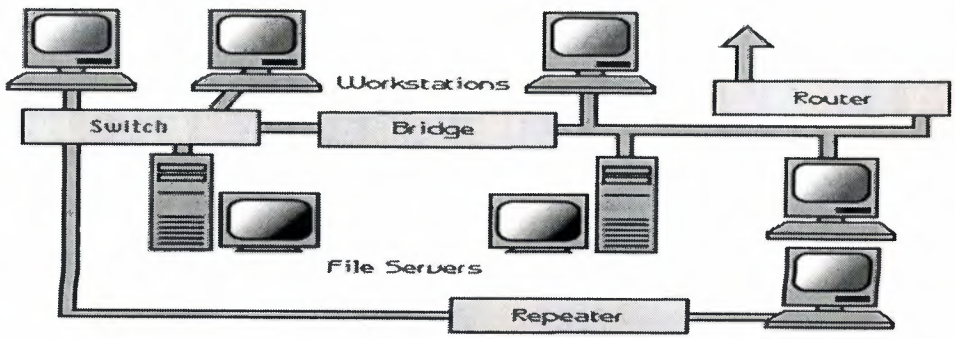


Figure 2.13

This section provides information on the following components:

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

2.4.1 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 of 512 MB of RAM

2.4.2 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.

2.4.3 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 (Sant'Angelo, R. (1995). NetWare Unleashed, Indianapolis, IN: Sams Publishing).

2.4.4 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) . 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.

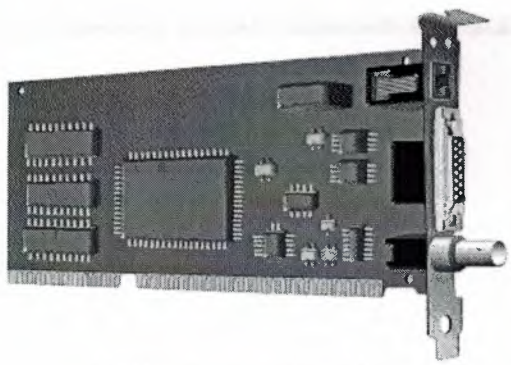


Figure. 2.14 Ethernet card.
From top to bottom:
RJ-45, AUI, and BNC connectors

2.4.5 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)

Table 2.3 LocalTalk connectors

Ethernet Cards vs. LocalTalk Connections	
Ethernet	**LocalTalk**
Fast data transfer (10 to 100 Mbps)	Slow data transfer (.23 Mbps)
Expensive - purchased separately	Built into Macintosh computers
Requires computer slot	No computer slot necessary
Available for most computers	Works only on Macintosh computers

2.5 Network Architectures

2.5.1 Ethernet

- Baseband signaling.
- Linear or star-bus topology.
- Usually transmits at 10 Mbps with 100 Mbps possible.
- Uses CSMA/CD for traffic regulation.
- IEEE specification 802.3.
- Uses thicknet, thinnet or UTP cabling
- Media is passive => it draws power from the computer

2.5.2 Ethernet Frames

Ethernet breaks data into frames. A frame can be from 64 to 1,518 bytes long in total. The Ethernet frame itself takes up 18 bytes, so the actual data can be from 46 to 1,500 bytes.

- Preamble: marks the start of a frame.
- Destination and Source: addressing information.

- Type: Identifies network layer protocol.
- CRC: error checking data.

2.6 Network Hardware

Some components can be installed which will increase the size of the network within the confines of the limitations set by the topology. These components can:

- Segment existing LANs so that each segment becomes its own LAN.
- Join two separate LANs.
- Connect to other LANs and computing environments to join them into a larger comprehensive network.

2.6.1 Modems

- Modems share these characteristics
    - a serial (RS-232) interface
    - an RJ-11C telephone line connector
- Telephones use analog signal; computers use digital signal. A modem translates between the two
- BAUD refers to the speed of the oscillation of the sound wave on which a bit of data is carried over the telephone wire
- The BPS can be greater than the baud rate due to compression and encode data so that each modulation of sound can carry more than one bit of data is carried over the telephone line. For example, a modem that modulates at 28,000 baud can actually send at 115,200 bps => bps is the most important parameter when looking at throughput.
- There are 2 types of modems

2.6.1.1 Asynchronous Communications (Async)

- use common phone lines
- data is transmitted in a serial stream
- not synchronized, no clocking device => no timing
- both sending and receiving devices must agree on a start and stop bit sequence

- error control
    - a parity bit is used in an error checking and correction scheme called parity checking
    - It checks to see if the # of bits sent = # of bits received
    - The receiving computer checks to make sure that the received data matches what was sent.
    - 25 % of the data traffic in async communications consists of data control and coordination
    - MNP (Microcom Network Protocol) has become the standard for error control
    - Later LAPM (Link Access Procedure for Modems) is used in V.42 modems (57,600 baud).
        - It uses MNP Class 4.
        - LAPM is used between two modems that are V.42 compliant
        - If one or the other modems is MNP 4 - compliant, the correct protocol would be MNP Class 4
- Communication performance depends on
    1. signaling or channel speed - how fast the bits are encoded onto the communications channel
    2. throughput - amount of useful information going across the channel
        - You can double the throughput by using compression. One current data compression standard is the MNP Class 5 compression protocol
        - V.42 bis is even faster because of compression.
            - bis => second modification
            - terbo => third, the bis standard was modified
- This is a good combination:
    0. V.32 signaling
    1. V.42 error control
    2. V.42bis compression

2.6.1.2 Synchronous Communication

- relies on a timing scheme coordinated between two devices to separate groups of bits and transmit them in blocks known as frames
- NO start and stop bits =. A continuous stream of data because both know when the data starts and stops.
- if there's error, the data is retransmitted
- some synchronous protocol perform the following that asynchronous protocols don't:
    1. format data into blocks
    2. add control info
    3. check the info to provide error control
- the primary protocols in synchronous communication are:
    1. Synchronous data link control (SDLC)
    2. High-level data link control (HDLC)
    3. binary synchronous communication protocol (bisync)
- Synchronous communications are used in almost all digital and network communications
- 2 types of telephone lines:
    1. public dial network lines (dial-up lines) - manually dial up to make a connection
    2. leased (dedicated) lines - full time connection that do not go through a series of switches, 56 Kbps to 45 Mbps

2.6.2 Repeaters

- Repeaters
    - EXTEND the network segment by REGENERATING the signal from one segment to the next
    - Repeaters regenerate BASEBAND, digital signals
    - Don't translate or filter anything
    - Is the least expensive alternative
    - Work at the Physical layer of OSI

- Both segments being connected must use the same access method e.g. an 802.3 CSMA/CD (Ethernet) LAN segment can't be joined to an 802.5 (Token Ring) LAN segment. Another way of saying this is the Logical Link Protocols must be the same in order to send a signal.
- BUT repeaters CAN move packets from one physical medium to another: for example can take an Ethernet packet from a thinnet coax and pass it on to a fiber-optic segment. Same access method is being used on both segments, just a different medium to deliver the signal
- They send every bit of data on => NO FILTERING, so they can pass a broadcast storm along from on segment to the next and back. So you want to use a repeater when there isn't much traffic on either segment you are connecting.
- There are limits on the number of repeaters that can be used. The repeater counts as a single node in the maximum node count associated with the Ethernet standard [30 for thin coax].
- Repeaters also allow isolation of segments in the event of failures or fault conditions. Disconnecting one side of a repeater effectively isolates the associated segments from the network.
- Using repeaters simply allows you to extend your network distance limitations. It does not give you any more bandwidth or allow you to transmit data faster.
- Why only so many repeaters are allowed on a single network: "propagation delay". In cases where there are multiple repeaters on the same network, the brief time each repeater takes to clean up and amplify the signal, multiplied by the number of repeaters can cause a noticeable delay in network transmissions.
- It should be noted that in the above diagram, the network number assigned to the main network segment and the network number assigned to the other side of the repeater are the same.
- In addition, the traffic generated on one segment is propagated onto the other segment. This causes a rise in the total amount of traffic, so if the network segments are already heavily loaded, it's not a good idea to use a repeater.
- A repeater works at the Physical Layer by simply repeating all data from one segment to another.

2.6.2.1 Repeater features

- increase traffic on segments
- limitations on the number that can be used
- propagate errors in the network
- cannot be administered or controlled via remote access
- no traffic isolation or filtering

2.6.3 Bridges

- have all the abilities of a repeater
- Bridges can
  - take an overloaded network and split it into two networks, therefore they can divide the network to isolate traffic or problems and reduce the traffic on both segments
  - expand the distance of a segment
  - link UNLIKE PHYSICAL MEDIA such as twisted-pair (10Base T) and coaxial Ethernet (10Base2)
  - VERY IMPORTANT: they can link UNLIKE ACCESS CONTROL METHODS, on different segments such as Ethernet and Token Ring and forward packets between them. Exam Cram says this is a Translation Bridge that can do this - not all bridges - but my observation is questions don't necessarily mention the distinction.

- Bridges work at the Data Link Layer of the OSI model => they don't distinguish one protocol from the next and simply pass protocols along the network. (use a bridge to pass NetBEUI, a non-routable protocol, along the network)
- Bridges actually work at the MEDIA ACCESS CONTROL (MAC) sublayer. In fact they are sometimes called Media Access Control layer bridges. Here's how they deal with traffic:
  - They listen to all traffic. Each time the bridge is presented with a frame, the source address is stored. The bridge builds up a table which identifies the segment to which the device is located on. This internal table is then used to determine which segment incoming frames should be forwarded

to. The size of this table is important, especially if the network has a large number of workstations/servers.

- they check the source and destination address of each PACKET
- They build a routing table based on the SOURCE ADDRESSES. Soon they know which computers are on which segment
- Bridges are intelligent enough to do some routing:
  - If the destination address is on the routing table and is on the SAME SEGMENT, the packet isn't forwarded. Therefore, the bridge can SEGMENT network traffic
  - If the destination address is the routing table, and on a remote segment, the bridge forwards the packet to the correct segment
  - If the destination address ISN'T on the routing table, the bridge forwards the packet to ALL segments.
  - BRIDGES SIMPLY PASS ON BROADCAST MESSAGES, SO they too contribute to broadcast storms and don't help to reduce broadcast traffic

- Remote Bridges
  - two segments are joined by a bridge on each side, each connected to a synchronous modem and a telephone line
  - there is a possibility that data might get into a continuous loop between LANs
  - The SPANNING TREE ALGORITHM (STA)
    - senses the existence of more than one route
    - determines which is the most efficient and
    - configures the bridge to use that route
    - This route can be altered if it becomes unusable.
    - Transparent bridges (also known as spanning tree, IEEE 802.1 D) make all routing decisions. The bridge is said to be transparent (invisible) to the workstations. The bridge will automatically initialize itself and configure its own routing information after it has been enabled.
- Comparison of Bridges and Repeaters
  - Bridges

        - regenerate data at the packet level
        - accommodate more nodes than repeaters
        - provide better network performance than repeaters because they segment the network
- Implementing a Bridge
    - it can be an external, stand-alone piece of equipment
    - or be installed on a server

2.6.4 Routers

- Determine the best path for sending data and filtering broadcast traffic to the local segment. They DON'T pass on broadcast traffic
- work at the Network layer of OSI => they can switch and route packets across network segments
- They provide these functions of a bridge
    - filtering and isolating traffic
    - connecting network segments
- routing table contains
    1. all known network addresses
    2. how to connect to other networks
    3. possible paths between those routers
    4. costs of sending data over those paths
    5. not only network addresses but also media access control sublayer addresses for each node
- Routers
    - REQUIRE specific addresses: they only understand network numbers which allow them to talk to other routers and local adapter card addresses
    - Only pass Packets to the network segment they are destined for.
    - routers don't talk to remote computers, only to other routers
    - they can segment large networks into smaller ones
    - they act as a safety barrier (firewall) between segments
    - they prohibit broadcast storms, because broadcasts and bad data aren't forwarded
    - are slower than most bridges

- can join dissimilar access methods: a router can route a packet from a TCP/IP Ethernet network to a TCP/IP Token Ring network

- Routers don't look at the destination computer address. They only look at the NETWORK address and they only pass on the data if the network address is known => less traffic

- Routable protocols:
  - DECnet, IP, IPX, OSI, XNS, DDP (Apple)
  - Routable protocols have Network *layer addressing embedded*
- Non-routable protocols:
  - LAT, NetBEUI, DLC
  - Non-routable protocols don't have network layer addressing

2.6.4.1 Choosing Paths

- routers can choose the best path for the data to follow
- Routers can accommodate multiple active paths between LAN segments. To determine the best path, it takes these things into account:
  - If one path is down, the data can be forwarded over on alternative route
  - Routers can listen and determine which parts *of the network are busiest.*
  - it decides the path the data packet will follow by determining the number of hops between internetwork segments
- OSPF (Open Shortest Path First)
  - is a link-state routing algorithm
  - routes are calculated based on
    - # of hops
    - line speed
    - traffic
    - cost
  - TCP/IP supports OSPF
  -
- RIP (Routing Information Protocol)
  - RIP is the protocol used to determine the # of hops to a distant segment.
  - uses distance-vector algorithm to determine routes

- TCP/IP & IPX support RIP
- NLSP (NetWare Link Services Protocol)
  - is a link-state algorithm for use with IPX
- There are 2 types of routers
  - Static - manually setup and configure the routing table and to specify each route
  - Dynamic
    - automatic discovery of routers
    - use information from other routers

2.6.5 Brouters

- Combine the best qualities of both bridges and routers
- First, a brouter checks to see if the protocol is routable or non-routable
- Route selected routable protocols.
- They can bridge non-routable protocols. Like a Bridge, they use the MAC address to forward to destination. They act like a router for one protocol and a bridge for all the others
- More cost effective than individual bridges and routers.
- SO, use a brouter when you have routable and non-routable protocols.

2.6.6 Hubs

There are many types of hubs:

- Passive hubs are don't require power and are simple splitters or combiners that group workstations into a single segment
- Active hubs require power and include a repeater function and are thus capable of supporting many more connections.
- Intelligent hubs provide
  - packet switching
  - traffic routing

2.6.7 Gateways

- The TRANSLATOR -- allows communications between dissimilar systems or environments
- A gateway is usually a computer running gateway software connecting two different segments. For example an Intel-based PC on one segment can both communicate and share resources with a Macintosh computer or an SNA mainframe. Use gateways when different environments need to communicate. One common use for gateways is to translate between personal computers and mainframes
- GSNW is a gateway to allow Microsoft clients using SMB to connect to a NetWare server using NCP.
- Gateways work at the Application --> Transport layer
- They make communication possible between different architectures and environments
- They perform protocol AND data conversion / translation.
- they takes the data from one environment, strip it, and re-package it in the protocol stack from the destination system
- they repackage and convert data going from one environment to another so that each environment can understand the other environment's data
- gateway links two systems don't use the same
    1. protocols
    2. data formatting structure
    3. languages
    4. architecture
- they are task specific in that they are dedicated to a specific type of conversion: e.g. "Windows NT Server -> SNA Server Gateway"
- Usually one computer is designated as the gateway computer. This adds a lot of traffic to that segment
- Disadvantages
    - They slow things down because of the work they do
    - they are expensive
    - difficult to configure

- Remember, gateways can translate
    - protocols e.g. IPX/SPX --> TCP/IP
    - and data (PC --> Mac)
    - E-mail standards --> an e-mail gateway that translates on e-mail format into another (such as SMTP) to route across the Internet.

2.7 WAN Transmission

Communication between LANs over a WAN link will involve one of these technologies

- Analog
    - These use conventional telephone lines, with voice signaling (modem) technologies
- Digital
    - These use digital grade telephone lines, with digital technologies all the way
- Packet Switching
    - These use multiple sets of links between sender and receiver to move data

2.7.1 Analog

- dial-up line
    - via public switched telephone network (PSTN)
    - requires modems which are slow
    - inconsistent quality of service
- dedicated line
    - fast
    - reliable
    - expensive
    - service provider can implement line conditioning (a service that reduces delay and noise on the line, allowing for better transmissions) can make the leased lines even more reliable,

2.7.2 Digital

- Digital Data Service (DDS) provide point-to-point synchronous communications at:
    - 2.4 Kbps
    - 4.8 Kbps
    - 9.6 Kbps or
    - 56 Kbps
- guarantees full-duplex bandwidth by setting up a permanent link from each endpoint
- 99% error free
- Doesn't requires modem, requires bridge or router through a device called a CSU/DSU. This device translates standard digital signals a computer generates into bipolar digital signals used by synchronous communications
- Available in several forms:

2.7.3 T1

- Point to point transmission => no switching
- uses two-wire pairs (1 pair to send, 1 to receive)
- full-duplex signal at 1.544 Mbps
- Used to transmit digital, voice, data and video signals
- multiplexing - signals from different source are collected into a component called a multiplexer and fed into one cable 8,000 times a second
- A T1 divides into 24 64 Kbps channels. Subscribers can lease one 64 Kbps channel known as a Fractional T-1.
    - Each channel can transmit at 64 Kbps. This is called a DS-0
    - the whole 1.544 Mbps is known as DS-1
- Connecting a T1 line to your network is similar to a connecting a DDS or frame relay line. You will need a T1-compatible CSU/DSU, and a bridge or router. To distribute the T1's bandwidth between voice and data traffic, you will need a multiplexer/demultiplexer to combine voice and data signals for transmission, and separate them upon reception.

2.7.4 T3

equivalent to 28 T-1 lines

- T3 and Fractional T-3 leased line service provides voice and data service from 6 Mbps to 45 Mbps
- REALLY expensive
- T-1 uses copper wire, while T-3 uses fiber optic cables or microwave transmission equipment.

2.7.5 Switched 56

- In reality, a Switched 56 line is nothing more than a circuit-switched version of a standard 56 Kbps DDS leased line. As customers pay only for connection time, resulting costs are usually significantly lower than those of a dedicated line.
- is a LAN to LAN digital dial-up service
- Used on demand => not dedicated => less expensive.
- Both ends must be equipped with a Switched 56 compatible CSU/DSU to dial-up another switched 56 site.

2.7.6 Packet Switching

- Switching (as in switched connections) refers to finding a path for data transmission across a number of potential links between sender and receiver. On the other hand, analog and digital connections require a fixed connection to exist, at least for the duration of each communication session. Switching methods include both circuit switching and packet switching. Essentially, when data is received on an incoming line, the switching device must find an appropriate outgoing line on which to forward it. These switching devices are usually called routers, based on the functions they perform.
- Data package is broken into packers and each package is tagged with a destination address and other info.

- relayed through stations in a computer network
- Data paths for individual packets depend on the best route at any given instant. The main point is that the small, individual packets are all take their own route to the destination, and an error in any one of them is easier to correct than a huge chunk of data
- These networks are sometimes called "any to any networks"
- Can use a virtual circuit
    - logical connection between the sending computer and the receiving computer
    - not actual cable, but bandwidth used on demand .

CHAPTER 3

ROUTING

3.1 Overview

This chapter introduces the underlying concepts widely used in routing protocols. Topics summarized here include routing protocol components and algorithms. In addition, the role of routing protocols is briefly contrasted with the role of routed or network protocols. Subsequent chapter, "Routing Protocols," address specific routing protocols in more detail, while the optimization problem are discussed at the 4th chapter of this project.

3.2 what is Router?

Is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways(A node on a network that serves as an entrance to another network), the places where two or more networks connect.

Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols such as ICMP to communicate with each other and configure the best route between any two hosts.

Very little filtering of data is done through routers.

The Internet is one of the 20th century's greatest communications developments. It allows people around the world to send e-mail to one another in a matter of seconds, and it lets you read, among other things, the articles on HowStuffWorks.com. We're all used to seeing the various parts of the Internet that come into our homes and offices -- the Web pages, e-mail messages and downloaded files that make the Internet a dynamic and valuable medium. But none of these parts would ever make it to your computer without a piece of the Internet that you've probably never seen. In fact, most people have never stood "face to machine" with the technology most responsible for allowing the Internet to exist at all: the router

Routers are specialized computers that send your messages and those of every other Internet user speeding to their destinations along thousands of pathways. In this article, we'll look at how these behind-the-scenes machines make the Internet work.

3.3 History

1. In the old ARPANET, routing was static.

2. As the ARPANET grew, the routing became more dynamic, but with all routers sharing a single protocol.

3. As the Internet became the "network of networks" routing was separated into interior and exterior domains.

– Each AS could determine the IGP that suited it best

– A standard EGP was used between AS's

4. Today

– RIP and OSPF are the most widely used IGP's

– IS-IS is another IGP that is generally available

– EGP was the first EGP (confused?) but has been replaced with BGP (which is now in version 4)

Figure 3.1. Example Routing Architecture

3.4 How Routers Work?

It's said that it to remain constant for the duration of the call. This circuit approach means that the quality Keeping the Messages Moving When you send e-mail to a friend on the other side of the country, how does the message know to end up on your friend's computer, rather than on one of the millions of other computers in the world? Much of the work to get a message from one computer to another is done by routers, because they're the crucial devices that let messages flow between networks, rather than within networks.

Let's look at what a very simple router might do. Imagine a small company that makes animated 3-D graphics for local television stations. There are 10 employees of the company, each with a computer. Four of the employees are animators, while the rest are in sales, accounting and management. The animators will need to send lots of very large files back and forth to one another as they work on projects. To do this, they'll use a network.

When one animator sends a file to another, the very large file will use up most of the network's capacity, making the network run very slowly for other users. One of the reasons that a single intensive user can affect the entire network stems from the way that Ethernet works. Each information packet sent from a computer is seen by all the other computers on the local network. Each computer then examines the packet and decides whether it was meant for its address. This keeps the basic plan of the network simple, but has performance consequences as the size of the network or level of network activity increases. To keep the animators' work from interfering with that of the folks in the front office, the company sets up two separate networks, one for the animators and one for the rest of the company. A router links the two networks and connects both networks to the Internet.

Directing Traffic The router is the only device that sees every message sent by any computer on either of the company's networks. When the animator in our example sends a huge file to another animator, the router looks at the recipient's address and keeps the traffic on the animator's network. When an animator, on the other hand, sends a message to the bookkeeper asking about an expense-account check, then the router sees the recipient's address and forwards the message between the two networks.

One of the tools a router uses to decide where a packet should go is a **configuration table**. A configuration table is a collection of information, including:

- Information on which connections lead to particular groups of addresses
- Priorities for connections to be used
- Rules for handling both routine and special cases of traffic

A configuration table can be as simple as a half-dozen lines in the smallest routers, but can grow to massive size and complexity in the very large routers that handle the bulk of Internet messages.

A router, then, has two separate but related jobs:

- The router ensures that information doesn't go where it's not needed. This is crucial for keeping large volumes of data from clogging the connections of "innocent bystanders."
- The router makes sure that information does make it to the intended destination.

In performing these two jobs, a router is extremely useful in dealing with two separate computer networks. It joins the two networks, passing information from one to the other and, in some cases, performing translations of various protocols between the two networks. It also protects the networks from one another, preventing the traffic on one from unnecessarily spilling over to the other. As the number of networks attached to one another grows, the configuration table for handling traffic among them grows, and the processing power of the router is increased. Regardless of how many networks are attached, though, the basic operation and function of the router remains the same. Since the Internet is one huge network made up of tens of thousands of smaller networks, its use of routers is an absolute necessity.

Transmitting Packets When you make a telephone call to someone on the other side of the country, the telephone system establishes a stable circuit between your telephone and the telephone you're calling. The circuit might involve a half dozen or more steps through copper cables, switches, fiber optics, microwaves and satellites, but those steps are established of the line between you and the person you're calling is consistent throughout the call, but a problem with any portion of the circuit -- maybe a tree falls across one of the lines used, or there's a power problem with a switch -- brings your call to an early and abrupt end. When you send an e-mail message with an attachment to the other side of the country, a very different process is used.

Internet data, whether in the form of a Web page, a downloaded file or an e-mail message, travels over a system known as a packet-switching network. In this system, the data in a message or file is broken up into packages about 1,500 bytes long. Each of

these packages gets a wrapper that includes information on the sender's address, the receiver's address, the package's place in the entire message, and how the receiving computer can be sure that the package arrived intact. Each data package, called a packet, is then sent off to its destination via the best available route -- a route that might be taken by all the other packets in the message or by none of the other packets in the message. This might seem very complicated compared to the circuit approach used by the telephone system, but in a network designed for data there are two huge advantages to the packet-switching plan.

- The network can balance the load across various pieces of equipment on a millisecond-by-millisecond basis.
- If there is a problem with one piece of equipment in the network while a message is being transferred, packets can be routed around the problem, ensuring the delivery of the entire message.

The Path of a Packet The routers that make up the main part of the Internet can reconfigure the paths that packets take because they look at the information surrounding the data packet, and they tell each other about line conditions, such as delays in receiving and sending data and traffic on various pieces of the network. Not all routers do so many jobs, however. Routers come in different sizes. For example:

- If you have enabled Internet connection sharing between two Windows 98-based computers, you're using one of the computers (the computer with the Internet connection) as a simple router. In this instance, the router does so little -- simply looking at data to see whether it's intended for one computer or the other -- that it can operate in the background of the system without significantly affecting the other programs you might be running.
- Slightly larger routers, the sort used to connect a small office network to the Internet, will do a bit more. These routers frequently enforce rules concerning security for the office network (trying to secure the network from certain attacks). They handle enough traffic that they're generally stand-alone devices rather than software running on a server.
- The largest routers, those used to handle data at the major traffic points on the Internet, handle millions of data packets every second and work to configure the

network most efficiently. These routers are large stand-alone systems that have far more in common with supercomputers than with your office server.

Routing Packets: An Example Let's take a look at a medium-sized router -- the router we use in the HowStuffWorks office. In our case, the router only has two networks to worry about: The office network, with about 50 computers and devices, and the Internet. The office network connects to the router through an Ethernet connection, specifically a 100 base-T connection (100 base-T means that the connection is 100 megabits per second, and uses a twisted-pair cable like an 8-wire version of the cable that connects your telephone to the wall jack). There are two connections between the router and our ISP (Internet service provider). One is a T-1 connection that supports 1.5 megabits per second. The other is an ISDN line that supports 128 kilobits per second. The configuration table in the router tells it that all out-bound packets are to use the T-1 line, unless it's unavailable for some reason (perhaps a backhoe digs up the cable). If it can't be used, then outbound traffic goes on the ISDN line. This way, the ISDN line is held as "insurance" against a problem with the faster T-1 connection, and no action by a staff member is required to make the switch in case of trouble. The router's configuration table knows what to do.

In addition to routing packets from one point to another, the HowStuffWorks router has rules limiting how computers from outside the network can connect to computers inside the network, how the HowStuffWorks network appears to the outside world, and other **security** functions. While most companies also have a special piece of hardware or software called a firewall to enforce security, the rules in a router's configuration table are important to keeping a company's (or family's) network secure.

One of the crucial tasks for any router is knowing when a packet of information stays on its local network. For this, it uses a mechanism called a subnet mask. The subnet mask looks like an IP address and usually reads "255.255.255.0." This tells the router that all messages with the sender and receiver having an address sharing the first three groups of numbers are on the same network, and shouldn't be sent out to another network. Here's an example: The computer at address 15.57.31.40 sends a request to the computer at 15.57.31.52. The router, which sees all the packets, matches the first three

groups in the address of both sender and receiver (15.57.31), and keeps the packet on the local network.

Between the time these words left the Howstuffworks.com server and the time they showed up on your monitor, they passed through several routers (it's impossible to know ahead of time exactly how many "several" might be) that helped them along the way. It's very similar to the process that gets a postal letter from your mailbox to the mailbox of a friend, with routers taking the place of the mail sorters and handlers along the way.

Knowing Where to Send Data Routers are one of several types of devices that make up the "plumbing" of a computer network. Hubs, switches and routers all take signals from computers or networks and pass them along to other computers and networks, but a router is the only one of these devices that examines each bundle of data as it passes and makes a decision about exactly where it should go. To make these decisions, routers must first know about two kinds of information: addresses and network structure.

When a friend mails a birthday card to be delivered to you at your house, he probably uses an address that looks something like this:

The address has several pieces, each of which helps the people in the postal service move the letter along to your house. The ZIP code can speed the process up; but even without the ZIP code, the card will get to your house as long as your friend includes your state, city and street address. You can think of this address as a logical address because it describes a way someone can get a message to you. This logical address is connected to a physical address that you generally only see when you're buying or selling a piece of property. The survey plot of the land and house, with latitude, longitude or section bearings, gives the legal description, or address, of the property

3.5 Routing Components

Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork. In

the context of the routing process, the latter of these is referred to as packet switching. Although packet switching is relatively straightforward, path determination can be very complex.

3.5.1 Path Determination

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth, that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with a variety of information. Destination/next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the "next hop" on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop. depicts a sample destination/next hop routing table.

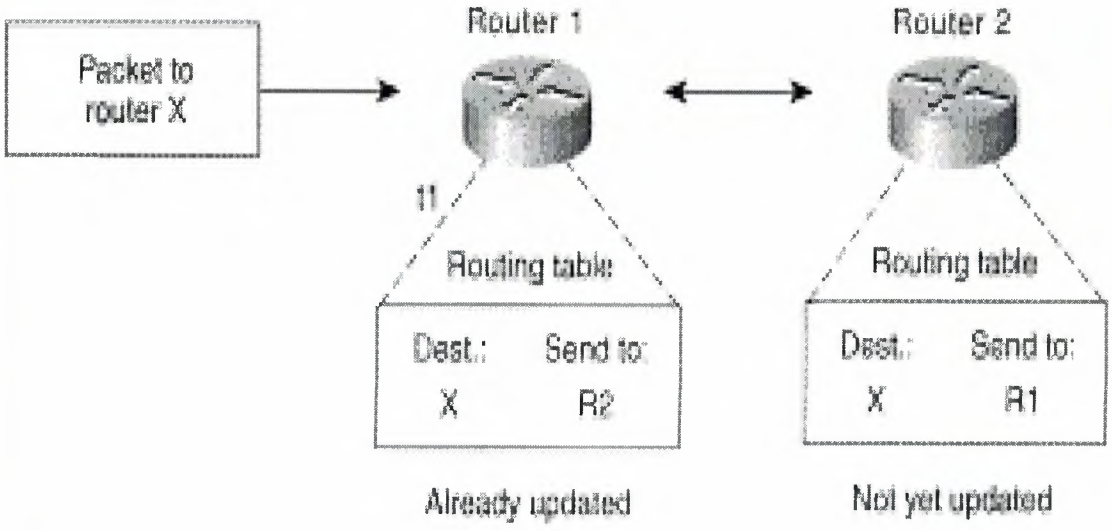


Figure 3.2 : Destination/Next Hop Associations Determine the Data's Optimal Path

Routing tables also can contain other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these

metrics differ depending on the design of the routing algorithm used. A variety of common metrics will be introduced and described later in this chapter.

Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A link-state advertisement, another example of a message sent between routers, informs other routers of the state of the sender's links. Link information also can be used to build a complete picture of network topology to enable routers to determine optimal routes to network destinations.

3.5.2 Switching

Switching algorithms is relatively simple; it is the same for most routing protocols. In most cases, a host determines that it must send a packet to another host. Having acquired a router's address by some means, the source host sends a packet addressed specifically to
a router's physical (Media Access Control [MAC]-layer) address, this time with the protocol (network layer) address of the destination host.

As it examines the packet's destination protocol address, the router determines that it either knows or does not know how to forward the packet to the next hop. If the router does not know how to forward the packet, it typically drops the packet. If the router knows how to forward the packet, however, it changes the destination physical address to that of the next hop and transmits the packet.

The next hop may be the ultimate destination host. If not, the next hop is usually another router, which executes the same switching decision process. As the packet moves through the internetwork, its physical address changes, but its protocol address remains constant

The preceding discussion describes switching between a source and a destination end system. The International Organization for Standardization (ISO) has developed a hierarchical terminology that is useful in describing this process. Using this

terminology, network devices without the capability to forward packets between subnetworks are called end systems (ESs), whereas network devices with these capabilities are called intermediate systems (ISs). ISs are further divided into those that can communicate within routing domains (intradomain ISs) and those that communicate both within and between routing domains (interdomain ISs). A routing domain generally is considered a portion of an internetwork under common administrative authority that is regulated by a particular set of administrative guidelines. Routing domains are also called autonomous systems. With certain protocols, routing domains can be divided into routing areas, but intradomain routing protocols are still used for switching both within and between areas

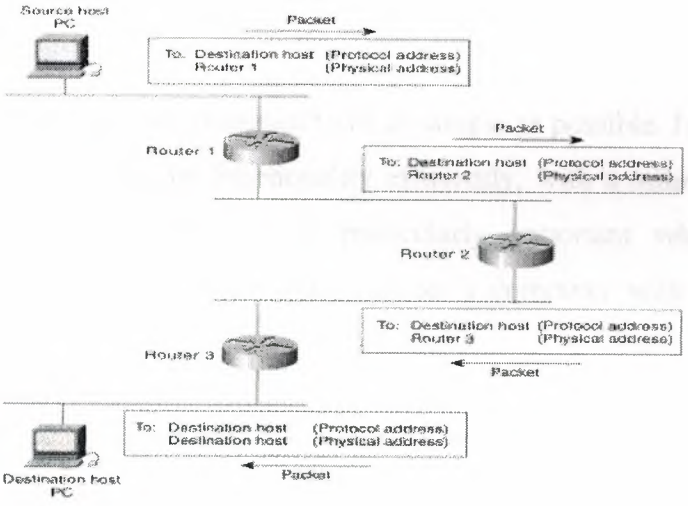


Figure 3.3: Numerous Routers May Come into Play During the Switching Process

3.6 Routing Algorithms

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

3.6.1 Design Goals

Routing algorithms often have one or more of the following design goals:

- Optimality
- Simplicity and low overhead
- Robustness and stability
- Rapid convergence
- Flexibility

Optimality refers to the capability of the routing algorithm to select the best route, which depends on the metrics and metric weightings used to make the calculation. For example, one routing algorithm may use a number of hops and delays, but it may weigh delay more heavily in the calculation. Naturally, routing protocols must define their metric calculation algorithms strictly.

Routing algorithms also are designed to be as simple as possible. In other words, the routing algorithm must offer its functionality efficiently, with a minimum of software and utilization overhead. Efficiency is particularly important when the software implementing the routing algorithm must run on a computer with limited physical resources.

Routing algorithms must be robust,which means that they should perform correctly in the face of unusual or unforeseen circumstances, such as hardware failures, high load conditions, and incorrect implementations. Because routers are located at network junction points, they can cause considerable problems when they fail. The best routing algorithms are often those that have withstood the test of time and that have proven stable under a variety of network conditions.

In addition, routing algorithms must converge rapidly. Convergence is the process of agreement, by all routers, on optimal routes. When a network event causes routes to either go down or become available, routers distribute routing update messages that permeate networks, stimulating recalculation of optimal routes and eventually causing all routers to agree on these routes. Routing algorithms that converge slowly can cause routing loops or network outages.

In the routing loop a packet arrives at Router 1 at time t1. Router 1 already has been updated and thus knows that the optimal route to the destination calls for Router 2 to be the next stop. Router 1 therefore forwards the packet to Router 2, but because this router has not yet been updated, it believes that the optimal next hop is Router 1. Router 2 therefore forwards the packet back to Router 1, and the packet continues to bounce back and forth between the two routers until Router 2 receives its routing update or until the packet has been switched the maximum number of times allowed.

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

3.6.2 Routing Metrics

Routing tables contain information used by switching software to select the best route. But how, specifically, are routing tables built? What is the specific nature of the information that they contain? How do routing algorithms determine that one route is preferable to others?

Routing algorithms have used many different metrics to determine the best route. Sophisticated routing algorithms can base route selection on multiple metrics, combining them in a single (hybrid) metric. All the following metrics have been used:

- Path length
- Reliability
- Delay
- Bandwidth
- Load
- Communication cost

Path length is the most common routing metric. Some routing protocols allow network administrators to assign arbitrary costs to each network link. In this case, path

length is the sum of the costs associated with each link traversed. Other routing protocols define hop count, a metric that specifies the number of passes through internetworking products, such as routers, that a packet must take en route from a source to a destination.

Reliability, in the context of routing algorithms, refers to the dependability (usually described in terms of the bit-error rate) of each network link. Some network links might go down more often than others. After a network fails, certain network links might be repaired more easily or more quickly than other links. Any reliability factors can be taken into account in the assignment of the reliability ratings, which are arbitrary numeric values usually assigned to network links by network administrators.

Routing delay refers to the length of time required to move a packet from source to destination through the internetwork. Delay depends on many factors, including the bandwidth of intermediate network links, the port queues at each router along the way, network congestion on all intermediate network links, and the physical distance to be traveled. Because delay is a conglomeration of several important variables, it is a common and useful metric.

Bandwidth refers to the available traffic capacity of a link. All other things being equal, a 10-Mbps Ethernet link would be preferable to a 64-kbps leased line. Although bandwidth is a rating of the maximum attainable throughput on a link, routes through links with greater bandwidth do not necessarily provide better routes than routes through slower links. For example, if a faster link is busier, the actual time required to send a packet to the destination could be greater.

Load refers to the degree to which a network resource, such as a router, is busy. Load can be calculated in a variety of ways, including CPU utilization and packets processed per second. Monitoring these parameters on a continual basis can be resource-intensive itself.

Communication cost is another important metric, especially because some companies may not care about performance as much as they care about operating expenditures. Although line delay may be longer, they will send packets over their own lines rather than through the public lines that cost money for usage time

3.6.3 Algorithm Types

Routing algorithms can be classified by type. Key differentiators include these:

- Static versus dynamic
- Single-path versus multipath
- Flat versus hierarchical
- Host-intelligent versus router-intelligent
- Intradomain versus interdomain
- Link-state versus distance vector

3.6.3.1 Static Versus Dynamic

Static routing algorithms are hardly algorithms at all, but are table mappings established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

Because static routing systems cannot react to network changes, they generally are considered unsuitable for today's large, constantly changing networks. Most of the dominant routing algorithms today are dynamic routing algorithms, which adjust to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly.

Dynamic routing algorithms can be supplemented with static routes where appropriate. A router of last resort (a router to which all unroutable packets are sent), for example, can be designated to act as a repository for all unroutable packets, ensuring that all messages are at least handled in some way.

3.6.3.2 Single-Path Versus Multipath

Some sophisticated routing protocols support multiple paths to the same destination. Unlike single-path algorithms, these multipath algorithms permit traffic

multiplexing over multiple lines. The advantages of multipath algorithms are obvious: They can provide substantially better throughput and reliability. This is generally called load sharing.

3.6.3.3 Flat Versus Hierarchical

Some routing algorithms operate in a flat space, while others use routing hierarchies. In a flat routing system, the routers are peers of all others. In a hierarchical routing system, some routers form what amounts to a routing backbone. Packets from nonbackbone routers travel to the backbone routers, where they are sent through the backbone until they reach the general area of the destination. At this point, they travel from the last backbone router through one or more nonbackbone routers to the final destination.

Routing systems often designate logical groups of nodes, called domains, autonomous systems, or areas. In hierarchical systems, some routers in a domain can communicate with routers in other domains, while others can communicate only with routers within their domain. In very large networks, additional hierarchical levels may exist, with routers at the highest hierarchical level forming the routing backbone.

The primary advantage of hierarchical routing is that it mimics the organization of most companies and therefore supports their traffic patterns well. Most network communication occurs within small company groups (domains). Because intradomain routers need to know only about other routers within their domain, their routing algorithms can be simplified, and, depending on the routing algorithm being used, routing update traffic can be reduced accordingly.

3.6.3.4 Host-Intelligent Versus Router-Intelligent

Some routing algorithms assume that the source end node will determine the entire route. This is usually referred to as source routing. In source-routing systems, routers merely act as store-and-forward devices, mindlessly sending the packet to the next stop.

Other algorithms assume that hosts know nothing about routes. In these algorithms, routers determine the path through the internetwork based on their own

calculations. In the first system, the hosts have the routing intelligence. In the latter system, routers have the routing intelligence.

3.6.3.5 Intradomain Versus Interdomain

Some routing algorithms work only within domains; others work within and between domains. The nature of these two algorithm types is different. It stands to reason, therefore, that an optimal intradomain-routing algorithm would not necessarily be an optimal interdomain-routing algorithm.

3.6.3.6 Link-State Versus Distance Vector

Link-state algorithms (also known as shortest path first algorithms) flood routing information to all nodes in the internetwork. Each router, however, sends only the portion of the routing table that describes the state of its own links. In link-state algorithms, each router builds a picture of the entire network in its routing tables. Distance vector algorithms (also known as Bellman-Ford algorithms) call for each router to send all or some portion of its routing table, but only to its neighbors. In essence, link-state algorithms send small updates everywhere, while distance vector algorithms send larger updates only to neighboring routers. Distance vector algorithms know only about their neighbors.

Because they converge more quickly, link-state algorithms are somewhat less prone to routing loops than distance vector algorithms. On the other hand, link-state algorithms require more CPU power and memory than distance vector algorithms. Link-state algorithms, therefore, can be more expensive to implement and support. Link-state protocols are generally more scalable than distance vector protocols.

3.7 Routing Information Protocol (RIP)

3.7.1 Introduction

1. RIP is a distance-vector dynamic routing protocol

– Based on theory developed by Bellman in 1957 that was further refined by Ford and Fulkerson in 1962

– Goal: Minimize the number of hops (distance) to the destination by routing packets via the proper interface (vector)

2. The most widely deployed IGP

3. Easy to implement

– Two messages and one table

4. Cannot be used in large networks (>15 hops)

5. Subject to transient instability

6. The best starting place is a simple example, so...

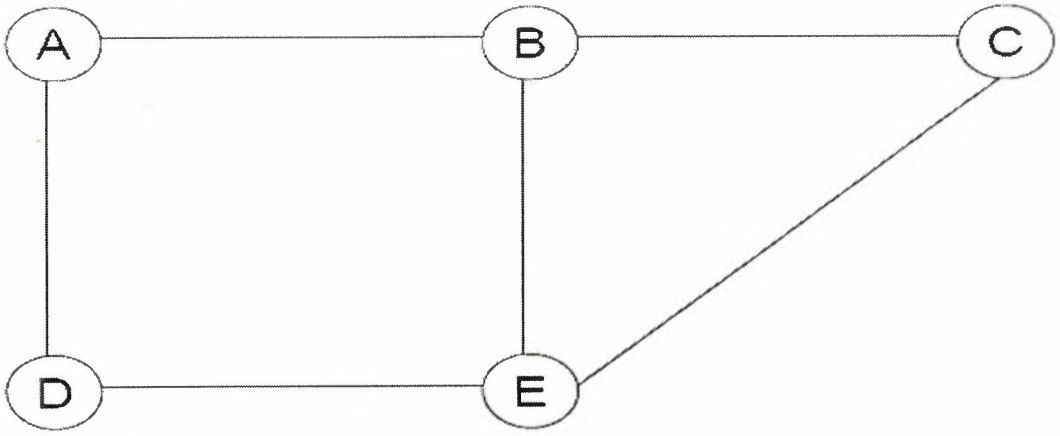


Figure 3.4. Distance Vector Example

7. Toy network of 5 routers and 6 links

– We'll ignore hosts

8. We'll assume that all links are the same distance

9. The link between x and y is called "link xy"

– I.e., AD, BE, AB, BC, CE, DE

3.7.2 Distance Vector Example:

3.7.2.1 Startup

1. All routers boot simultaneously

2. The routers do not know anything about the network

3. They each contain only a single routing table entry to

Them selves

– Assume no static routes except loop back

- For example, Router A:

Dest	Link	Cost
A	local	0

Table 3.1. Distance Vector Example

3.7.2.2 First Broadcast

1. Each router sends its table to its directly-connected neighbors

– I.e., A sends its table to B and D, receives tables from B and D

2. Tables are only updated if the received route information for a given destination indicates a shorter path than the one currently listed

3. A's table now contains:

Dest	Link	Cost
A	local	0
B	AB	1
D	AD	1

Table 3.2 A's

3.7.2.2.1 First Broadcast (Cont.)

1. The rest of the tables:

B

Dest	Link	Cost
B	local	0
A	AB	1
C	BC	1
E	BE	1

D

Dest	Link	Cost
D	local	0
A	AD	1
E	DE	1

C

Dest	Link	Cost
C	local	0
B	BC	1
E	CE	1

E

Dest	Link	Cost
E	local	0
B	BE	1
C	CE	1
D	DE	1

Table 3.3. First Broadcast

3.7.2.3 Second Broadcast

1. Each router sends its table to its neighbors again:

A

Dest	Link	Cost
A	local	0
B	AB	1
C	AB	2
D	AD	1
E	AB	2

B

Dest	Link	Cost
B	local	0
A	AB	1
C	BC	1
D	AB	2
E	BE	1

D

Dest	Link	Cost
D	local	0
A	AD	1
B	AD	2
C	DE	2
E	DE	1

C

Dest	Link	Cost
C	local	0
A	BC	2
B	BC	1
D	CE	2
E	CE	1

E

Dest	Link	Cost
E	local	0
A	BE	2
B	BE	1
D	CE	1
C	DE	1

Table 3.4. Second Broadcast

7.2.4 Stability

1. At this point, routing in the network is stable

– Routing updates will continue, periodically

– No changes made because shorter paths cannot be found

2. When multiple equal-cost paths exist, only the first will be used

– Update algorithm

3. If new cost(X,Y) < old cost(X,Y) then old cost(X,Y) = new cost(X,Y)

4. As long as the network is stable, distance vector protocols work reasonably well

– When an outage occurs, they may take a while to converge, if at all!

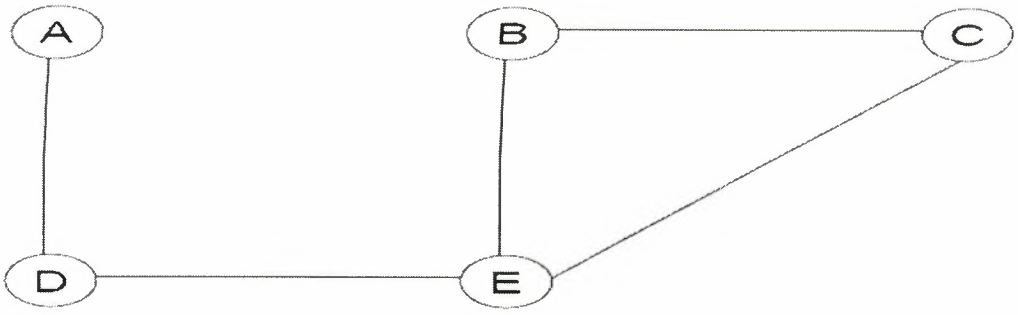


Figure 3.5. Link AB Goes Down

5. A and B will both immediately update their routing tables and send these updated tables to their neighbors

6. The routing will take a couple of steps to converge

3.7.2.5 Updated Routing Tables

A

Dest	Link	Cost
A	local	0
B	AB	INF
C	AB	INF
D	AD	1
E	AB	INF

B

Dest	Link	Cost
B	local	0
A	AB	INF
C	BC	1
D	AB	INF
E	BE	1

D

Dest	Link	Cost
D	local	0
A	AD	1
B	AD	2
C	DE	2
E	DE	1

C

Dest	Link	Cost
C	local	0
A	BC	2
B	BC	1
D	CE	2
E	CE	1

E

Dest	Link	Cost
E	local	0
A	BE	2
B	BE	1
C	CE	1
D	DE	1

27

Table 3.5. Updated Routing Tables

3.7.2.6 A and B Broadcast Their Tables

A

Dest	Link	Cost
A	local	0
B	AB	INF
C	AB	INF
D	AD	1
E	AB	INF

B

Dest	Link	Cost
B	local	0
A	AB	INF
C	BC	1
D	AB	INF
E	BE	1

D

Dest	Link	Cost
D	local	0
A	AD	1
B	AD	INF
C	DE	2
E	DE	1

C

Dest	Link	Cost
C	local	0
A	BC	INF
B	BC	1
D	CE	2
E	CE	1

E

Dest	Link	Cost
E	local	0
A	BE	INF
B	BE	1
C	CE	1
D	DE	1

Table 3.6.A and B Broadcast Their Tables

3.7.2.7 C, D, and E Broadcast Their Tables

A

Dest	Link	Cost
A	local	0
B	AB	INF
C	AD	3
D	AD	1
E	AD	2

B

Dest	Link	Cost
B	local	0
A	AB	INF
C	BC	1
D	BE	2
E	BE	1

D

Dest	Link	Cost
D	local	0
A	AD	1
B	DE	2
C	DE	2
E	DE	1

C

Dest	Link	Cost
C	local	0
A	BC	INF
B	BC	1
D	CE	2
E	CE	1

E

Dest	Link	Cost
E	local	0
A	DE	2
B	BE	1
C	CE	1
D	DE	1

29

Dest	Link	Cost
C	local	0
A	BC	INF
B	BC	1
D	CE	2
E	CE	1

Dest	Link	Cost
E	local	0
A	BE	INF
B	BE	1
C	CE	1
D	DE	1

28

Table 3.7.C, D, and E Broadcast Their Tables

3.7.2.8 Final Broadcast Updates A, B, and C

A

Dest	Link	Cost
A	local	0
B	AD	3
C	AD	3
D	AD	1
E	AD	2

B

Dest	Link	Cost
B	local	0
A	BE	3
C	BC	1
D	BE	2
E	BE	1

D

Dest	Link	Cost
D	local	0
A	AD	1
B	DE	2
C	DE	2
E	DE	1

C

Dest	Link	Cost
C	local	0
A	CE	3
B	BC	1
D	CE	2
E	CE	1

E

Dest	Link	Cost
E	local	0
A	DE	2
B	BE	1
C	CE	1
D	DE	1

30

Table 3.8. Final Broadcast Updates A, B, and C

3.8 Problems With Distance Vector

1. In our example, a single outage occurred

– Required 3 sets of broadcasts to fix

– In the mean time, packets are delayed and/or dropped

2. In a larger network, it could take much, much longer

– Dependent on topology and link cost, weird things can happen

3. Additionally, distance vector is prone to "count to infinity"

– Part of the network becomes isolated

– The isolated routers keep telling each other that they know how to get to the rest of the network

4. But they don't!

– Routing loops are created

3.9 Counting to Infinity

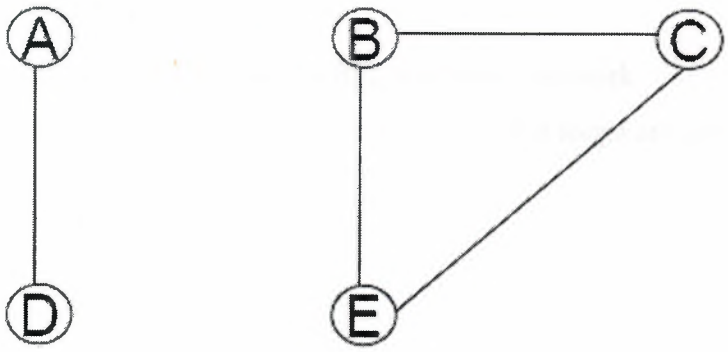


Figure 3.6. Counting to Infinity

1. Continuing our previous example.

– AB went down then the network converged...

2. Link DE goes down

– If D immediately sends an update to A, telling A that all costs to B, C, and E are infinite, then the system converges

– If A sends an update first, D will think it can reach B, C, and E through A!!

- Since all of A's paths are via D, when D sends the next routing update, A's costs will increase by 2

– Etc., etc.

3.10 Trying to Avoid Count to Infinity

1. Set "infinity" to be a finite (and small) number

– RIP uses 16, which is why RIP is limited to networks with 15 or fewer hops

2. Use Split Horizon

– Don't advertise to X a route to Y if you go through X to get to Y

– With "poison reverse"

3. If you go through X to get to Y, advertise to X an infinite-cost route to Y

4. Issue: potentially large routing updates sent because each router also lists all the routes that it *can't* get to

– Works fine for loops of size two

5. Still counts to infinity when loops are larger

6. Use triggered updates

– Whenever a router receives an update, it immediate sends them on to its neighbors: faster convergence

– Still not foolproof - packet loss hurts

– Generates a lot of highly synchronized traffic, may flood network

– Moderately successful in preventing count to infinity when loops are larger than two

3.11 Routing Information Protocol (RIP)

1. RIPv1

– First documented in RFC 1058 in 1988

– Before that, used in very simple form in BSD UNIX

2. Uses UDP port 520 for sending and receiving

– An ephemeral source port can be used for queries

3. Packets consist of control information followed by a list of routes and their associated metrics

4. Route updates normally sent every 30 seconds

– Faster for triggered updates, but with extra delay of 1-5 seconds to avoid synchronization

5. A route is timed out (metric set to infinity) if no updates are heard within 180 seconds

– After 120 more seconds, route is deleted

3.12 Open Shortest Path First) (OSPF)

3.12.1 History

1. IETF Working Group chartered in 1987
2. Version 1 published in 1989 as RFC 1131

– Problems

3. Some routing traffic not deleted after being used
4. Specification unclear on a number of issues
5. Version 2 published in 1991 as RFC 1247

– Proposed standard

6. The IAB designates OSPF as the preferred IGP in 1992
7. Version 2 was updated in 1993 as RFC 1583 and again in 1997 as RFC 2178

– Draft standard

8. Version 2 was elevated to full Standard in 1998

– Note the long, slow process!

3.12.2 Link State Routing

1. OSPF uses link state routing

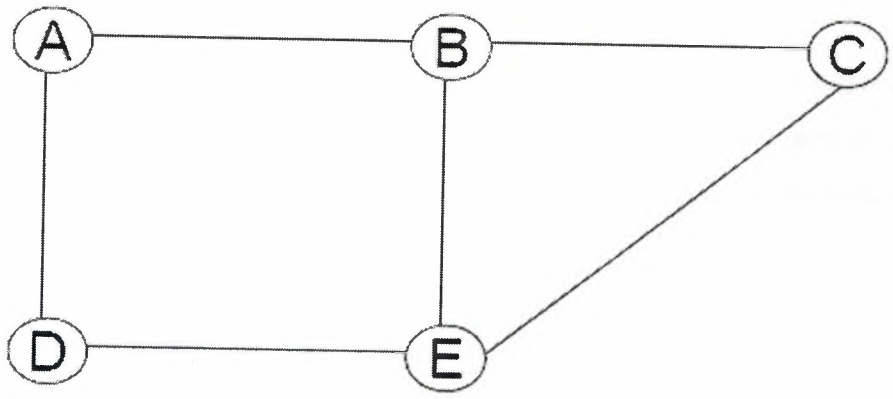
– Significantly different than distance vector routing

2. Each router keeps a complete map of the network, rather than just how to get to each of the other routers

– This map is used to populate routing tables

– All routers should have exactly the same map

3. Routing updates are "flooded" to all nodes
4. Shortest paths between any two points are very easy to compute
5. Fast convergence when the network topology changes



From->To	Link	Cost
A -> B	AB	1
A -> D	AD	1
B -> A	AB	1
B -> C	BC	1
B -> E	BE	1
C -> B	CB	1
C -> E	CE	1
D -> A	AD	1
D -> E	DE	1
E -> B	BE	1
E -> C	CE	1
E -> D	DE	1

Figure 3.7. Link State Example

3.12.3 Shortest Path Calculation

1. Once the map is known to a router, it can compute the shortest path to all other routers

2. Variables:

– S: Source node

– E: All evaluated nodes (shortest path known)

– R: Remaining nodes (shortest path not known)

– O: Sorted list of paths

– P: Shortest cost path in O

– V: The last router in path P

3.13 Dijkstra's Algorithm

1. S = source router, R = all other routers, O = all 1 hop paths from S, in order of cost
2. If O is empty or lowest cost path is infinite, mark all routers in R as unreachable, stop
3. Remove P from O, if V is in E, goto 2, otherwise P is the shortest path from S to V, put V into E with the path and the cost, remove V from R
4. Build new paths by concatenating P with the links that emanate from P, with appropriate metrics added
5. Insert new paths in O, in order
6. Go to 2

3.14 Flooding Algorithm

1. Receive a link state update message
2. If it refers to an entry not yet in the local table
   a) Add the entry to the database
   b) Broadcast the message on all outgoing interfaces except the one the message was received on
3. Else if the metric in the entry is lower than the one in the database
   a) Replace the entry to the database
   b) Broadcast the message on all outgoing interfaces except the one the message was received on
4. Else if the metric is lower in the database than the one in the entry
   a) Broadcast a new message reflecting the metric from the database on the receiving interface

3.15 Why is Link State Better Than Distance-Vector

1. Fast convergence
– Speed is proportional to number of nodes in the network
2. Loopless convergence
– After flooding all routes are stable, no count to infinity
3. Support of multiple metrics
– Throughput, delay, loss, cost, policy, security…
– But all routers should use the same metric, otherwise loops may occur
4. Support for multiple equivalent paths
– In theory, but not so easy in practic

CHAPTER FOUR

NETWORK OPTIMIZATION PROBLEMS

4.1 Introduction

Linear programming problems defined on networks have many special properties. These properties allow the simplex method to be implemented more efficiently, making it possible to solve large problems efficiently. The structure of a basis, as well as the steps in the simplex method, can be interpreted directly in terms of the network, providing further insight into the workings of the simplex method. These relationships between the simplex method and the network form one of the major themes of this chapter. We use them to derive the network simplex method, a refinement of the simplex method specific to network problems.

Network problems arise in many settings. The network might be a physical network, such as a road system or a network of telephone lines. Or the network might only be a modeling tool, perhaps reflecting the time restrictions in scheduling a complicated construction project. A number of these applications are discussed in Section 2.

4.2 What Is Network Optimization

What has happened to our simple network? Do we struggle daily to make our network perform like it still has youth, stability, and endurance? Do users call the complaints: "The network is running slow"; or "I've been waiting ten minutes for my document to print"; or "Our file server just went down." Is this the same network that used to have one file server, 25 workstations, and only one network protocol?

What you have now is an in Internet work. Your network runs TCP/IP, SNA, NetWare, and NetBEUI protocols. Your simple network has grown and now comprises five separate token rings with over 400 workstations and 30 file servers.

The easy days are over. A network that used to be easy to manage now requires a complicated; intricate set of steps involving calculated technical moves to manage this monster you created-this Internet work.

Techniques are available to help you get a handle on your network-to under-stand how it is running and performing, and how it is utilizing the innovative technologies you implemented yesterday. You can also use certain techniques based on calculated measurements to implement changes so that your network will run and perform better. This is known as **network optimization**.

Network optimization is the process of measuring to a defined level a network's workload characteristics and then making modifications to the network's layout, design, and configuration to improve its overall performance.

Most often network optimization involves using a **protocol analyzer** to evaluate the operation of the complete network, including all its hardware and software components. After evaluating the operational state of the network, the next step is to tune all the components. The goal is to make the network components work together so that your Internet work can perform the mission critical operations for which it was intended-at a higher performance level.

Protocol analyzers enable you to optimize and view data on your network to help you understand how that data is performing. Protocol analyzers are mostly independent of protocols, the network operating stem you are running, or the of applications on your network. Protocol analyzers need to be configured, and you need a certain skill set to use them effectively; nonetheless, these tools are extremely valuable.

It is important to understand that a protocol analyzer actually enables you to examine the protocols on a network. The **protocols** are the actual transmission vehicles used to get data from one point to another within the Internet work, regardless of the entity doing the transmitting on the network. The only way to actually view and troubleshoot any problems in the protocols themselves is with a protocol analyzer.

Some tools available today enable you to view just the statistics from the protocols and how they affect the network. These tools could be appropriately labeled **monitoring tools**, but they are not true protocol analyzers. Protocol analyzer is more in depth than a monitoring tool, and enables you to view the internals of the protocol and its operations.

4.3 Network Modification Analysis

After any major network modification, a critical final step is to retest the network with a protocol analyzer to get a benchmark of the network's performance level. Only

one change should be made to a network at a time, followed by retesting the network with a protocol analyzer to see the effect on performance.

Testing the network before and after the change enables you to evaluate and document the performance effect of the network modification. For example, if a protocol analyzer captured a particular workstation to file server read at one minute and there now has been a 16-megabytes upgrade in file server memory~, the network read should be remeasured; this is called post analysis. After the analyzer test is complete, the results of the post analysis show a workstation4~file-server read of 20 second this is a 40 second increase in performance for the particular task.

4.4 Measuring Network Application Efficiency

Optimizing application efficiency is a goal to be established when a particular application is having problems on the network. The usual symptom is a user or group of users complaining about a particular application's performance. There are fairly easy ways to benchmark the application's performance with respect to its standard configuration as it is documented, and how it is actually operating on a particular network.

Some protocol analyzers and network monitoring tools can be used to trap certain application access events. After a particular application event is captured, you can determine if it is performing to its optimum level.

For all applications, some application processing occurs in the workstation, and some occurs in the file server. Through examination with a protocol analyzer of a complete traffic event of an application access, an analyst can watch the request to the file server for the application, the access from the file server, and the return to the particular workstation. The specific interprocess times at the workstation and at the file server can be stamped and benchmarked for their actual interprocess time.

File search processes also occur for the application, and certain hand-off- techniques are available for reading and writing files across the network involved. A protocol analyzer helps to pinpoint whether the application is working the way it was originally intended by the designer or manufacturer. The efficiency of the application can only be measured against its original specifications from the designer or manufacturer; if a particular application is performing at its optimum level, that specifically needs to be verified.

Additionally, some applications may not work well on certain internet work configurations. The network operation staff may have a perception of how an application will work, but the analyst must capture some events of the application's actual operation on the network to verify its overall integrity. It is possible that a certain application can contribute to bandwidth peaks on a network.

At times, applications may perform general file searches inefficiently. These are easily picked up by examining the network for multiple file searches during searches for an application. Application tuning approaches can be used to examine ways to reconfigure an application so that it performs at its peak.

4.5 Topological Optimization of Network using Integer Programming

Conventional routing such as OSPF is the most common routing protocol inside an Autonomous System (AS), such as an Internet Service Provider (ISP) network. Each link is assigned a cost, which is often set proportional to the inverse link capacity. Traffic is routed via the shortest path between the source and the destination, or "load balanced" among equal cost shortest paths where they exist. Therefore, the only way that the network operator can change the routing is by changing the link weights. The usual way that network operators try to reduce network congestion is by increasing the link cost of the congested link(s). However doing this may lead to the shifting of a large amount of traffic from that particular link to other less congested ones, overloading the other links, often in an unexpected way. There is a need for a tool for modeling OSPF routing and for determining the link weights before implementing changes to a real network [5], [45].

Several approaches have been presented [45], [8], [7], [6], [5], [46]. The approach that will be implemented in this thesis uses a integer programming module based on link costs and link reliability. The objective is to minimize the usage of links and at the same time maintain a highly reliable network.

In the design of communication networks, one of the fundamental considerations is the reliability and the availability of the communication paths between all terminals. Together, these form the network system reliability. The other important aspect is the layout of the paths to minimize cost while meeting the reliability demands.

An important part of network design is to find the best way to layout the components (nodes and arcs) to minimize cost while meeting performance requirements

such as transmission delay, throughput or reliability. This design stage is called 'Network Topological Optimization'. In a topological network design problem, the main concern is to design networks, which will operate effectively and without interruption in the presence of component failure. Reliability is concerned with the ability of a network to carry out desired network operations.

The mathematical approach used in this thesis is based on integer programming where a binary coding structure for representing candidate solutions is used. If we have a network that has five nodes and 10 possible links, they can be represented as:

[1	1	0	1	0	1	0	1	0	1]
[x_{12}	x_{13}	x_{14}	x_{15}	x_{23}	x_{24}	x_{25}	x_{34}	x_{35}	x_{45}]

Where x_{ij} represents a link connecting two nodes I and j. if x_{ij} is equal to 1, there is a connection between these nodes. If x_{ij} is equal to 0, then there is no connection.

Using this approach, the following characteristics will be used:

1. Arc probabilities between *[0,1]* which determine the existence of an arc between nodes, are selected.
2. The system reliability value of each connected network is estimated using a random generation function on a scale of 10. {1 is 10% and 10 is 100%}.
3. The cost values for each connected link is simulated using network metrics generation functions.

The aim is to determine the best combination of links such that, the network will meet the required reliability measure.

The mathematical module is based on the minimum cost flow problem that can be stated as a integer program as follows:

Minimize cx

Subject to: Nx = b, Where x = {0,1}.

Here, N is an m x n matrix called the node-arc incidence matrix and the integer equation system Nx = b is the mass balance equations, representing the inflow and outflow of each node in the network.

Network planning is concerned with the design of sufficiently reliable networks at reasonable cost, to deliver high capacity and speed [8].

A network is modeled by a probabilistic undirected graph G=(N, L, p), in which N represents the set of nodes, L is a given set of possible links, and p is reliability of each link. It is assumed one bi-directional link between each pair of nodes.

The optimization problem may be stated as:

$$Minimize\ Z = \sum_{i=1}^{I} \sum_{j=1}^{J} C_{ij} X_{ij}$$

$$Subject\ to:\ R(x) \geq R_0$$

Where x_{ij} is a decision variable (0,1), c_{ij} is the cost of the link (i,j), $R(x)$ is the network reliability and R_0 is the minimum reliability requirements.

Its possible that sometimes the link reliability is so low that additional constrains are required, if the network link reliability is below 30% or 3 on a scale of 10. Additional constraints may be needed to decrease or limit that link.

To solve this problem, the following assumptions are made:

- The N nodes are perfectly reliable. A problem with a node may be simulated by the failure of its incident links.
- The cost c_{ij} and the reliability R_{ij} of each link (i,j), are already known or to be known.
- The links have two states: either operational (x_{ij}= 1) or failed (x_{ij}= 0).
- The links failure are independent.
- No repair is considered.
- Two connectivity is required.

Below is the network diagram to be solved:

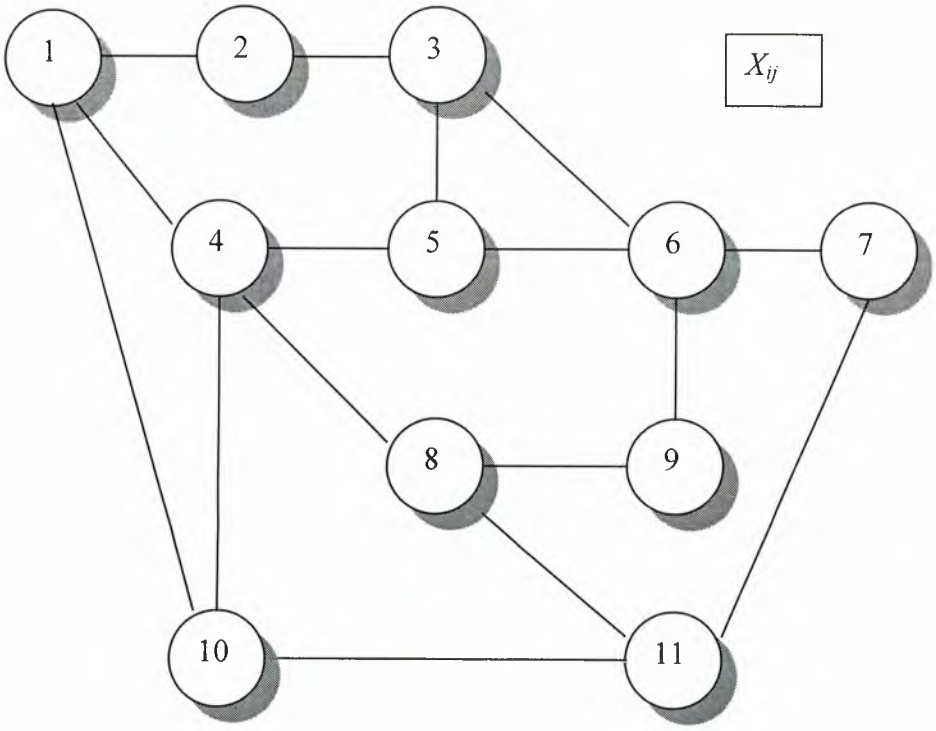


Figure 4.1

While in conventional routing there is no relation to network reliability, or link bandwidth. There is only a cost constraint and the routing protocol will route packets based on the lowest cost. Cost in networks is a linear function based on the load [5], capacity [6], or a combination of the two [6].

In conventional routing a path is taken to be singular route from start to finish. And when two paths have the exact shortest value from start node to end node, one of those paths maybe chosen or the load is distributed across the two using a round robin fashion, opening a door for packet integrity and redundancy loss [23], [44].

Below, is a demonstration of conventional routing path selection, and optimized routing path selection. In conventional routing only one route is taken from node 1 to node 8.While in optimized routing more than one path is taken depending on links reliability.

This is how conventional routing path selection process from node 1 to ode 8 are made:

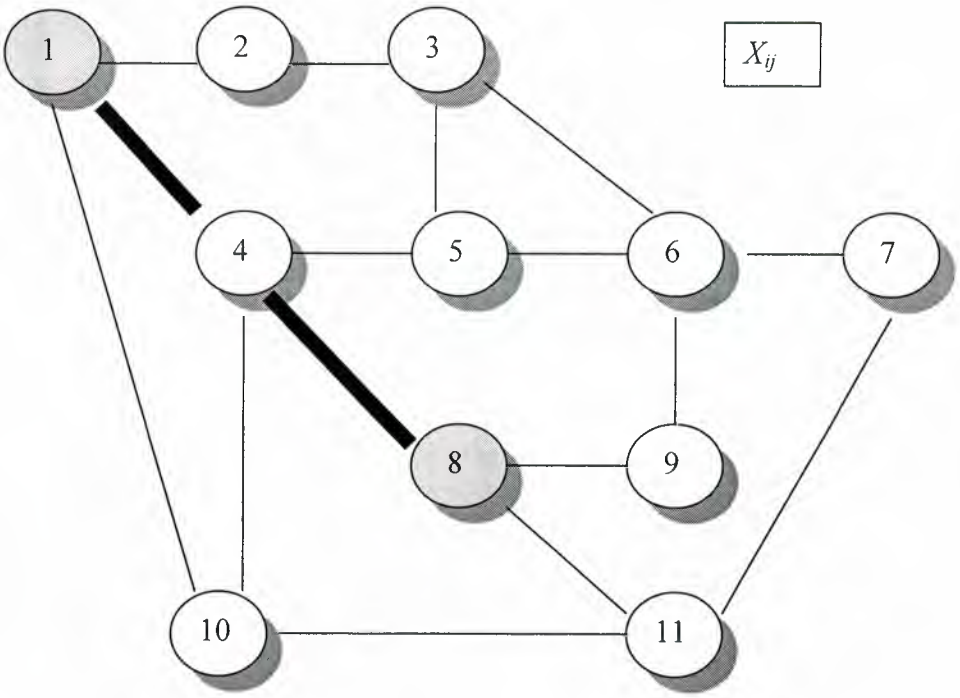


Figure 4.2

This is how optimized routing is selecting paths based on link reliability assuming that the shortest path 1-4-8 is under very low reliability:

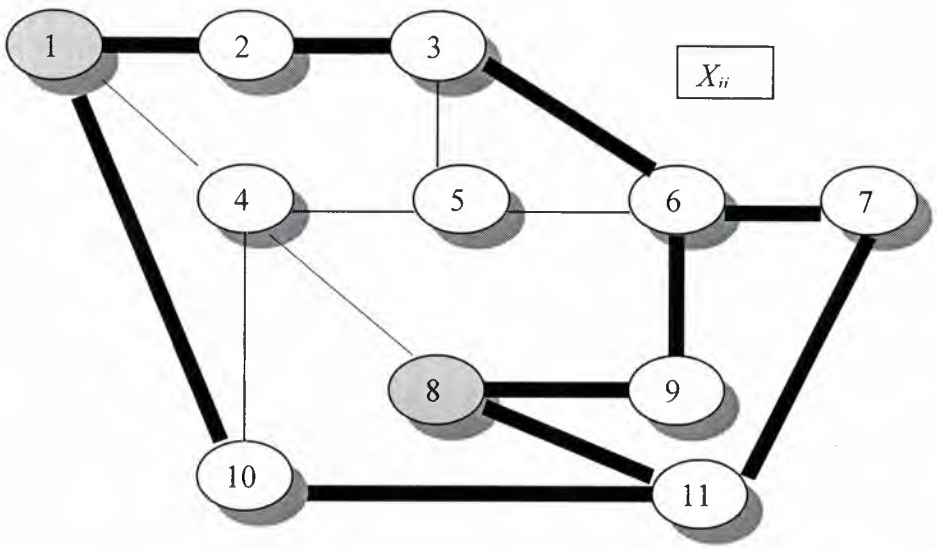


Figure 4.3

First, we labeled all the possible paths from all nodes using the x_{ij} labeling convention.

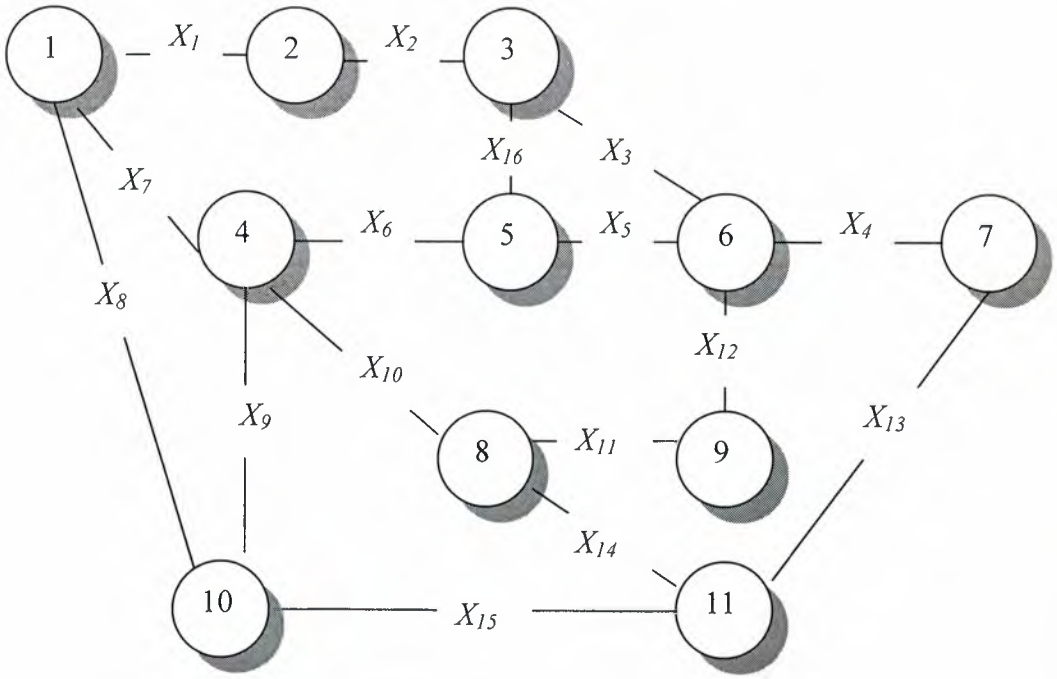


Figure 4.4

Second, we defined all the variables to feed them later to the optimizer. All the variables are shown in the table below.

Table4.1

C_{ij}	Cost Function.
λij	Load on the network or effective bandwidth.
Rij	Reliability of the network links.
X_{ij}	Unknown path combinations.

The cost is achieved using the linear function Cost = load in packets / 5

Table4.2

Costs	Run1	Run2	Run3	Run4	Run5
C_1	4	3	3	1	4
C_2	3	5	1	5	0
C_3	3	5	1	0	5
C_4	1	1	3	2	2
C_5	2	3	0	2	3
C_6	4	5	2	2	4
C_7	2	1	5	1	0
C_8	4	3	1	2	3
C_9	4	1	4	1	2
C_{10}	4	5	2	3	1
C_{11}	1	3	1	3	3
C_{12}	2	0	5	1	3
C_{13}	4	3	3	5	1
C_{14}	4	0	3	3	1
C_{15}	2	0	2	3	4
C_{16}	5	4	0	2	4
Average	3.06	2.62	2.25	2.25	2.5

The reliability is generated based on a probability of 1.0 (100%) to 0 (0%). The numbers here are random numbers.

Table4.3

Reliability	Run1	Run2	Run3	Run4	Run5
R_1	0.9	0.3	0.6	0.1	0.6
R_2	0.1	0	0.7	0.8	1
R_3	1.0	0.3	0.9	0.5	0.9
R_4	0.4	0.4	0.8	0.8	0.2
R_5	0.5	0.3	0	0.6	0.7
R_6	0.8	0.9	0.5	0.8	1
R_7	0.1	1.0	0.9	0	0.2
R_8	0.6	0.4	0.4	0.2	0.5
R_9	0.5	0.3	0.7	0.1	0.1
R_{10}	0.3	0.2	0.5	0.1	1
R_{11}	0.6	0.2	0.5	0.3	0.7
R_{12}	0.6	0.6	0.5	0.1	0
R_{13}	0.3	0.4	0.4	0	0.6
R_{14}	0.3	0.4	0.4	0.5	0.1
R_{15}	0.8	0.7	0.3	0.7	0.1
R_{16}	0.8	0.3	0.1	0.5	0.8
Average	0.537	0.418	0.512	0.381	0.531

Table4.4

Run	Conventional Routing	Optimized Routing

Table4.5

	Overall Reliability
Conventional	0.50
Optimized	0.76

Using conventional routing, the shortest path from node1 to node11, based on the shortest cost is determined to be x_8 -x_{15}. Having with an average reliability of 0.6 + 0.8 = 1.4 / 2 = 0.7 or 70%.

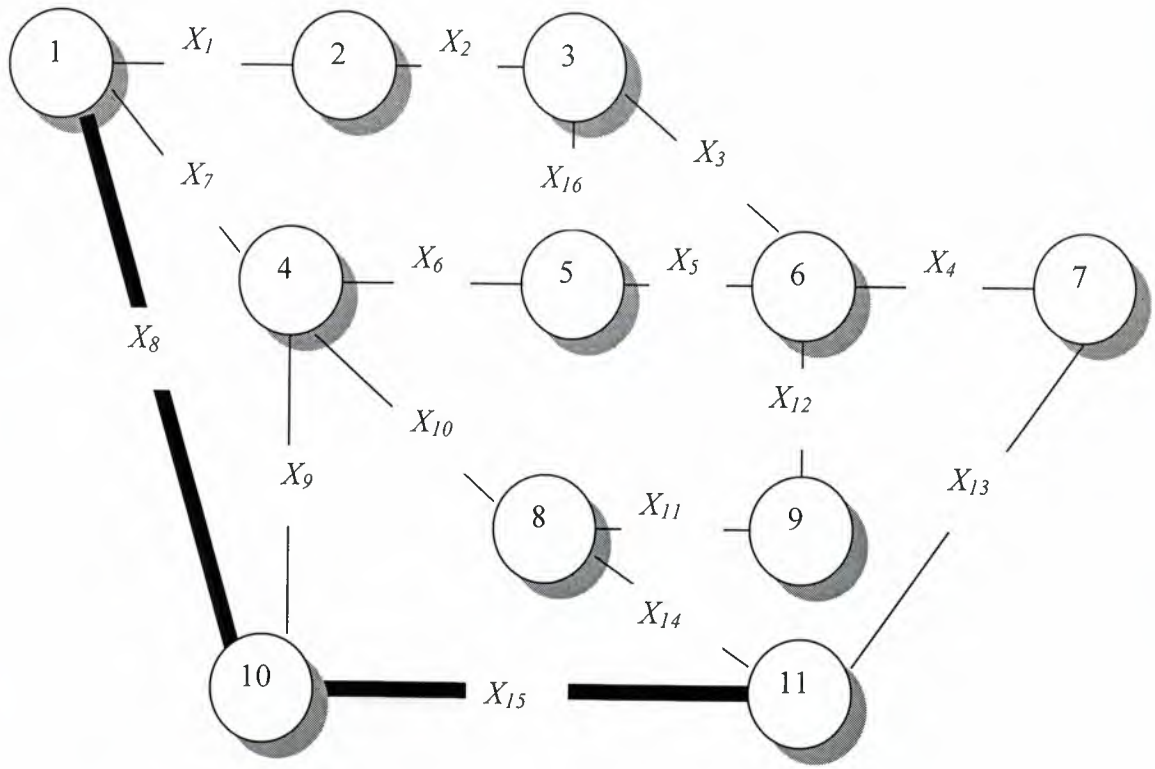


Figure 4.5

	Avr. Cost	Reliability	Avr. Cost	Reliability
1	3.06	0.7	3.06	0.7
2	2.62	0.5	2.62	0.8
3	2.25	0.4	2.25	0.7
4	2.25	0.3	2.25	0.8
5	2.50	0.6	2.50	0.8

Table 4.6

Run1:

In this case, the reliability was quite high for link x_8 and link x_{15}. However, in some cases the links reliability can be very low, resulting in a degrading performance for the whole network.

Paths	Cost	Reliab.
X_1	4	0.9
X_2	3	0.1
X_3	3	1.0
X_4	1	0.4
X_5	2	0.5
X_6	4	0.8
X_7	2	0.1
X_8	4	0.6
X_9	4	0.5
X_{10}	4	0.3
X_{11}	1	0.6
X_{12}	2	0.6
X_{13}	4	0.3
X_{14}	4	0.3
X_{15}	2	0.8
X_{16}	5	0.8
Average	3.06	0.537

Table 4.7

Here, the candidate links, using optimized routing are shown in the figure below, in this particular case, optimized routing cannot exceed 70% due to the inclusion of x_8 and x_{15}.

If the shortest path from node1 to node11, is to be $x_7 - x_{10} - x_{14}$ then based on optimized routing solution that path is not to be taken, because x_{10} and x_{14} are out of the candidate paths. They are under very low reliability. The paths that are not considered as candidate paths are x_2, x_{10}, x_{13} and x_{14} as shown below.

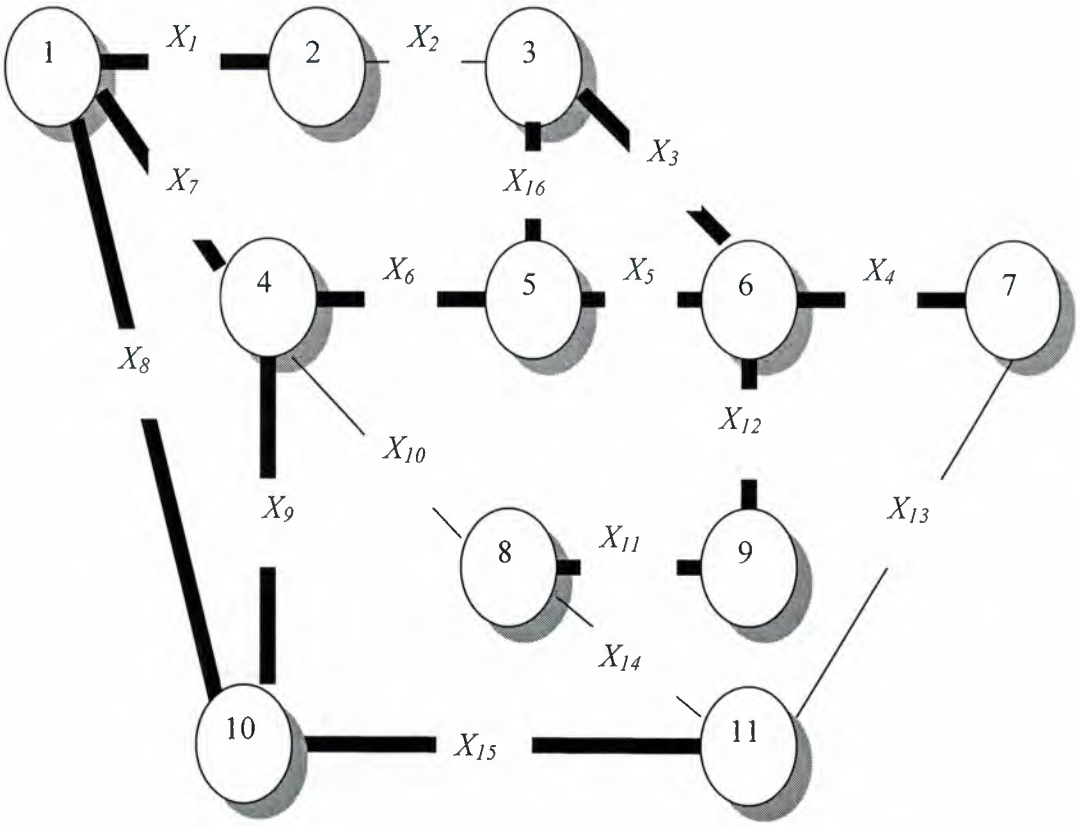


Figure 4.6

4.3 Topological Optimization of Network Using Integer Programming

After careful research and analysis, the best way to solve optimization problems is believed to be using optimization packages. Other solvers like MATLAB™, MATHMATICA™, and MAPLE™ were incapable of solving such problems, those packages have general purpose support for most mathematical problems. And was not efficient when solving the integer programming module discussed in this thesis [31],[32],[33].

A number of optimization packages is available in the market today, which are categorized into two main groups:

1. Commercial Packages: Those are very efficient and capable of handling a huge amount of variables(50,000 variable and more).[29],[21]. They have the

disadvantage of being expensive to license. Examples include, Lindo[29] and lpsolve[21],[10]

2. Educational Packages: Those packages come with optimization books, they can handle small to medium sized optimization problems. And there is no licensing fee for using them, they come with the book with no additional fee. Examples include Quick Quant Plus by Dr. Alpin[4], and QSB+[3] Those packages run under the Dos prompt. The newer version of QSB+ is published in a separate book but from the same author [2] the package is called WinQSB and will be used in this thesis to solve the mathematical module.

We implemented the mathematical module into WinQSB and fed the network metrics achieved from the network generator, we solved the module five times, in each time optimized routing equals or is slightly less than the required network reliability requirement.

Conventional routing has no means to adjust it self based on the current network reliability requirements. The most useful network protocols can provide administrators with network metrics that they have to manually alter the network link costs to maintain network stability and reliability [34].

Below is a view of the WinQSB solver, this is where the module is written into the solver, up to 16 limiting constraints can be added into this solver. It will then work its way, using branch and bound approach discussed in chapter 1 and it finally display the results based on the reliability requirements. Sometimes the solver converge to the solution on other times it can only be as close as possible.

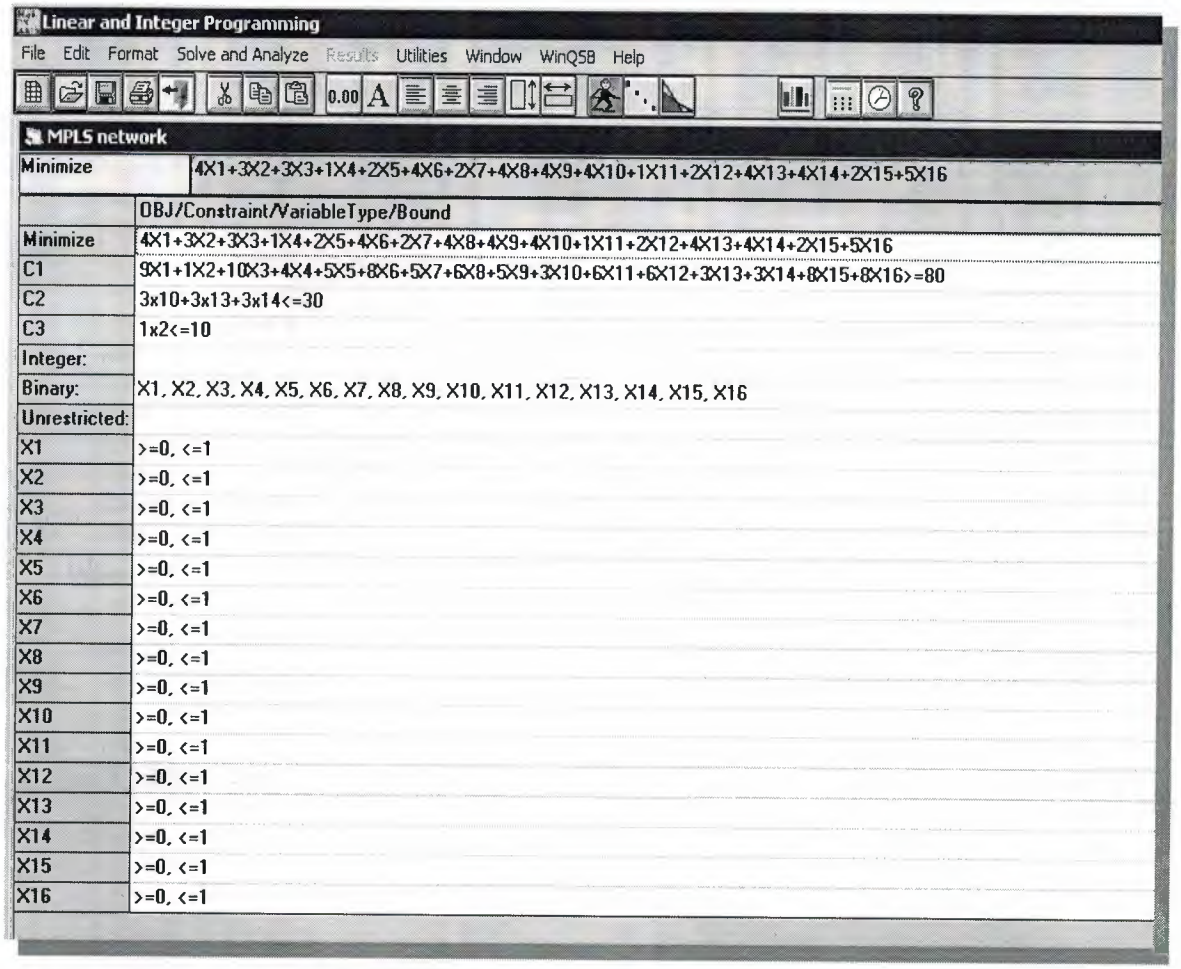


Figure 4.7

In figure 4.7, the output after running WinQSB. The solution value 1 means tat this path will be used or its operational. If the solution value is zero it means that the path is not used or not operational. In this module the solution of 80% reliability is achieved in this network. We have only 4 paths out of 16 that will not be operational. The rest of the paths are operational or candidates to route data from any two nodes in the network.

	Decision Variable	Solution Value	Unit Cost or Profit c(j)	Total Contribution	Reduced Cost	Basis Status	Allowable Min. c(j)	Allowable Max. c(j)
1	X1	1.0000	4.0000	4.0000	0	basic	-M	7.2000
2	X2	0	3.0000	0	2.2000	at bound	0.8000	M
3	X3	1.0000	3.0000	3.0000	0	basic	-M	8.0000
4	X4	1.0000	1.0000	1.0000	0	basic	-M	3.2000
5	X5	1.0000	2.0000	2.0000	0	basic	-M	4.0000
6	X6	1.0000	4.0000	4.0000	0	basic	-M	6.4000
7	X7	1.0000	2.0000	2.0000	0	basic	-M	4.0000
8	X8	1.0000	4.0000	4.0000	0	basic	-M	4.8000
9	X9	1.0000	4.0000	4.0000	0	basic	3.3333	6.6667
10	X10	0	4.0000	0	1.6000	at bound	2.4000	M
11	X11	1.0000	1.0000	1.0000	0	basic	-M	4.8000
12	X12	1.0000	2.0000	2.0000	0	basic	-M	4.8000
13	X13	0	4.0000	0	1.6000	at bound	2.4000	M
14	X14	0	4.0000	0	1.6000	at bound	2.4000	M
15	X15	1.0000	2.0000	2.0000	0	basic	-M	6.4000
16	X16	1.0000	5.0000	5.0000	0	basic	-M	6.4000
	Objective	Function	(Min.) =	34.0000				
	Constraint	Left Hand Side	Direction	Right Hand Side	Slack or Surplus	Shadow Price	Allowable Min. RHS	Allowable Max. RHS
1	C1	80.0000	>=	80.0000	0	0.8000	75.0000	80.0000
2	C2	0	<=	30.0000	30.0000	0	0	M
3	C3	0	<=	10.0000	10.0000	0	0	M

Figure 4.8

CONCLUSION

From my project about Network routing and optimization; I conclude that as we know that this is the computer era. So there is need for advancement in any field of life speacilly in computer fields. There are many networks connected together due to heavy traffic.

Also sometimes we need information very fast as this is the era of multimedia and if we have to send a multimedia file over a network it will take too much time so we have new and new technologies of networking to compensate with the needs of the day.

We use routing to at least networks with packets that forward data. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols. Very little filtering of data is done through routers. Routers are specialized computers that send messages and those of every other Internet user speeding to their destinations along thousands of pathways

In computer networks, each router has a table that shows where to send each incoming packet. This table is created when the router comes online, and used for all packets. A system that updates this routing table periodically is called a dynamic system, whereas a system that does not change the routing table is called a static system.

Routing algorithms are the algorithms that decide the route a packet is going to follow namely its source to its destination.

In computer network routing link state better than distance-vector, that is link state of routing is Fast convergence, Loop less convergence, Supports of multiple metrics, and supports for multiple equivalent paths.

Network optimization is the process of measuring to a defined level a network's workload characteristics and then making modifications to the network's layout, design, and configuration to improve its overall performance.

Techniques are available to help us to get a handle on our network--to understand how it is running and performing, and how it is utilizing the innovative technologies implemented. We can also use certain techniques based on calculated measurements to implement changes so that your network will run and perform better. This is known as *network optimization.*

REFERENCES

Books

[1] F. Baker, "Requirements for IP Version 4 Routers," Internet RFC 1812, Jun. 1995

[2] C. Hedrick, "Routing Information Protocol," Internet RFC 1058, Jun. 1988.

[3] C. Huitema, *Routing in the Internet*, 2nd Edition, Prentice Hall, 2000.

[4] G. Malkin, "RIP Version 2," Internet RFC 2453, Nov. 1998.

[5] P. Miller, *TCP/IP* Explained, Digital Press, 1997.

[6] J. Moy, "OSPF Version 2," Internet RFC 2328, Apr. 1998.

[7] J. Moy, *OSPF: Anatomy of a Routing Protocol*, Addison-Wesley, 1998.

[8] C. Partridge, "Designing and Building Gigabit and Terabit Internet Routers," *SIGCOMM '98*
Tutorial, Sep. 1998.

[9] Y. Rekhter and T. Li, "A Border Gateway Protocol (BGP-4)," Internet RFC 1771, Mar. 1995.

[10] Y. Rekhter and P. Gross, "Application of the Border Gateway Protocol in the Internet," Internet RFC 1772, Mar. 1995.

[11] R. Stevens, *TCP/IP Illustrated, Vol. 1*, Addison-Wesley, 1994.

[12] J. W. Stewart, *BGP4: Inter-Domain Routing in the Internet*, Addison-Wesley, 1999.

[13] D. P. Bertsekas and R. Gallager. *Data Networks*. Prentice-Hall, 1992. Second Edition.

Web Sites

www.comptechdoc.org
www.cdn.com
www.fcit.usf.edu
www.cb4arab.com