DESIGN AND IMPLEMENTATION OF DOMAIN TYPE LOCAL AREA NETWORK

BY

MOSUDI ISIAKA O. E.

REG NO 97/6073EE

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

SCHOOL OF ENGINEERING AND ENGIEERING TECHNOLOGY

FEDERAL UNIVERSITY OF TECHOLOGY MINNA, NIGERIA

AUGUST 2003

DESIGN AND IMPLEMENTATION OF DOMAIN TYPE LOCAL AREA NETWORK

BY

MOSUDI ISIAKA O. E.

REG NO 97/6073EE

A THEISS REPORT SUBMITTED IN PARTIAL FUFILLMENT OF THE REQUIRMENT OF THE AWARD OF BACHELOR OF ENGINEERING (B.ENG) DEGREE IN THE DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING SCHOOL OF ENGINEERING AND ENGINEERING TECHNOLOGY FEDERAL UNIVERSITY MINNA NIGER, STATE.

AUGUST 2003.

CERTIFICATION

I certify that this project title "THE DESIGN AND IMPLEMENTATION OF DOMAIN TYPE LOCAL AREA NETWORK" was designed and constructed by MOSUDI ISIAKA O. E. under the supervision of ENGR. M. D. ABDULLAHI. And submitted to electrical and Computer Engineering Department, Federal University of Technology Minna. In partial fulfillment for the requirement for the award of Bachelor of Engineering (B.Eng), in Electrical and Computer Engineering.

ENGR. M. D. ABDULLAHI

.....

PROJECT SUPERVISOR

28/10/03

DATE AND SIGN

ENGR. M. N. Nwohu

.....

HEAD OF DEPARTMENT

.....

DATE AND SIGN

.....

EXTERNAL EXAMINER

.....

DATE AND SIGN

DECLARATION

I, Mosudi Isiaka O.E, hereby declared that this project work is an original work of mine and that it is a record of my research work, which to the best of my knowledge barring coincidence has never been presented elsewhere.

Mosudi Isiaka O. E.

97/6073EE

..... 16/10/03

DATE AND SIGN

ACKNOWLEGDMENT

I do acknowledge and appreciate the support and encouragement from my mother, Mrs. R. Mosudi, Mr. Babatunde Lateef, Coker Efundayo, Abolade Suleiman, Adisa O. Abdul-Jalil, Yekeen Yinusa, Ibrahim Abdul-Majeed, Ajayi Adewale, Ifebule Adekunle and Adesokan Bashir. The inspirations and effort of my father, Mr. Mosudi Ibrahim and the project supervisor, Engr. M. D. Abdulahi is second to none. I acknowledge Mr. Oboyega Ogunrayewa of Baford Technologies and Datacomm Express ltd. both in Lagos for providing the study materials and Mrs. Agbachi for the privilege to use equipments. I also appreciate the effort of other friends who were of assistance in one way or another towards the commencement, progress and completion of this project.

Also to all the lecturers and the entire members and staff of Electrical and Computer Engineering department, I wish you all God's favour all the days of your lives

DEDICATION

This project is dedicated to my son, Mosudi Sheriff and my mother, Mrs. R. Mosudi. To God Almighty, the invincible, is all the glory.

ABSTRACT

This project report is the design and implementation of domain type local area network. This aim is achieved through implementation of star topology network base on IEEE 802.3 of specification, i.e. Ethernet specification, in a domain type local area networking whereby the server coordinates every process over the network and all task are synchronized removing disperse in property and behaviour of all networked systems. The resulting network reduces the task of managing the network, upfront, running and maintenance costs, all at the expense of dedicated system planning, design and implementation. The project highlights the importance, concept, and configuration, and practicalizes dynamic host configuration protocol (DHCP), domain naming system (DNS), and Internet information services (IIS) among other things.

TABLE OF CONTENTS

CHAPTER ONE

1.1 ILITERATURE REVIEW

Networking involves techniques, physical connections, and computer programs used to link two or more computers. Network users are able to share files, printers, and other resources; send electronic messages; and run programs on other computers.
A network has three layers of components: application software, network software, and network hardware. Application software consists of computer programs that interface with network users and permit the sharing of information, such as files, graphics, and video, and resources, such as printers and disks. One type of application software is called client-server. Client computers send requests for information or requests to use resources to other computers, called servers that control data and applications. Another type of application software is called peer-to-peer. In a peer-to-peer network, computers send messages and requests directly to one another without a server intermediary.

Network software consists of computer programs that establish protocols, or rules, for computers to talk to one another. Sending and receiving formatted instructions of data called packets carry out these protocols. Protocols make logical connections between network applications, direct the movement of packets through the physical network, and minimize the possibility of collisions between packets sent at the same time.
Network hardware is made up of the physical components that connect computers. Two important components are the transmission media that carry the computer's signals, typically on wires, wireless or fiber-optic cables, and the network adapter, which accesses the physical media that link computers, receives packets from network software, and transmits instructions and requests to other computers. Transmitted information is in the

form of binary digits, or bits (1s and 0s), which the computer's electronic circuitry can process.

1.2 INTRODUCTION

1.2.1 NETWORK CONNECTIONS

A network has two types of connections: physical connections that let computers directly transmit and receive signals and logical, or virtual, connections that allow computer applications, such as word processors, to exchange information. Physical connections are defined by the medium used to carry the signal, the geometric arrangement of the computers (topology), and the method used to share information. Logical connections are created by network protocols and allow data sharing between applications on different types of computers, such as an Apple Macintosh and an International Business Machines Corporation (IBM) personal computer (PC), in a network. Some logical connections use client-server application software and are primarily for file and printer sharing. The Transmission Control Protocol/Internet Protocol (TCP/IP) suite, originally developed by the United States Department of Defense, is the set of logical connections used by the Internet, the worldwide consortium of computer networks. TCP/IP, based on peer-to-peer application software, creates a connection between any two computers.

1.2.2 Media

The medium used to transmit information limits the speed of the network, the effective distance between computers, and the network topology. Copper wires and coaxial cable provide transmission speeds of a few thousand bits per second for long distances and about 100 million bits per second (Mbps) for short distances. Optical fibers carry 100 million to 1 billion bits of information per second over long distances.

1.2.3 Topology

Common topologies used to arrange computers in a network are point-to-point, bus, star, and ring. Point-to-point topology is the simplest, consisting of two connected computers. The bus topology is composed of a single link connected to many computers. All computers on this common connection receive all signals transmitted by any attached computer. The star topology connects many computers to a common hub computer. This hub can be passive, repeating any input to all computers similar to the bus topology, or it can be active, selectively switching inputs to specific destination computers. The ring topology uses multiple links to form a circle of computers

1.4.4 Sharing Information

When computers share physical connections to transmit information packets, a set of Media Access Control (MAC) protocols are used to allow information to flow smoothly through the network. An efficient MAC protocol ensures that the transmission medium is not idle if computers have information to transmit. It also prevents collisions due to simultaneous transmission that would waste media capacity. MAC protocols also allow different computers fair access to the medium.

1.2.5 NETWORK OPERATION AND MANAGEMENT

Network management and system administration are critical for a complex system of interconnected computers and resources to remain operating. A network manager is the person or team of people responsible for configuring the network so that it runs efficiently. For example, the network manager might need to connect computers that communicate frequently to reduce interference with other computers. The system

administrator is the person or team of people responsible for configuring the computer and its software to use the network. For example, the system administrator may install network software and configure a server's file system so client computers can access shared files.

Networks are subject to hacking, or illegal access, so shared files and resources must be protected. A network intruder could eavesdrop on packets being sent across a network or send fictitious messages. For sensitive information, data encryption (scrambling data using mathematical equations) renders captured packets unreadable to an intruder. Most servers also use authentication schemes to ensure that a request to read or write files or to use resources is from a legitimate client and not from an intruder

1.2.6 Local Area Network

Local Area Network is a collection of interconnected computers that can share data, applications, and resources, such as printers. Computers in a LAN are separated by distances of up to a few kilometers and are typically used in offices or across university campuses. A LAN enables the fast and effective transfer of information within a group of users and reduces operational costs.

Other connected computer resources are wide area networks (WANs) and private branch exchanges (PBXs). WANs are similar to LANs but they connect computers separated by longer distances, typically across the country or internationally, and they use specialized and expensive hardware and leased communications services. PBXs provide continuous computer connections for the transfer of specialized data such as telephone

transmissions, but they are not ideally suited to send and receive the short bursts of data used by most computer applications.

1.2.7 ADVANCES

Progress in how network routes information will allow data to move directly from a source computer to a destination computer without interference from other computers. This will enhance the transmission of continuous streams of data, such as audio and video. The wide use of notebook and other portable computers has produced advances in wireless networks. Wireless networks use infrared or radio frequency transmissions to connect mobile computers to networks. Infrared wireless LANs connect computers within a room, while wireless radio frequency LANs can connect computers separated by walls.

New LAN technologies will be faster and will support multimedia applications. Asynchronous Transfer Mode (ATM) and Ethernet LANs that are 10 to 15 times faster than standard LANs are now available. To take advantage of faster LANs, computers must become faster; especially the connection called the bus that links the computer's memory to the network. In addition, computer software must be developed that is able to efficiently transfer large amounts of data from networks to computer applications.

1.2.8 FUTURE TECHNOLOGIES AND TRENDS

The wide use of notebook and other portable computers drives advances in wireless networks. Wireless networks use either infrared or radio frequency transmissions to link these mobile computers to networks. Infrared wireless LANs work only within a

room, while wireless LANs based on radio-frequency transmissions can penetrate most walls. Wireless LANS have capacities from less than 1 Mbps to 8 Mbps and operate at distances up to a few hundred meters. Wireless communication for WANS use cellular telephone networks, satellite transmissions, or dedicated equipment to provide regional or global coverage, but they have transmission rates of only 2000 to 19,000 bits per second. New networks must also meet the growing demand for faster transmission speeds, especially for sound and video applications.

One recently developed network, called an Asynchronous Transfer Mode (ATM) network, has speeds of up to 625 Mbps and can be used by either LANS or WANS. In February 1996 Fujitsu Ltd., Nippon Telephone and Telegraph Corporation, and a team of researchers from AT&T succeeded in transmitting information through an optical fiber at a rate of 1 trillion bits per second—the equivalent of transmitting 300 years of newspapers in a single second. This was accomplished by simultaneously sending different wavelengths of light, each carrying separate information, through the optical fiber. If it can be integrated into a network, this new technology will make it easy, inexpensive, and incredibly fast to send information, such as video and memory-sensitive three-dimensional images. Local area networks (LANs), which connect computers separated by short distances, such as in an office or a university campus, commonly use bus, star, or ring topologies. Wide area networks (WANs), which connect distant equipment across the country or internationally, often use special leased telephone lines as point-to-point links.

1.3 MOTIVATION

Over the years, network users and engineers alike have paid for reliability and availability as appointments might not be met, and time as a resources are expended to cater for downtime due to ineffective means applied in solving problems arising from the need to setup a network. The most prominent is the Internet cyber cafes, sometimes running four or less out of say ten systems available for business. Actually, this is more peculiar to small and medium scale organizations, as large corporations can acquire high-end systems, which are usually very expensive. Though cost effective, small and medium scale organizations like a university departments, departmental stores, and cyber cafes may not be able to afford them yet they can not avoid effective communication within and to the outside world.

Therefore, the need for an effective solution to provide network availability and reliability of 75% or more for small-scale organization calls for a genuine research.

1.4 OBJECTIVES

The aims and objectives of this project "Design and Implementation of Domain Type Local Area Networking (LAN)" are as follows:

1. To design and implement a star topology network base on IEEE 802.3 specifications, i.e. Ethernet.
2. To design and implement a domain type network, arrangements of server and clients computers that share common security database, unlike workgroup, which is a collection of computers like those in departments that do not require a central security.
3. To design and implementation of a network that reduces the task of network administrator that have to do with internet protocol (IP) address allocation and troubleshooting, system identification and network segmentation through the use of DHCP.
4. To create a LAN segment that can be used to host organization and individuals e.g. FUT Minna web sites in-house through the configuration of Internet information services (IIS), actually the main focus here is organization or individual corporate integrity as regards security of document contained in a web site. At least web site like www.futminna.edu can be hoisted right in the heart of the institution and accessible worldwide and/or beyond within the realm of the Internet. This increases content security and privacy as an alternative to this is to out source external hosting of the web site.
5. To exploit the multitasking and multi-user capabilities of super systems.

1.5 PROJECT OVERVIEW

In the 1980s, the desktop computer emerged as a low-cost alternative to terminals connected to a high-priced mainframe. Each desktop computer was capable of integrating peripherals and software to accomplish certain tasks, but data transfer between systems all too often required the cumbersome intervention of a human with a floppy disk. As the computer industry grew, PC managers, marketers, users, and designers began to see the advantages of sharing data and hardware among a group of individual, by cooperating, PCs. The first PC network operating systems (such as Novell NetWare and Microsoft LAN Manager) were designed as add-ons to existing desktop operating systems. A new breed of PC operating systems, such as Microsoft Windows 95 and Windows NT, now include a fully integrated system of network services. The integration of network services within personal desktop operating systems and the public emergence of the worldwide network—the Internet—have generated incredible momentum in the movement to "get connected." Networks have become the primary means of disseminating information in most modern offices.

Networking Concepts and Components

A network is a group of interconnected systems sharing services and interacting by means of a shared communications link (see fig.1 .1).

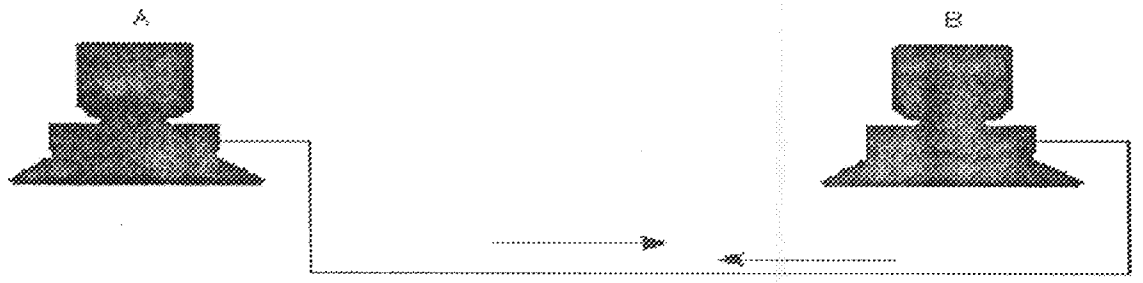

Fig. 1.1At its simplest, a computer network is two or more computers sharing information across a common transmission medium

A network, therefore, requires two or more individual systems with something to share (data). The individual systems must be connected through a physical pathway (called the transmission medium). All systems on the physical pathway must follow a set of common communication rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules that govern computer communication are called protocols.

In summary, all networks must have the following:

Something to share (data).

A physical pathway (transmission medium)

Rules of communication (protocols)

Merely having a transmission pathway does not produce communication.

When two entities communicate, they do not merely exchange data; rather, they understand the data they receive from each other. The goal of computer networking, therefore, is not simply to exchange data, but to be able to understand and use data received from other entities on the network. Because all computers are different, are used

in different ways, and can be located at different distances from each other, enabling computers to communicate is often a daunting task that draws on a wide variety of technologies. Remembering that the term network can be applied to human communication can be useful. When you are in a classroom, for example, the people in that class form a human information network (see fig.1.2). In computer terms, the instructor is the server, and the students are network clients. When the instructor speaks, the language he uses is equivalent to a computer protocol. If the instructor speaks French, and the student understands only English, the lack of a common protocol makes productive communication difficult. Likewise, air is the transmission medium for human communication. Sound is really nothing more than wave vibrations transmitted across the air to our eardrums, which receive and interpret the signals. In a vacuum, we cannot communicate via speech because our transmission pathway is gone.

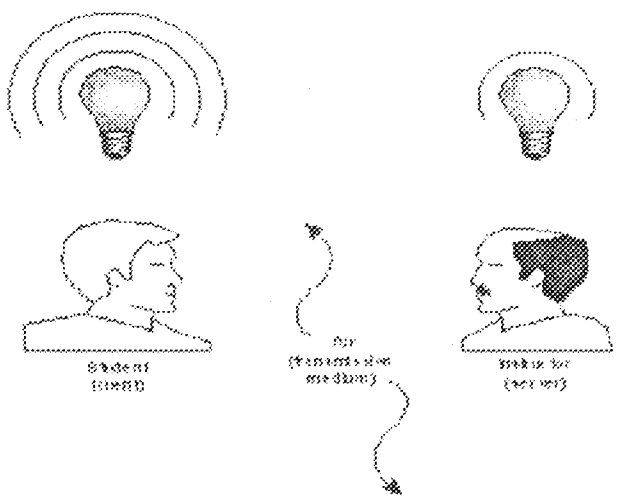

Fig. 1.2 Human communications is a kind of network.

The goals of computer networking are to provide services and to reduce equipment costs. Networks enable computers to share their resources by offering services to other computers.

Some of the primary reasons for networking PCs are as follows:

Sharing files

Sharing printers and other devices

Enabling common administration and security

Supporting network applications such as electronic mail and

Database services.

Models of Network Computing

After you have the necessary prerequisites for network communication, a structure must be put in place that organizes the way communication and sharing occur. Three methods of organization, or models, are generally recognized. The three models for network computing are as follows:

Centralized computing

Distributed computing

Collaborative or cooperative computing

Network Models: Comparing Server-Based and Peer-to-Peer Configurations

PC networks generally fall within one of these two network types:

Server-based

A server-based network consists of a group of user-oriented PCs (called clients) that request and receive network services from specialized computers called servers. Servers are generally higher-performance systems; optimized to provide network services to other PCs. (Some common server types include file servers, mail servers, print servers, fax servers, and application servers.) A good example of server-based network is Domain, in

Microsoft networks, an arrangement of client and server computers referenced by a specific name that shares a single security permissions database.

Peer-to-peer

A peer-to-peer network is a group of user oriented PC's that basically operate as equals. Each PC is called a peer. The peers share resources, such as files and printers, but no specialized servers exist. Each peer is responsible for its own security, and, in a sense, each peer is both a client (because it requests services from the other peers) and a server (because it offers services to the other peers). Small networks—usually under 10 machines—may work well in this configuration. Many network environments are a combination of server-based and peer-to-peer networking models. A good configuration of peer-to-peer network is Workgroup, a group of computer working together and shares the same files and database over a local area network (LAN).

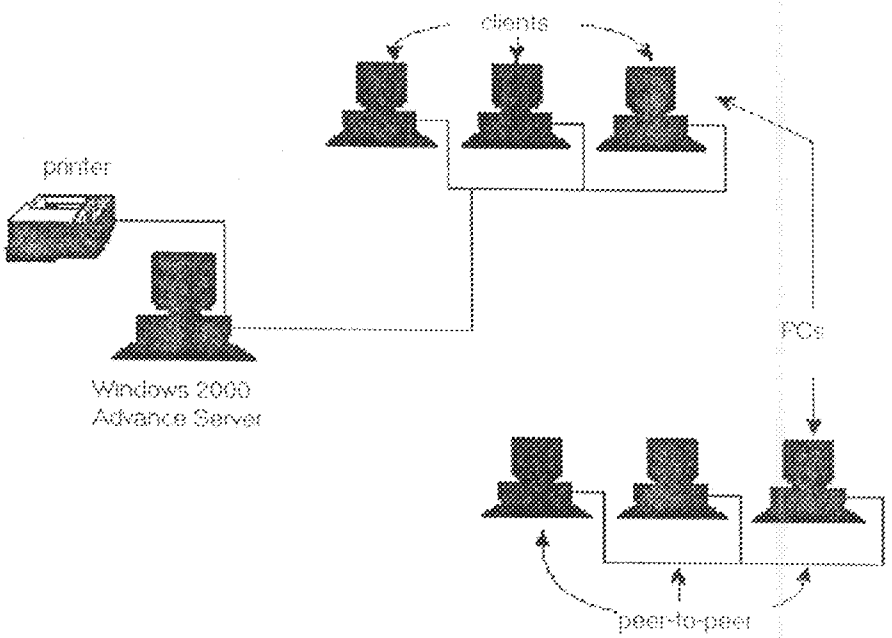

Fig.1 .3 Windows 2000 Advance Server is optimized for file, print, and application services. Network client operating systems are optimized for desktop performance, either as a network client or as a peer.

Local and Wide Area Networks

Networks come in all shapes and sizes. Network administrators often classify networks according to geographical size. Networks of similar size have many similar characteristics. The most common size classifications are the following:

Local area networks (LANs);

Wide area networks (WANs).

Each of these size classifications is described in the following sections.

Local Area Networks (LANs)

A local area network (LAN) is a group of computers and network communication devices interconnected within a geographically limited area, such as a building or campus. A LAN tends to use only one type of transmission medium—cabling. LANs are characterized by the following:

They transfer data at high speeds;

They exist in a limited geographical area;

Their technology is generally less expensive.

Wide Area Networks (WANs)

A wide area network (WAN) interconnects LANs. A WAN may be located entirely within a state or country, or it may be intereonnected around the world.

WANs are characterized by the following:

They exist in an unlimited geographical area;

They are more susceptible to errors due to the distances data travels;

They interconnect multiple LANs;

They are more sophisticated and complex than LANs; their technology is expensive.

WANs are often a natural outgrowth of the need to connect geographically separate LANs into a single network. For instance, a company might have several branch offices in different cities. Every branch would have its own LAN so that branch employees could share files and other resources, and all the branches together would be part of a WAN, a greater network that enables the exchange of files, messages, and application services between cities. Much of the complexity and expense of operating a WAN is caused by the great distances that the signal must travel to reach the interconnected segments. WAN links are often slower and typically depend on a public transmission medium leased from a communications service provider.

Metropolitan Area Networks (MANs)

These are networks that tend to occupy the ever widening between LANs and WANs. Also, usually private, MAN is a large network, typically constructed to span locations within a single big complex e.g. a Federal University of Technology, Bosso Campus, Minna, Niger State. It is also a collection of LANs, unlike WANs, this collection of LANs that are not all that logically isolated. Large companies within the same, though large, complex frequently use this type of network.

Network Operating Systems

The PCs in a network must have special system software that enables them to function in a networking environment. The early network operating systems were really add-on packages that supplied the networking software for existing operating systems, such as

MS-DOS or OS/2. More recent operating systems, such as Microsoft Corporation Windows- 9X, NT 4.0, 2000, XP, 2003 come with the networking components built in. Client and server machines require specific software components. A computer that is in a peer-to-peer network is functioning as both a client and a server and thus requires both client and server software. Operating systems, such as Windows 2000 Advance Server, include dozens of services and utilities that facilitate networking.

CHAPTER TWO

2.0 SYSTEM DESIGN AND ANALYSIS

2.1 Transmission Media

Twisted-Pair Cable

Twisted-pair cable has become the dominant cable type for all new network designs that employ copper cable. Among the several reasons for the popularity of twisted-pair cable, the most significant is its low cost. Twisted-pair cable is inexpensive to install and offers the lowest cost per foot of any cable type. A basic twisted-pair cable consists of two strands of copper wire twisted together (see fig. .1). This twisting reduces the sensitivity of the cable to EMI and also reduces the tendency of the cable to radiate radio frequency noise that interferes with nearby cables and electronic components. This is because the radiated signals from the twisted wires tend to cancel each other out.

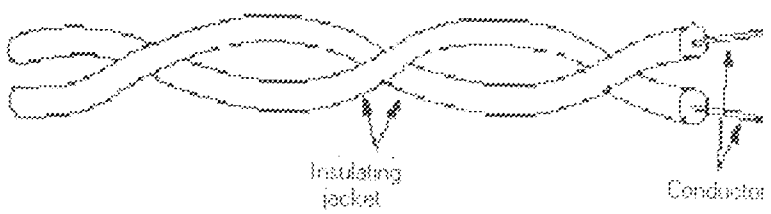

Fig. 1.1.Twisted pair cable

Twisting also controls the tendency of the wires in the pair to because EMI in each other. Whenever two wires are in close proximity, the signals in each wire tend to produce noise, called crosstalk, in the other. Twisting the wires in the pair reduces crosstalk in much the same way that twisting reduces the tendency of the wires to radiate EMI. Two types of twisted-pair cable are used in LANs: shielded and unshielded. Typically, Ethernet networks use unshielded twisted pair (UTP), although, some varieties of local

area network such as Token ring network use shielded twisted pair (STP). The contemporary interest in using unshielded twisted pair (UTP) wiring has resulted in a scheme for cabling that uses unshielded twisted pair (UTP): the 10BASE-T cabling standard, which uses UTP in a star physical topology.

Unshielded Twisted-Pair (UTP) Cable

Unshielded twisted-pair cable doesn't incorporate a braided shield into its structure. However, the characteristics of UTP are similar in many ways to STP, differing primarily in attenuation and EMI. As shown in figure .2, several twisted-pairs can be bundled together in a single cable. These pairs typically are color coded to distinguish them. Telephone systems commonly use UTP cabling. Network engineers can sometimes use existing UTP telephone cabling (if it is new enough and of a high enough quality to support network communications) for network cabling.

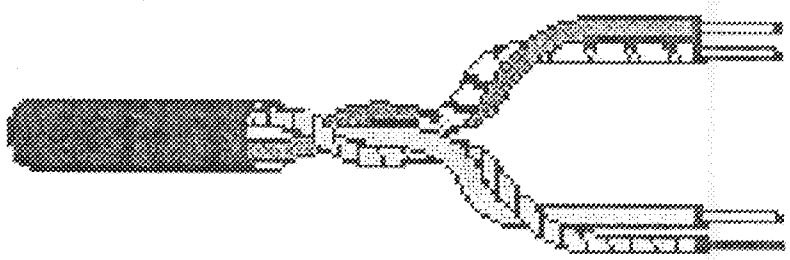

Fig. 1.2 Multipair UTP cable

UTP cable is a latecomer to high-performance LANs because engineers only recently solved the problems of managing radiated noise and susceptibility to EMI. Now, however, a clear trend toward UTP is in operation, and all new copper-based cabling schemes are based on UTP. UTP cable is available in the following five grades, or categories:

Categories 1 and 2; these voice-grade cables are suitable only for voice and for low data rates (below 4 Mbps). Category 1 was once the standard voice-grade cable for telephone systems.

Category 3; as the lowest data-grade cable, this type of cable generally is suited for data rates up to 10 Mbps. Some innovative schemes, however, enable the cable to support data rates up to 100 Mbps. Category 3, which uses four twisted-pairs with three twists per foot, is now the standard cable used for most telephone installations.

Category 4; this "data-grade cable", which consists of four twisted-pairs, is suitable for data rates up to 16 Mbps.

Category 5; this "data-grade cable", which also consists of four twisted-pairs, is suitable for data rates up to 100 Mbps. Most new cabling systems for 100 Mbps data rates are designed around Category 5 cable. In a UTP cabling system, the cable is only one component of the system. UTP cable offers an excellent balance of cost and performance characteristics.

Cost

UTP cable is the least costly of any cable type, although properly installed Category 5 tends to be fairly expensive. In some cases, existing cable in buildings can be used for LANs, although, the network engineer should verify the category of the cable and know the length of the cable in the walls. Distance limits for voice cabling are much less stringent than for data-grade cabling.

Installation

UTP cable is easy to install. Some specialized equipment might be required, e.g. crimping tool, can be mastered with a bit of practice. Properly designed UTP cabling

systems easily can be reconfigured to meet changing requirements. A UTP for LAN can either be configured as a straight- through, for connection between a node and hub or a crossed-over, used for direct connection between two nodes

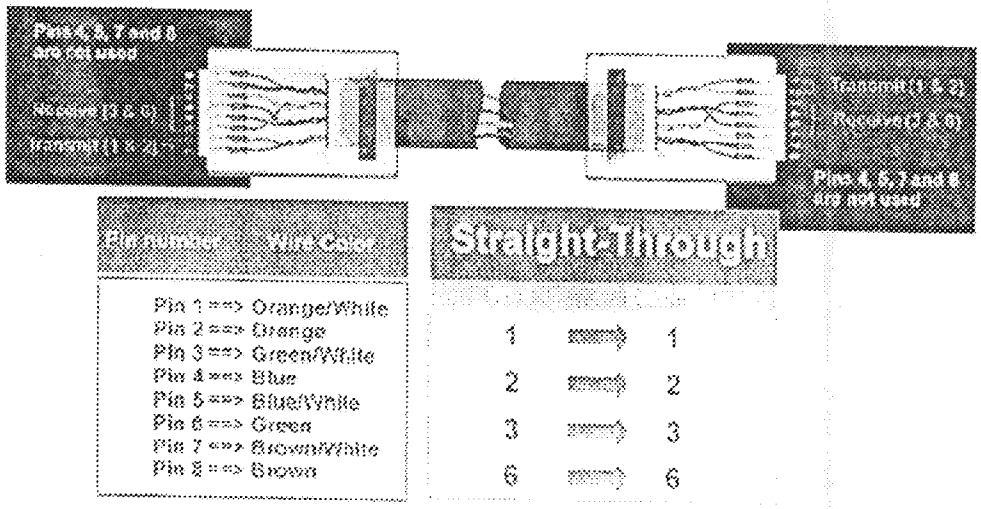

Fig.1.3. *Straight-through termination of UTP*

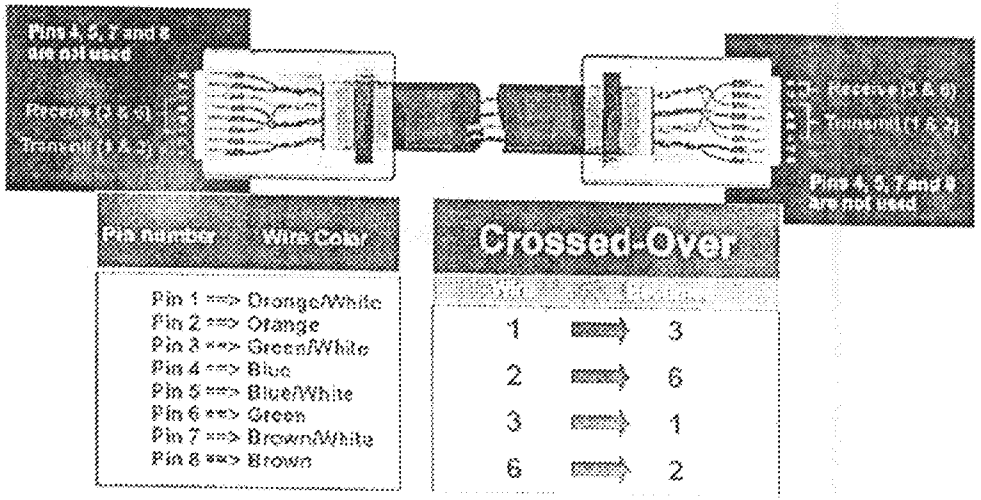

Fig.1.4. Crossed-over termination of UTP

Capacity

The data rates possible with UTP have pushed up from 1 Mbps, past 4 and 16 Mbps, to the point where 100 Mbps data rates are now common.

Attenuation

UTP cable shares similar attenuation characteristics with other copper cables. UTP cable runs are limited to a few hundred meters, with 100 meters as the most frequent limit.

EMI Characteristics

Because UTP cable lacks a shield, it is more sensitive to EMI than coaxial or STP cables. The latest technologies make it possible to use UTP in the vast majority of situations, provided that reasonable care is taken to avoid electrically noisy devices such as motors and fluorescent lights. Nevertheless, UTP might not be suitable for noisy environments such as factories. Crosstalk between nearby unshielded pairs limits the maximum length of cable runs.

Connectors for UTP

The most common connector used with UTP cables is the RJ-45 connector, shown in figure 1.5. These connectors are easy to install on cables and are also extremely easy to connect and disconnect. An RJ-45 connector has eight pins and looks like a common RJ-11 telephone jack. They are slightly different sizes and won't fit together: an RJ-11 has only four pins.

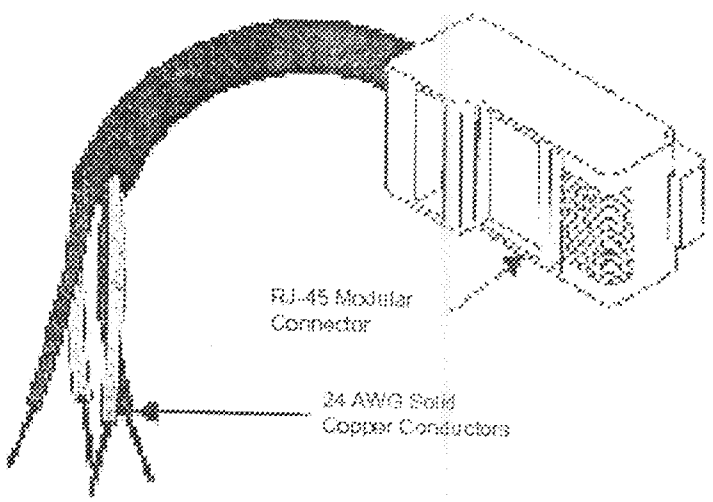

Fig.1.5. An RJ-45 connector

Distribution racks, shelves, and patch panels are available for large UTP installations. These accessories enable you to organize network cabling and also provide a central spot for expansion and reconfiguration. One necessary accessory, a *jack coupler*, is a small device that attaches to a wall plate or a patch panel and receives an RJ-45 connection. Jack couplers can support transmission speeds of up to 100 Mbps.

Table 1.1

Comparison of Cable Media

Cable Type	Cost	Installation	Capacity	Range	EMI
Coaxial Thinnet	<STP	Inexpensive/ easy	10 Mbps typical	185 m	<sensitive than UTP
Coaxial Thicknet	>STP <fiber	Easy	10 Mbps typical	500 m	<sensitive than UTP
Shielded Twisted-Pair (STP)	>UTP <Thicknet	Relatively easy	16 Mbps typical up to 500 Mbps	100 m typical	<sensitive than UTP
Unshielded Twisted-Pair (UTP)	Lowest	Inexpensive/ easy	10 Mbps typical up to 100 Mbps	100 m typical	Most sensitive
Fiber-Optic	Highest	Expensive/ difficult	100 Mbps typical	10s of kilometers	Insensitive

2.2 Network Topologies and Architectures

Access Methods

An *access method* is a set of rules governing how the network nodes share the transmission medium. The rules for sharing among computers are similar to the rules for sharing among humans in that they both boil down to a pair of fundamental philosophies: 1) first come, first serve and 2) take turns. These philosophies are the principles defining the two most important types of media access methods:

Contention: in its purest form, contention means that the computers are contending for use of the transmission medium. Any computer in the network can transmit at any time (first come, first serve) unlike token passing- the computers take turns.

Contention-based access methods can give rise to situations in which two or more of the network nodes try to broadcast at the same time and the signals collide. Specifications for contention-based access methods include procedures for how to avoid collisions and what to do if a collision occurs. On most contention-based networks, the nodes are basically equal. No node has a higher priority than other nodes. A new access method called demand priority, however, resolves contention and collisions and in so doing accounts for data type priorities. Contention in pure contention-based access control, any computer can transmit at any time. This system breaks down when two computers attempt to transmit at the same time, in which case a collision occurs (see fig.1.6). Eventually, when a network gets busy enough, most attempts to transmit result in collisions and little effective communication can take place.

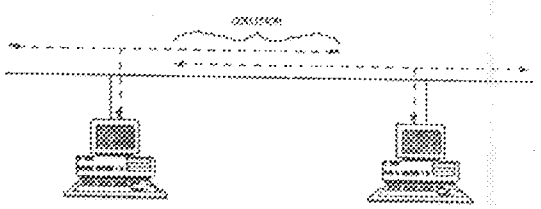

Fig.1.6. Collision on a contention- based network

Mechanisms, therefore, usually are put into place to minimize the effects of collisions. One mechanism is carrier sensing, whereby each computer listens to the network before attempting to transmit. If the network is busy, the computer refrains from transmitting

until the network quiets down. This simple "listen before talking" strategy can significantly reduce collisions. Another mechanism is *carrier detection*. With this strategy, computers continue to listen to the network as they transmit. If a computer detects another signal that interferes with the signal it's sending, it stops transmitting. Both computers then wait a random amount of time and attempt to retransmit. Unless the network is extremely busy, carrier detection along with carrier sensing can manage a large volume of transmissions. Carrier detection and carrier sensing used together form the protocol used in all types of Ethernet: *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*. CSMA/CD limits the size of the network to 2,500 meters. At longer distances, the broadcast-sensing mechanisms don't work—a node at one end can't sense when a node at the other end starts to broadcast. Contention (in particular CSMA/CD in the form of Ethernet) is the most popular media access control method on LANs. Contention is a simple protocol that can operate with simple network software and hardware.

2.3 Physical and Logical Topologies

A topology defines the arrangement of nodes, cables, and connectivity devices that make up the network. Two basic categories form the basis for all discussions of topologies:

Physical topology: Describes the actual layout of the network transmission media

Logical topology: Describes the logical pathway a signal follows as it passes among the network nodes. Another way to think about this distinction is that a physical topology defines the way the network *looks*, and a logical topology defines the way the *data passes* among the nodes. A network with a star physical topology, for example, may actually have a bus or a ring logical topology. In common usage, the word "topology" applies to a

complete network definition, which includes the physical and logical topologies and also specifications for elements such as the transmission medium.

The three topologies are: bus topologies, ring topologies and star topologies. The network under consideration uses a star-bus topology- logical topology but is configured in a star physical topology.

Bus Topologies

A *bus physical topology* is one in which all devices connect to a common, shared cable (sometimes called the *backbone*). A bus physical topology is shown in figure

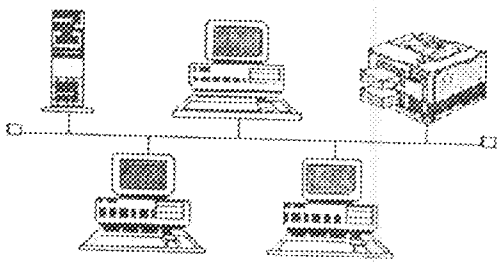

Fig.1.7. *A bus physical topology*

It is correct to believe that the bus topology seems ideally suited for the networks that use contention-based access methods such as CSMA/CD. Ethernet, the most common contention-based network architecture, typically uses bus as a physical topology.

10BASE-T Ethernet networks use bus as a logical topology but are configured in a star physical topology.

Star Topologies

Star topologies require that all devices connect to a central hub (see fig. .8). The hub receives signals from other network devices and routes the signals to the proper destinations. Star hubs can be interconnected to form *tree* or *hierarchical* network topologies.

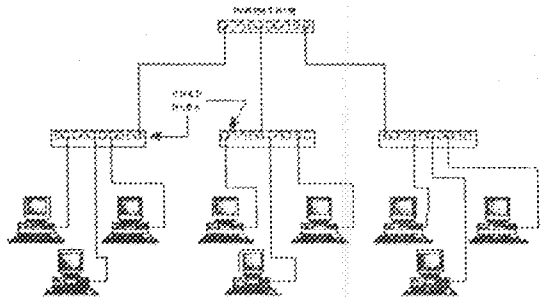

Fig.1.8.*A* a cascaded star topology

A *star physical topology* means that the nodes are all connected to a central hub. The path the data takes among the nodes and through that hub (the logical topology) depends on the design of the hub, the design of the cabling, and the hardware and software configuration of the nodes.

2.4 Ethernet

Ethernet is a very popular local area network architecture based on the CSMA/CD access method. The original Ethernet specification was the basis for the IEEE 802.3 specifications. In present usage, the term Ethernet refers to original Ethernet (or Ethernet II, the latest version) as well as the IEEE 802.3 standards. The different varieties of Ethernet networks are commonly referred to as *Ethernet topologies*. Typically, Ethernet networks use a bus physical topology, although, some varieties of Ethernet such as 10BASE-T use a star physical topology and a bus logical topology. (Microsoft uses the term "star bus" topology to describe 10BASE-T.) Ethernet networks, depending on the specification, operate at 10 or 100 Mbps using baseband transmission. Each of the IEEE 802.3 specifications prescribes its own cable types. Ethernet topology begins with a number (10 or 100). That number specifies the transmission speed for the network. For instance, 10BASET is designed to operate at 10Mbps; BASE band signal using Twisted pair cable.

Ethernet Frame

Ethernet networks transmit data in small units called *frames*. The size of an Ethernet frame can be anywhere between 64 and 1,518 bytes. Fighteen bytes of the total size are taken up by frame overhead, such as the source and destination addresses, protocol information, and error-checking information. A typical Ethernet II frame has the following sections:

Preamble; A field that signifies the beginning of the frame

Addresses; Source and destination addresses for the frame

Type; A field that designates the Network layer protocol

Data; The data being transmitted

CRC; Cyclical Redundancy Check for error checking

Ethernet Cabling

Engineers can use a variety of cables to implement Ethernet networks. Many of these cable types—Thinnet, Thicknet, and UTP. Ethernet networks traditionally have used coaxial cables of several different types. Fiber-optic cables now are frequently employed to extend the geographic range of Ethernet networks. The contemporary interest in using twisted-pair wiring has resulted in a scheme for cabling that uses unshielded twisted-pair (UTP): the 10BASE-T cabling standard, which uses UTP in a star physical topology. Ethernet remains closely associated with coaxial cable. Two types of coaxial cable still used in small and large environments are Thinnet (10BASE2) and Thicknet (10BASE5). Thinnet and Thicknet Ethernet networks have different limitations that are based on the Thinnet and Thicknet cable specifications.

10BASE-T

The trend in wiring Ethernet networks is to use unshielded twisted-pair (UTP) cable. 10BASE-T. It is based on the IEEE 802.3 standard. 10BASE-T supports a data rate of 10Mbps using baseband. 10BASE-T cabling is wired in a star topology. The nodes are wired to a central hub, which serves as a multiport repeater (see fig. 9). A 10BASE-T network functions logically as a linear bus. The hub repeats the signal to all nodes, and the nodes contend for access to the transmission medium as if they were connected along a linear bus. The cable uses RJ-45 connectors, and the network adapter cards used have RJ-45 jacks built into the back of the card.

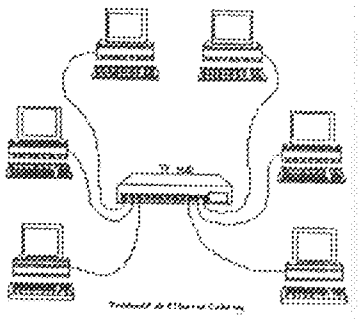

Fig.1.9. *A 10BASET network*

10BASE-T segments can be connected using coaxial or fiber optic backbone segments. Some hubs provide connectors for Thinnet and Thicknet cables (in addition to 10BASE-T UTP-type connectors). The star wiring of 10BASE-T provides several advantages, particularly in larger networks. First, the network is more reliable and easier to manage because 10BASE-T networks use a concentrator (a centralized wiring hub). These hubs are "intelligent" in that they can detect defective cable segments and route network traffic around them. This capability makes locating and repairing bad cable segments easier. 10BASE-T enables the design and implementation of one LAN segment at a time,

growing, as your network needs to grow. In some cases in which a data-grade phone system already has been used in an existing building, the data-grade phone cable can be used for the LAN. The maximum unshielded cable segment length (hub to transceiver) is 100 meters (328 feet). The cable distance between computers is 2.5 meters (8 feet).

2.5 Packets and Protocols

The purpose of a network is to exchange information among computers, and protocols are the rules by which computers communicate. Computers, like humans, can adopt any number of systems for passing messages as long as the sending and receiving computers are using the same (or compatible) rules. Computers, therefore, must agree on common protocols before they can communicate. Protocols describe the way in which network data is encapsulated in packets on the source end, sent via the network to a destination, and then reconstructed at the destination into the appropriate file, instruction, or request. Breaking network data into packet-sized chunks provides smoother throughput because the small packets don't tie up the transmission medium as a larger unit of data might. Also, packets simplify the task of error detection and correction. Each packet is checked separately for errors, and if an error is discovered, only that packet (instead of a whole file) must be retransmitted. The exact composition of a network packet depends on the protocols used. In general, network packets contain the following:

Header; the header signifies the start of the packet and contains a bundle of important parameters, such as the source and destination address and time/synchronization information.

Data; this portion of the packet contains the original data being transmitted.

Trailer; the trailer marks the end of the packet and typically contains error-checking (Cyclical Redundancy Check, or CRC) information. As the data passes down through the protocol layers, each layer performs its prescribed function, such as interfacing with an application, converting the data format, or adding addressing and error-checking parameters. When the packet reaches the transmission medium, the network adapter cards of other computers on the network segment examine the packet, checking the packet's destination address. If the destination address matches the PC's address, the network adapter interrupts the processor, and the protocol layers of the destination PC process the incoming packet.

2.6 OPEN SYSTEM INTERCONNECTION (OSI) MODEL

This is a reference model for network components interoperability developed by the International Standard Organization (ISO) to promote cross-vendor compatibility of hardware and software network systems. The open system interconnection model splits the process of networking into seven distinct services of layers. The seven layers, in a particular sequence are: Application layer; Presentation layer; Session layer; Transport layer; Network layer; Data Link layer; and the Physical layer. One layer uses the services of the layer immediately below it.

The upper layers of the OSI model (application, presentation, and session—Layers 7, 6, and 5) are oriented more toward services to the applications. The lower four layers (transport, network, data link, and physical—Layers 4, 3, 2, and 1) are oriented more toward the flows of data from end to end through the network based

OSI Reference Model

Application (Layer 7)

An application that communicates with other computers is implementing OSI application layer concepts. The application layer refers to communications services to applications. The protocols used by this layer include: Telnet, HTTP, FTP, WWW browsers, NFS, SMTP, SNMP, etc. The function is how data is displayed- User interface.

Presentation (Layer 6)

This layer's main purpose is defining data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG. Encryption is also defined by OSI as a presentation layer service. Examples of protocols used are JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, Encryption, MPEG, and MIDI. The functions are how data is presented and special processing such as encryption.

Session (Layer 5)

The session layer defines how to start, control, and end conversations (called sessions). This includes the control and management of multiple bi-directional messages so that the application can be notified if only some of a series of messages are completed. This allows the presentation layer to have a seamless view of an incoming stream of data. The protocols involved include RPC, SQL, NFS, and NetBIOS names, AppleTalk ASP, DECnet SCP. The function is keeping data separate from different applications. Example is Operating systems and application access scheduling.

Transport (Layer 4)

Layer 4 includes the choice of protocols that either do or do not provide error recovery. Multiplexing of incoming data for different flows to applications on the same host (for example, TCP sockets) is also performed. Reordering of the incoming data stream when

packets arrive out of order is included. The function is to ensure reliable or unreliable delivery of data and multiplexing TCP, UDP, and SPX.

Network (Layer 3)

This layer defines end-to-end delivery of packets. To accomplish this, the network layer defines logical addressing so that any endpoint can be identified. It also defines how routing works and how routes are learned so that the packets can be delivered. The network layer also defines how to fragment a packet into smaller packets to accommodate media with smaller maximum transmission unit sizes. The protocols used include IP, IPX, and AppleTalk DDP. Some protocols define details of multiple layers.

Data link (Layer 2)

The data link (Layer 2) specifications are concerned with getting data across one particular link or medium. The data link protocols define delivery across an individual link. These protocols are necessarily concerned with the type of media in question; for example, 802.3 and 802.2 are specifications from the IEEE, which are referenced by OSI as valid data link (Layer 2) protocols. The functions include combination of bits into bytes, and bytes into frames, access to the media using MAC address, error detection and error recovery.

Physical (Layer 1)

This layer deals with the physical characteristics of the transmission medium. Connectors, pins, use of pins, electrical currents, encoding, and light modulation are all part of different physical layer specifications. Multiple specifications are sometimes used to complete all details of the physical layer. Specifications used to complete all details of physical layer include EIA/TIA-232, V.35, EIA/TIA- 449, V.24, RJ45, Ethernet, 802.3,

802.5, FDDI, NRZI, NRZ, B8ZS. The functions include moving of bits between devices Specification of voltage, wire speed, and cable pin-outs.

Connection-Oriented Versus Connectionless Protocols

The terms *connection-oriented* and *connectionless* have some relatively well-known connotations inside the world of networking protocols.

Connection-oriented protocol: A protocol that either requires an exchange of messages before data transfer begins or has a required pre-established correlation between two endpoints.

Connectionless protocol: A protocol that does not require an exchange of messages and that does not require a pre-established correlation between two endpoints.

2.7 Protocols and Protocol Layers

Many of the addressing, error-checking, retransmission, and acknowledgment services most commonly associated with networking take place at the Network and Transport OSI layers.

Internet Protocols (TCP/IP)

The Internet protocol suite (also commonly called the TCP/IP protocol suite) was originally developed by the United States Department of Defense (DOD) to provide robust service on large internetworks that incorporate a variety of computer types. In recent years, the Internet protocols constitute the most popular network protocols currently in use. TCP/IP evolved in response to input from a wide variety of industry sources. Consequently, TCP/IP is the most open of the protocol suites and is supported by the widest variety of vendors.

Internet Protocol (IP)

The Internet Protocol (IP) is a connectionless protocol that provides datagram service, and IP packets are most commonly referred to as IP datagrams. IP is a packet-switching protocol that performs addressing and route selection. An IP header is appended to packets, which are transmitted as frames by lower-level protocols. IP routes packets through internetworks by utilizing dynamic routing tables that are referenced at each hop. Consulting logical and physical network device information, as provided by the Address Resolution Protocol (ARP), makes routing determinations. IP performs packet disassembly and reassembly as required by packet size limitations defined for the Data Link and Physical layers being implemented. IP also performs error checking on the header data using a checksum, although data from upper layers is not error-checked.

Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) enhances the error control provided by IP. Connectionless protocols, such as IP, cannot detect internetwork errors, such as congestion or path failures. ICMP can detect such errors and notify IP and upper-layer protocols.

Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is an internetwork protocol that corresponds to the OSI Transport layer. TCP provides full duplex, end-to-end connections. When the overhead of end-to-end communication acknowledgment isn't required, the User Datagram Protocol (UDP) can be substituted for TCP at the Transport (host-to-host) level. TCP and UDP operate at the same layer. TCP maintains a logical connection between the sending and receiving computer systems. In this way, the integrity of the

transmission is maintained. TCP detects any problems in the transmission quickly and takes action to correct them. TCP isn't as fast as UDP. TCP also provides message fragmentation and reassembly and can accept messages of any length from upper-layer protocols. TCP fragments message streams into segments that can be handled by IP.

User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless Transport (host-to-host) layer protocol. UDP does not provide message acknowledgments; rather, it simply transports datagrams. UDP is preferred over TCP when high performance or low network overhead is more critical than reliable delivery. Because UDP doesn't need to establish, maintain, and close connections, or control data flow, it generally outperforms TCP. UDP is the Transport layer protocol used with the *Simple Network Management Protocol (SNMP)*, the standard network management protocol used with TCP/IP networks. UDP enables SNMP to provide network management with a minimum of network overhead.

Address Resolution Protocol (ARP)

Three types of address information are used on TCP/IP internetworks:

1. Physical addresses; used by the Data Link and Physical layers. Otherwise, referred to as media access control (MAC) address

2. IP addresses; Provide logical network and host IDs. IP addresses consist of four numbers typically expressed in dotted decimal form. An example of an IP address is 134.135.100.13.

3. Logical node names; identify specific hosts with alphanumeric identifiers, which are easier for users to recall than the numeric IP addresses. An example of a logical node name is NetSERV. Given a logical node name, the Address Resolution Protocol (ARP)

can determine the IP address associated with that name. ARP maintains tables of address resolution data and can broadcast packets to discover addresses on the internetwork. The IP addresses discovered by ARP can be provided to Data Link layer protocols.

Domain Name System (DNS)

The Domain Name System (DNS) protocol provides name and address resolution as a service to client applications. DNS servers enable humans to use logical node names to access network resources. As oppose to NetBIOS domain

The DNS has three major components:

- The DOMAIN NAME SPACE and RESOURCE RECORDS, which are specifications for a tree structured name space and data associated with the names. Conceptually, each node and leaf of the domain name space tree names a set of information, and query operations are attempts to extract specific types of information from a particular set. A query names the domain name of interest and describes the type of resource information that is desired. For example, the Internet uses some of its domain names to identify hosts; queries for address resources return Internet host addresses.

- NAME SERVERS are server programs, which hold information about the domain tree's structure and set information. A name server may cache structure or set information about any part of the domain tree, but in general a particular name server has complete information about a subset of the domain space, and pointers to other name servers that can be used to lead to information from any part of the domain tree. Name servers know the parts of the domain tree for which they have complete information; a name server is said to be an AUTHORITY for these parts of the name space. Authoritative information is organized into units called ZONEs, and these zones can be

automatically distributed to the name servers, which provide redundant service for the data in a zone.

- RESOLVERS are programs that extract information from name servers in response to client requests. Revolvers must be able to access at least one name server and use that name server's information to answer a query directly, or pursue the query using referrals to other name servers. A resolver will typically be a system routine that is directly accessible to user programs; hence no protocol is necessary between the resolver and the user program. For hosts, the mapping depends on the existing syntax for host names which is a subset of the usual text representation for domain names, together with RR formats for describing host addresses, etc. Because we need a reliable inverse mapping from address to host name, a special mapping for addresses into the IN-ADDR.ARPA domain is also defined.

Internet Information Services (IIS)

Windows 2000 Advanced Server computer by default, though it may be exempted for later installation. The following services are installed as a part of IIS: Hypertext Transfer Protocol (HTTP), which is used to create content for web sites as well as to navigate web sites; File Transfer Protocol (FTP), which is used to transfer files between two computers using the TCP/IP protocol; Simple Mail Transfer Protocol (SMTP), which is used to provide newsgroup services between NNTP servers and NNTP clients. Web site description is the same as the name of the website, this usually appears by default in the Internet Information Services window. There is provision for configuration of the IP address associated with the site being configured; this IP address has already been configured for the server computer. There is also an option for specification of TCP/IP

port, which is used to respond to HTTP requests- it is port 80 by default but could be changed for additional security. There is Connection option during the configuration of the IIS, to specify the number of concurrent connection to the web site. Other options like Connection Timeout to specify how long an inactive user can remain connected to the web site before a connection is automatically terminated, Logging used to record details of web access, Operators can also be selected through the Operators tab to configure the users and group that are able to manage the web site. Actually Administrators group is assigned operator privileges by default; operator could be added or removed from the list. Performance tab allows the configuration of performance turning and enabling of bandwidth throttling. Configuration Home Directory Options, which includes options for content location, access permissions, content control and application settings.

The Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. DHCP supports three mechanisms for IP address allocation, are: automatic allocation, dynamic allocation and manual allocation. A DHCP client is an Internet host using DHCP to obtain configuration parameters such as a network address. A DHCP server is an Internet host that returns configuration parameters to DHCP clients. A BOOTP relay agent or relay agent is an Internet host or router that passes DHCP messages between DHCP clients and DHCP servers. The goals of DHCP

include the followings: DHCP should be a mechanism rather than a policy, Clients should require no manual configuration, Networks should require no manual configuration for individual clients, DHCP should not require a server on each subnet, a DHCP client must be prepared to receive multiple responses to a request for configuration parameters and DHCP must coexist with statically configured, non-participating hosts and with existing network protocol implementations.

File Transfer Protocol (FTP)

The *File Transfer Protocol (FTP)* is a protocol for sharing files between networked hosts. FTP enables users to log on to remote hosts. Logged-on users can inspect directories, manipulate files, execute commands, and perform other commands on the host. FTP also has the capability of transferring files between dissimilar hosts by supporting a file request structure that is independent of specific operating systems.

Simple Mail Transfer Protocol (SMTP)

The *Simple Mail Transfer Protocol (SMTP)* is a protocol for routing mail through internetworks. SMTP uses the TCP and IP protocols. SNMP doesn't provide a mail interface for the user. Creation, management, and delivery of messages to end-users must be performed by an e-mail application. (The most popular e-mail application on the Internet is named Eudora.)

Remote Terminal Emulation (TELNET)

TELNET is a terminal emulation protocol. TELNET enables PCs and workstations to function as dumb terminals in sessions with hosts on internetworks. TELNET implementations are available for most end-user platforms.

Other protocols are network file system (NFS), the internetwork Packet Exchange protocol (IPX), etc.

3.0 CHAPTER THREE

This chapter reports the implementation procedures of the hardware layout, testing and result obtained.

3.1 IMPLEMENTATION

In order to effect a smooth implementation, the entire project was divided into group. Then a component layout plan was designed to ease solutions to implementation problems.

COMPONENT LAYOUT

The components making up the project layout include:

1. The network server computer
2. Network client computers
3. Network cables
4. Hub

The systems were arranged in such a manner that will suit the system operators and the optimum setting of the location but not to sacrifice network installation precautions. Each system, including the network server, was connected to the hub using straight- through UTP cable with RJ45 terminator via the Ethernet adapter. Actually, the network server ought to be kept in position not within the reach of all and comers but as far as the installation and configuration are concerned the network server could not be isolated but consideration was given to its safety.

3.2 INSTALATION AND CONFIGURATION

The network server and the clients were installed; in this case Windows 2000 Advanced Server was used as the server operating system and Windows 2000 Professional and other operating systems e.g. Windows 98, Windows XP, Linux, etc could be used as network client operating system. The configuration of the network started with the server. The major services that were configured include:

1. Transmission control protocol/Internet protocol (TCP/IP)
2. Dynamic host configuration protocol (DHCP) server
3. Domain naming system (DNS)
4. Active directory
5. Internet information services (IIS)

The network clients were configured and connected to the server with the necessary user profile with right to connect a network node to the network. It is of great importance here to note that configuring a network client with the necessary IP address, subnet mask address and what have you conforming to the settings of a domain type network, LAN or WAN, does not necessarily guarantee access to the network as the case with workgroup type of network where things are not centralized. The services configured on the network clients include:

1. Internet protocol (IP) address
2. Computer domain name
3. Clients for Microsoft network

To connect computer to a domain type of network there is a need to gather domain and account information. These include the following information

1. Username
2. Password
3. User account domain

Others, which might also be required, though are compulsory for Windows 2000 Advanced server controlled domains are:

1. Computer name

2. Computer domain

3.3 TESTING

Each computer was subjected to testing using the following tools at the command prompt:

IPCONFIG; this is used to access the current Internet protocol configuration of a host. This include host name, primary DNS suffix, node type, IP routing status, WINS proxy status, number of network adapter on the host with their description, physical (MAC) address, IP address, DHCP status, subnet mask, the default gateway and the DNS server(s). Options of the IPCONFIG command are:

1. /all, which display full configuration information.
2. /release, release the IP address for specified adapter (DHCP enabled adapter).
3. /renew, renew the IP address for specified adapter (same as release).
4. /flushdns, purges the DNS resolver cache.
5. /displaydns, display the contents of the DNS resolver cache.
6. /registerdns, refreshes all DHCP and re-register DNS name.
7. /showclassid, display all DHCP class Ids allowed for adapter.
8. /setclassid, modifies the DHCP class Id.

PING; this is Internet control message protocol (ICMP) echo message that sends and receives reply when a remote host bearing the IP address or DNS name as in the with Windows 2000 and its successors, has been reached. PING has the following options

1. –t, ping the specified host until stopped.
2. –a, resolve address to hostnames.

3. –n count, number of echo requests to send.
4. –l size, send buffer size.
5. –f, set do not fragment flag in packet.
6. –i TTL, time to live
7. –v TOS, type of service.
8. –r count, record route for count hops.
9. –s count, timestamp for count hops.
10. –w timeout, timeout in milliseconds to wait for each reply.

TRACERT: trace route (tracert) is used to count the number of hops between the host and a remote node bearing the referred IP address.

CHAPTER FOUR

4.1 CONCLUSSION

The aim and objective of this project has largely been achieved that is to design and implement low cost domain type local area network. This has been successfully carried out as described in the preceding chapters. This venture into the field of computer network engineering will server as a model for others who consider undertaking topics related to it

The final objective and its focus are to meaningfully contribute to the economy and provide optimum usage of the Internet and intranet. This combination of hardware and software devices is cost effective as in terms of upfront, running and maintenance cost.

4.2 RECOMMENDATION

In view of the strategic importance of intranet to our activities, the domain type of type domain local area networking gives the alternative to the common workgroup type of local area network. Based on this and the successes and limitations recorded by the project work, I wish to recommend the following:

1. Presently, almost all the Internet cyber cafes lack efficient services as regards reliability and availability, to this end a deliberate approach to the design and implementation of domain type local area networking by our research institutes and universities has to be adopted so that effective communication be ensured at any location.
2. Student should be encouraged to undertake research in other areas of computer engineering using low cost and effective hardware and software devices.
3. Every organization, even cyber café, can purpose domain type local area network instead of the epileptics, though thought to be simpler, workgroup type local area network.

REFERENCES

1. Internet Engineering Task Force (IETF) www.ieft.org. RFC1034, RFC1035 AND RFC 2131
2. Microsoft® Encarta® Encyclopedia 2003. © 1993-2002 Microsoft Corporation.
3. www.microsoft.com/hwtest/hcl
4. MCSE TRAINING GUIDE: Networking Essentials

   By Joe Casad and Dan Newland, MCSE, MCT

   New Riders Publishing

5. Lisa Donald with James Chellis

   MCSE: Windows 2000 Server Study Guide

   Copyright 2000 Sybex Inc. www.sybex.com.

   ISBN:0-7821-2752-5

5. Lisa Donald with James Chellis

   MCSE: Windows 2000 Server Study Guide

   Copyright 2000 Sybex Inc. www.sybex.com.

   ISBN:0-7821-2752-5

6. MCSE: Windows 2000 Directory Services Administration

   Anil Desai with James Chellis

   Copyright 2000 Sybex Inc.www.sybex.com.

   ISBN: 0-7821-2756-8