NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

Performance Investigation of Ethernet LAN

Graduation Project
COM - 400

Student: Ercan BAĞLI

Supervisor: Dr.Halil ADAHAN

Nicosia 2004

Acknowledgements

First I want to thank Halil ADAHAN to be my advisor. Under his guidance, I successfully overcome many difficulties and learn a lot about student registration system with LAN Network Management. In each discussion, he explained my questions patiently, and I felt my quick progress from his advices. He always helps me a lot either in my study or my life. I asked him many questions in my subject and he always answered my questions quickly and in detail.

My thanks and regard goes to Faculty of Engineering staff for having such a good computational and electronically environment.

Special thanks to Ümit İLHAN and Kaan UYAR for their practical advices. And thanks to Faculty of Engineering for having such a good computational and computer environment.

I also want to thank to my friends in Near East University. Special thanks to Ayhan for helping computer side of my project, Ferit.

Finally, I want to thank my family, especially my parents. Without their endless support and love for me, I would never achieve my current position. I wish my mother and father lives happily always.

Abstract

I prepared this Graduation Project as a result of my graduation studies. The main topic of this project is Performance Investigation of The Ethernet LAN. I selected topic because of my interest in Network system and LAN segments in these networks. I thought that I can learn more about networks and their performance analysis, and this work would be a good experience for me. I chose this topic in the beginning of the semester, and then I started to research about this topic. I tried to find a good approaching way. I also asked my supervisor Mr. Halil Adahan and he orders me to use the Starter and Performance Evaluations in this project to investigate the performance analysis of the LAN. I greatly appreciate to Mr. Halil Adahan for answering all my questions; he was very helpful to me.

Table of Contents

List of Figures

Chapter I: Introduction

1.1 Purposes of Networking

By bringing together the already rapidly expanding technologies of computing and telecommunications, computer networks is adding to both of these technologies capabilities that neither of them would have separately.

On the one hand, it makes possible a form of computing that is distributed in several ways. For example, several users at different locations can access the same computing system. The same user can carry out a data processing job, different parts of which are carried out by different computers in a network. A group of linked users can use their own computers or "intelligent" terminals for some purposes, but also use commonly held file stores, printers or processors for others. Users can not only access a very wide variety of computer data bases, sometimes over very long distances, but often extract and transform for their own purposes selected subsets of the information that these data bases contain.

On the other hand, computer networking adds an extra dimension to the scope of telecommunications in the ordinary sense. It provides several communications media and channels for numerical data, text, formulae, diagrams, graphics and images, as well as voice; indeed, in its most advanced form, it can handle, multimedia messages, using all these modes of message content, to telephone communications and broadcasting, it has added data communications, telex, telefacsimile, and more recently Teletex (a sophisticated form of communicating word-processing) videotext (the communication of information from computers to user- friendly displays).

But the potentialities of computer networking go farther still, because totally new applications of integrated information processing are emerging, that require both computing and telecommunications for their fulfillment. These include the whole realm of office automation that is now evolving rapidly, financial transaction services that are coming more and more to the public attention, electronic publishing, integrated information services, and a variety of ways in which geographically separated people will be able to communicate, exchange ideas, and interact with each other.

Thus computer networking has already established itself as a vitally important area of practical application, and will rapidly become much more important during the next few years. Not only will it perform many valuable functions in business and industry, but it will also be used increasingly widely by more and more members of the public.

Considering business sides, most business is done in developed countries through networks. Management networking are used for many purposes, some of these purposes are mentioned below.

1. Increasing company profitability, efficiency or effectiveness.
2. Improving customer service.
3. Achieving business and personal targets.
4. Preparing for future personal advancement .

Other purposes of implementing network for normal users include:

1. Implementation of administrative and financial database.
2. Staff access to company records.
3. Automation of letter, report or specification writing.
4. E-mail for staff.
5. Staff scheduling.
6. General information automation (including library, plans, graphics and images).
7. Learning or training aids (interactive software).
8. Computer skills training rooms (word processing, publishing, CADD, spreadsheets, databases).

Networking is based on some very uncomplicated principles. Three common sense philosophies underpin the concept of networking and they can be summed up as follows:

1. Relationship building i.e. personally connecting with others.
2. Relationship maintenance i.e. timely reconnecting and communicating.
3. Information sharing i.e. adding value to the relationship.

1.2 User Requirements

If computer networking is to become a widely used and well-integrated set of techniques, for large groups of people, whether executives, managers, professionals office workers, or citizens, one of the first requirements that it must fulfill is user friendliness.

In other words, it should positively invite the user to come and try it; no longer should it put up a barrier, and convey a feeling of inaccessibility, together with a uneasy sense that it can be practiced only by a few "esoteric wizards".

That this is a real challenge is evident not only from the very genuine technical not to mention human, political and social, difficulties of computer networking those problems tend to be very much harder than those of computing alone and telecommunications alone, It also requires considerable, if not great, advances over the low degree of user friendliness all too often present in many areas of "ordinary" telecommunications and "ordinary" computing. Which of us will not have come across the exasperating difficulties, under too many circumstances, of trying to make even commonplace telephone calls? Which computer user will not have experienced the ham-handed ways in which manuals of even highly popular computer systems quite often do not explain sufficiently clearly accurately what the user should do in certain types of situation? Worse still, they sometimes forget to mention these contingencies at all.

Thus one vitally important ingredient of user-friendliness is that the basic concepts of computer networking be explained as simply as possible, given the circumstances, in as easy and clear a language as possible, with all necessary technical terms properly defined where they arise, preferably with illustrative examples.

A closely related ingredient is that, for any specific function of computer networking that a user needs to carry out with a specific system, either on the job or as a member of the public, there should be a clear but comprehensive statement of the whole sequence of steps that need to be carried out. This statement should neither be too long and complicated which makes the user unsatisfied nor too short and concise to be unreadable, and it should include at least one example.

Another important requirement of a computer networking system or service is that it should provide its users with a range of functions and facilities that are appropriate for their needs. Thus, for a business system, there is a fairly well defined group of requirements for office automation and integrated information systems, even now, and these will doubtless develop further. For private users, there are not only requirements for simple individual or household functions, such as electronic mail and financial transactions, but also the need to contribute to information, education and entertainment. In assessing this sort of requirement, it should be realized that it is not static, but rather that it is evolving rapidly. Not only that; users may well increasingly demand their own say in the new facilities to be offered by the computer-information-communication networks of the future.

1.3 User interfaces

A typical user interface to a computer network, whether it is a terminal or a more colaborate work station, includes both a display and a keyboard; these are two of the most basic means of communication between the network and its users. Displays are usually obtained through specially designed visual display units (VDUs), not unlike television sets that can present a combination of text and graphics information, usually in black and white or black and green, although colour displays are also available. A display not only conveys the most important messages from the computer network and computing systems themselves; it can also show messages from other users and generally provides an immediate visual record of information input through its associated keyboard. Keyboards allow users to input text of their own choice to the network and to the system. This next includes their instructions to the system, messages that they want to send to other users, information that they wish to file, and programs that they decide to run. Typically, terminals have a keyboard that is alphanumeric, containing keys for digits, letters of the alphabet (now usually though not always in both upper and lower case), punctuation marks, and special symbols. Many terminals also have cursor control keys, controlling the movement of the cursor, a small symbol, appearing on a display, which indicates where the next keyboard input will be shown.

Visual information for users is often provided also by printers that capture on paper what may otherwise be fleeting images on display screens. Output on paper is usually an extra advantage, as printed page images typically contain much more text than VDU displays and are often more readable. Some printers can also provide graphics output, occasionally in colour too, and plotters are available which can provide high quality graphical forms on paper.

Voice channels are being provided on some data networks and communication networks. This is sometimes done by integrating telephone communications with data communications and text communications. In addition, special devices for voice input and voice output are becoming available; for example, the former can allow the recognition of up to several dozen different spoken sounds, while the latter implement various forms of computer speech.

1.3.1 Examples of User Interface

1.3.1.1 Acme Windows

It is arrayed in columns and are used more dynamically than in an environment like.Acme windows have two parts: a tag holding a single line of text, above a body holding zero or more lines ,The body typically contains an image of a file being edited or the editable output of a program, analogous Acme has no single notion of 'current directory'. Instead, every command, file name, action, and so on is interpreted or executed in the directory named by the tag of the window containing the command. For example, the string `mammals` in a window labeled `/lib/` or `/lib/insects` will be interpreted as the file name.

1.3.1.2 X Windows

The system frequently creates them automatically and the user can order a new one with a single mouse button click. The initial placement of a new window is determined automatically, but the user may move an existing window anywhere by clicking or dragging a layout box in the upper left corner of the window.

1.3.1.3 Macintosh

The middle and right buttons are used, somewhat like the left button, to 'sweep' text, but the indicated text is treated in a way that depends on the text's location—*context*—as well as its content. This context, based on the directory of the file containing the text, is a central component of Acme's style of interaction.

1.4 Network Applications

Perhaps the single most important application of computer networking, and certainly one of the most rapidly expanding, is its use for integrated office and business systems, in conjunction with other forms of office automation. These systems can operate at a local level, using LANs to carry out various office functions at a single site; they can also operate on behalf of organizations with several premises, using WANs to link their different LANs. Functions that can be supported by these systems include word processing and text processing, electronic mail and message services, and management information systems, as well as ordinary computing and data processing.

In addition, computer networks can support various financial transaction services for companies and other organizations. Similar transaction services for citizens are less well advanced; but electronic banking, credit card, shopping and travel booking facilities are beginning to operate or are being planned.

Computer networks have already been able to improve greatly the operation of data bases, information retrieval facilities, and other information services. Data bases made available in this way include those provided by private and public videotex systems, to provide useful information on a wide variety of subjects, and very large specialist data bases accessed by "ordinary" online retrieval services. One of the most significant developments is the provision of "third party data base" facilities, which allow a network's own data bases to be supplemented by a large number of other computer data bases, which can be linked to it through network "gateways."

There are many other actual and potential applications of networking, covering most aspects of human life. These include the use of network for: distributed computing and data processing, telesoftware, education and training, electronic publishing, message services, computer conferencing, community information services, and home information systems.

1.5 Network Structures

The first basic principle of network structure is that a computer network can be subdivided into several computing and information processing devices, all linked together by a common communications subsystem, sometimes called the *subne.* The essential requirement is that, regardless of the diversity of the different devices, the subnet should nevertheless be able to establish effective communication and interchange of information between all of them.

The subnet may itself have a variety of configurations.These configurations include: the *star* network, where there is one central node, usually attached to a central computer; the *loop* or *ring* network, where all the nodes are strung round a single loop of wire or cable; the *bus* network, where all the nodes occur in linear sequence, from one end of a long line, the "bus" to the other; the mesh 'network, where there is a rich interconnection between many different nodes, indeed sometimes between all pairs of nodes; the radio network, where there is no configuration of specific paths between different nodes, but where they are all in effective "wireless" radio contact with each other.

There are also important distinctions to be made between local area network (LAN) configurations, sited within a compact geographical area, and wide area network (WAN) configurations, the distances between whose nodes range from less than a mile to thousands of miles.

Usually, the LANS have ring or bus configurations, while the WANS are usually meshes; star networks, though now less usual than before, can appear as either LANS or WANS.

The other basic principle of network architecture is that different types of network may be interconnected with each other, in such a may that any pair of nodes, accessible to each other via a path through several consecutive interconnected networks, can communicate effectively with each other. More specifically, neighboring networks are joined to each other by "gateways," which can be viewed either as single nodes, belonging to two or more networks, or as a configuration of neighboring, mutually linked, nodes,belong Terminals different networks that are being brought together there.

1.6 Equipment Linked to Networks

In the early days of computer networks, there were usually only two kinds of device attached to them, computers and terminals. The situation is very different now, when just about every information or communications device under the sun can belinked to a network.

User interfaces that can be connected to networks, include "ordinary" terminals that are usually VDUs, graphics terminals and plotters, that specialize in more or less sophisticated types of visual display, word processors, a wide variety of printers, voice input devices and voice output devices. Sometimes, clusters of devices are joined to a. network through a multiplexer, rather than each of these devices being connected directly.

Any sort of computer can now be interfaced with a network, ranging from the smallest microcomputer, through personal computers and minicomputers, to mainframes and distributed array processors.

Rapidly becoming more important, with the onset of office automation and other technological advances, are the multi-purpose work stations and integrated work stations, which combine several functions in a single device in a more or less unified way.

Typically, devices of this sort can act as terminals, displays, word processors, computers, and data communicators, all at once.

Another very important class of devices that can be attached to networks are the file stores and mass memories. These can hold from about a hundred thousand to many million characters of information. They range from floppy disks and "hard" magnetic disks of various shapes and sizes, through magentic tapes and video storage, to the optical information stores, which can already hold very large amounts of information very compactly and promise to have very much better performance within only a few years from now.

1.7 Data Transmission

Originally, computer networks relied entirely on telephone lines for the long distance communication of information across them. Today, with the advance of technology, the range of possible data transmission media is quite considerable. High bandwidth transmission lines and coaxial cables are providing channels for data transmission, over both short and long distances, that are far more ample and reliable than those available on telephone lines. Recently, fibre optics cables have begun to develop steadily, and will soon be able to provide local and even medium distance channels of even higher capacity, at costs that are still reasonable.

"Wireless" data communications of several types are coming into their own. Radio waves have not only provided the basis for more or less local "packet radio" services; they are also used in satellite communications systems, and information, "piggybacked" on broadcast television systems, is used in several teletext systems. Recently, advances in electro-optical technology have allowed the development of communications system using laser light.

1.8 Network Architectures and Their Protocols

The architecture of a computer network precisely defines the functions that the network and its components should perform, and the ways in which the network should be organised.

The main purpose of the architecture is to ensure that the design and user requirements of the network are met as far as possible, by arranging that the different parts of the network cooperate effectively and by enabling the network system as a whole to evolve according to its aims. In effect, the architecture is an "organization chart" of the network. It is defined in terms of the relations between the different parts of the network; these relations include both protocols and interfaces.

Network protocols are essential, both for providing the basic rules of formatting and handling information that is to be communicated from one part of a network to another, and for helping to overcame problems of mutual "incompatibility" between different devices that are connected to a network, or, more generally, a system of interconnected networks. Very closely related to the design of protocols is the formulation of suitably agreed network standards, which is actively promoted by various national and international standards bodies, together with the specialist working parties that they have set up to consider and discuss new protocols.

In accordance with the principles of network architecture, the functions of a network, and therefore the protocols that implement them, operate at different layers and levels, of which seven are now generally recognized. At the lowest level, there is the physical intercommunication system, then, going progressively higher, there are link protocols, covering data transmission over links, and network protocols, primarily concerned with communication and routing across networks. At a middle level, there are transport protocols, looking after reliable end-to-end transmission of a message from one device, over a network or sequence of networks, to another.

Higher still are the session protocols, responsible for handling connections between individual processes in computers and devices that communicate with each other, and presentation protocols, performing generally useful transformations and conversions of the data to be exchanged. At the top level, there are application Protocols, covering a range of user- oriented functions, such as transfer of information between data bases, distributed computing, and electronic mail and message services.

1.9 LAN Performances

I determined the topic of my project as a PERFORMANCE INVESTIGATION OF THE ETHERNET LAN. Communication with computers using networks is very popular in our world now. The speed up of the communication is another important point.

According to these things, the importance of a LAN segment also increases. We have to know how computers work together in the Ethernet LAN? And how their performance changes? My aim is to investigate the behavior of a network system consisting of a set of workstations and a file server in the environment of the Departmental LAN. All of these things would be explained in the main part of the report.

1.10 Network Technologies

Computer networking brings together various technologies concerned with electronics, telecommunications, computing and information processing.

A considerable variety of network architecture has been devised. The "star" network, linking a cluster of terminals to a central computer, has been used in both LANs, and WANs. However, LANs usually have either a "ring" configuration, with all their devices attached to nodes in a loop of cable, or a "bus" configuration, where their devices are attached to nodes on a single line of cable. WANs tend to use fairly general configurations of nodes, including peripheral (device) nodes and switching nodes. WANs are linked to neighboring LANs and WANs by special gateways, which are nodes or node-pairs that act as interfaces between them.

Although the earliest computer networks used very simple terminals, to provide users with access to local or remote computers, more sophisticated, "intelligent,"forms of network terminals were later developed, to be used predominantly by business users and information providers, and having additional capabilities. A whole range of devices that can be attached to networks is now available for users, including: graphics displays, sometimes in colour, word processors, a variety of printers and computers, even voice input and output devices. Multi-purpose terminals, with a considerable range of facilities, including local computing, word processing and data storage, are beginning to appear on the market. Memory devices and tile stores that can be attached include: floppy disk drives, "hard" *(fixed)* magnetic disks, magnetic tapes, video storage and, very recently, optical storage.

Transmission technologies, used in telecommunications, include: telephone lines, high bandwidth transmission lines, coaxial cables, fibre optics, lasers, radio waves, and satellite communications.

Standardization is becoming increasingly necessary, to avoid a chaotic proliferation of mutually incompatible network systems; on the whole, it seems to have been making good progress during recent years. Standard protocols are being developed, that provide operating rules for the interchange of information and for communication, both for data networks themselves and for the wide variety of applications that these networks support.

Technologies and techniques are also required for network control and for the improvement of network performance. To be fully effective, network control, to keep the network in full working order as continuously as possible, requires network measurements and regular monitoring of network performance. The performance and other characteristics of network behavior can be investigated both empirically and with the aid of mathematical models of networks and network traffic and protocols. Predictions of network performance can then be made by means of a judicious combination of analytical and simulation techniques applied to the models. Network design can be improved by devising appropriate performance and operating criteria, using models and empirical data to predict the performance of propose modifications or new features, and learning from practical experience of networks.

Network Technology is the first thing that I should explain in this work. Networking is the sharing of information and services. Networking is possible when individuals or groups have information or abilities that they wish to share with others. Computer networking provides the communication tools to allow computers to share information and abilities. Today's computer networks include computers and computer operating system associated with all of the computing models. A typical network includes mainframes, personal computers and a variety of other computers and communications devices. Computer networks fit the general definition of networking since they share electronic data and computing services.

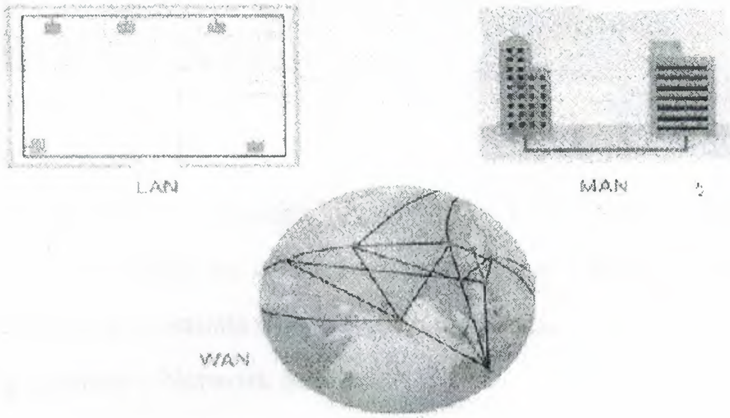

Figure 1.1: Computer Network Classifications

Computer networks are often classified by size, distance covered or structure. Even though the distinctions are rapidly fading the following network classifications are commonly used.

1. Local area network (LAN).
2. Metropolitan area network (MAN).
3. Wide area network (WAN).

1.10.1 Local Area Network

A local area network (LAN) refers to a combination of computer hardware and transmission media that is relatively small. LANs normally do not exceed tens of kilometers in size and tend to use only one type of transmission medium. In addition, a LAN is normally entirely contained within a building or campus.

1.10.2 Metropolitan Area Network

A metropolitan area network (MAN) is a network that larger than a LAN. It is called metropolitan since it normally covers the area of a city (a few tens to about one hundred kilometers). Different hardware and transmission media are often used in MANs because they must efficiently cover these distances or because they do not require complete access to locations between the network sites.

1.10.3 Wide Area Network

A wide area network (WAN) includes all networks larger than a MAN does. WANs interconnect LANs which may be at opposite sides of a country or located around the world. All network analogy consists of three basic elements.

- Something to share – Network Services.
- A pathway for contacting others – Transmission Media.
- Rules for communication – Protocols.

1.10.4 Peer-to-peer Networks

Peer-to-peer networks allow any entity to both request and provide network services. Peer-to-peer network software is designed so those peers perform the same or similar functions for each other.

1.11 Network Services

Network services are capabilities that networked computers share. Network services are provided by numerous combinations of computer hardware and software depending upon the task, network services requires data, input/output resources, and processing power to accomplish their goals. In the computer industry, a distinction is often made between the following three types of service providers and requestors:

- Servers.
- Clients.
- Peers.

These entities are differentiated by what they are allowed to do on the network:

1. Servers are only allowed to provide services.
2. Clients are only allowed to request services from others.
3. Peers may do both concurrently.

Often, these names are mistakenly used to label a specific computer. Theoretically, a single computer can simultaneously act as a client, a server, and a peer depending on what software is running. Software determines the computer's limitations and therefore its role as a client, server, or peer. However, most computers only fill one role at a time so this distinction is often overlooked. Computer networks are often classified as one of the following two types:

- Peer-to-peer
- Server-centric

1.12 Server-Centric Networks

Server-centric networks involve strictly defined roles. By definition, a server-centric network places restrictions upon which entity may make requests or service them. Currently, the most popular personal computer is server-centric.

1.13 Transmission Media

Transmission media is the pathway network entities use to contact each other. Computer transmission media includes cable and wireless technologies that allow networked devices to connect one other. Transmission media cannot guarantee that other network devices will understand a message. It can, however, guarantee a message delivery path.

1.14 Protocols

Protocols are the rules required helping entities communicate or understand each other. A protocol can be one rule or complete set of rules and standards that allow different devices to hold conversations.

1.15 Cable Media

In LAN environment, people generally use coaxial unshielded twisted pair and fiber optic cables. The speed of the propagation delay in cable is related with the kind of communication method and modulation frequency. And these rules affect the length of cables. There are some procedures about the cables:

- Thick coaxial 50 Ohm (standard Ethernet 10 Mbps) : 500 m
- Thin coaxial 50 Ohm (thin Ethernet, CDDI, Token ring, ATM): 185 m
- Fiber Optic, Multi-mode (Ethernet, Token Ring, FDDI, and ATM) : 100 m
- Fiber Optic, Multi-mode (Fast Ethernet): 400 m
- Fiber Optic, Multi-mode (Full duplex, Fast Ethernet): 2 km

Fiber optic cables should be used commonly because of the distance and also between the buildings, and also it should be used because of the risk of thunder. In case of thunder, because of the electricity on copper cables, all the Ethernet cards and transceivers can be burned.Cable media are wires or fibers that conduct electricity or light. The following cables are:

- Twisted pair cable
- Coaxial cable
- Fiber optic cable

1.15.1 Twisted Pair Cable

Twisted pair is a common scheme for using copper wire as telecommunication cable. Because copper is such a good conductor of electrons, copper wires do not constrain electromagnetic signals well. When two copper wires conduct electric signals in close proximity, a certain amount of electromagnetic interference occurs. The type of interference is called crosstalk. In addition, because of the electromagnetic range used, TP transmits and receivers unwanted signals from other sources. Twisting the copper wires reduces crosstalk and signal emission. Each intertwined strand conducts a current whose emitted waves are cancelled out by the other wire's emissions.

Figure 1.15.1: Twisted Pair Cable

Twisted pairs are formed by two insulated 22 to 26 gauge copper wires that are twisted about each other. When one or more twisted pairs are combined within a common jacket, they form a twisted pair cable. The two types of **TP** cables are:

- Unshielded
- Shielded

1.15.2 Unshielded Twisted Pair Cable

Unshielded twisted pair (UTP) cable is composed of a set of twisted pairs with a simple plastic encasement. We are probably already familiar with UTP since it is commonly used in telephone systems. It is widely available and has been largely standardized.

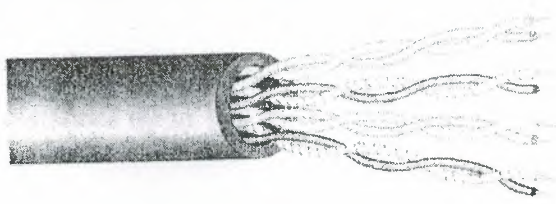

Figure 1.15.2.1: Unshielded Twisted Pair Cable

Due to its voice telecommunication heritage, computer network UTP is often installed in the same manner as most telephone installations. A user device contains a port, which accommodates a modular RJ-45 (4-pair), or RJ-1 1 (2-pair) telephone connector.These connectors are attached to both ends of a patch cable. One end of the patch cable is inserted into the device's port and the opposite end is inserted into a wall jack.

The wall jack connects the UTP cable drop (the drop is a length of cable that extends to the user's location) to one side of a 66 block (also referred to as punch-down block).

The opposite side of the punch-down block is wired to a patch panel. This patch panel provides multiple ports, which use patch cables to connect to other user devices or to the connectivity devices. While RJ-45 connectors are currently the most common, Multiplan RS-232 and RS-449 connections can also be used.

Cost Factor: The cost of UTP is extremely low compared to other transmission media. It continues to be mass-produced for telecommunications and has become a popular computer network medium. Some network integrators use existing spare wires from telephone cables to significantly reduce the already low implementation costs. However, this practice is not recommended if the existing UTP cable is lower than Category 3, if the cable drops exceed 100 meters, or if significant crosstalk is already present between the voice wires.

Ease of Installation: UTP installation equipment is also inexpensive, easy to use, and widely available. Installation techniques are so simple that the cable can be adequately installed with very little training. Because voice telecommunication connection techniques have optimized for easy moves, ads, and changes, UTP is easily managed and reconfigured.

Capacity: Using current and emerging technologies, UTP may support data transfer rates from 1 to 100 Mbps at distances up to 100 m. Ten Mbps is the most common transmission rate in use today.

Attenuation: All copper wires suffer from rapid attenuation when used as a communications medium. UTP is no exception. Current technology restricts the effective range of UTP to hundreds of meters.

Immunity from EMI: The copper cable used in UTP is very susceptible to EMI. Although the twists greatly reduce crosstalk, a certain amount of interference exists between pairs of wires. Also, signals on the pairs are easily influenced by outside emitters of electromagnetic wave (like electric motors). External devices can also be used to intercept signals that are emitted from the pairs, breaching the security of a network.

1.15.3 Shielded Twisted Pair Cable

Today, most TP cable is unshielded, but some forms of shielded twisted pair (STP) still exist. STP is insulated cable which includes bundled pairs wrapped in a foil shielding. Various transmission media specifications from Apple Computer and IBM use STP cable. For example, IBM employs a type specification for different qualities and configurations of STP. Networks conforming to each vendor's specifications have their own unique installation requirements, including connectors and length restrictions.

Cost: Bulk STP is moderately expensive. It currently costs more than UTP but less expensive than thick coaxial or fiber optic cable.

Ease of installation: STP is more difficult to install than UTP. Like coaxial cable, an electric ground, created by special connectors and installation techniques, must be provided for the shield. However, STP is more difficult to install than coaxial cable if we use standardized and reconfigured cables, this simplifies installation.

Capacity: Theoretically, with the reduction of outside interference, STP can use higher frequencies and more bandwidth-efficient signaling techniques. It is capable of greater transmission speeds, up to 500 Mbps at 100 m, but has not been widely implemented at data rates higher than 155 Mbps. The most common transmission rate in use today is 16 Mbps.

Attenuation. STP suffers from attenuation at a rate similar to UTP .Current technology also restricts the effective range of STP to hundreds of meters.

Immunity from EMI. The biggest difference between UTP and STP is the reduction of interference and EMI emissions provided by STP's shielding. However, STP still suffers from relatively low immunity from interference.

1.15.4 Coaxial Cable

Coaxial cable is made of two conductors that share a common axis, hence the name. Typically, the center of the cable is a relatively stiff solid copper wire or stranded wire encased in insulating plastic foam. The foam is surrounded by the second conductor, a wire mesh tube (some include conductive foil wrap), which serves as a shield from EMI. A tough, insulating plastic tube forms the cover of the cable.

Several coaxial cable standards are in common use for computer networking. The most common types meet one of the following ohms and size standards (ohms are a measurement of the cable's resistance to direct or alternating electric currents):

- 50 ohm RG-8 and RG-11 (used in thick Ethernet specifications)
- 50 ohm RG-58 (used in thin Ethernet specifications)
- 75 ohm RG-59 (used for cable TV)
- 93 ohm RG-62 (used for ARCnet specifications)

Coaxial cable is most installed from device to device. At each user location a connector is attached to provide a use r interface. The interface may be attached by cutting the cable and installing a T-connector to both ends or by applying special clamp-like devices called taps. Taps are mechanical devices that use conducting teeth to penetrate the insulation and attach directly to the wire conductor.

To maintain the correct electrical properties of wire, the cable must be grounded and terminated. An electrical ground completes the required electrical circuit, while a terminator dampens signal reflections.

Cost: The cost of coaxial cable increases with the diameter and composition of the conductors. The cost of thin coaxial cable is relatively low (less than STP or Category 5 UTP). Thick coaxial cable is moderately expensive (more than STP or Category 5 UTP). Both are more expensive than category 3 UTP (all comparisons are made in reference to bulk cable with connectors)

Ease of Installation: The initial installation of coaxial cable is relatively simple. However, current installation techniques usually use a single strand of cable, which may become difficult to manage and reconfigure. Local drops may be connected to the base cable to make device connections easier.

Capacity: Using current technologies, coax supports data transfer rates between twisted pair and fiber optic cable. Although the typical data rate in use today is 10 Mbps. Much greater data rates are available. However, these higher rates are only infrequently used in computer networking. It is important to note that coaxial cable's bandwidth potential increases with the diameter of the inner conductor.

Attenuation: As a copper wire media, coaxial cable suffers from high attenuation, but at a much lower rate than either variety of twisted pair. Using current LAN technology, the effective range of coaxial cable is the low thousand of meters.

Immunity from EMI: While copper wire generally is a poor resistor to EMI, the shielding provided by coaxial cable greatly reduces its effects.

1.15.5 Fiber Optic Cable

Fiber optic cable is made of a light conducting glass or plastic core surrounded by more glass, called cladding, and though outer sheath. The center core provides the light path or waveguide while the cladding is composed of varying layers of reflective glass. The glass cladding is designed to refract light back into the core. Each core and cladding strand is surrounded by a tight or loose sheath.

In tight configurations, the strand is completely surrounded by the outer plastic sheath. Loose configurations use liquid gel or other material between the strand and the protective sheath. In both cases the sheath provides the necessary cable strength to protect the fiber from excessive temperature changes, bending, stretching or breaking.

Fiber optic cable can be composed of a single jacketed strand, but often multiple strands are bundled together in the center of a cable. Some fiber optic cable will also provide an additional metallic, Kevlar, or fiberglass wire to increase cable strength, but this is not required.

Optical fibers are much smaller and more lightweight than copper wires. Therefore, large fiber optic cables can carry more conductors than similar sized copper cables, which make them ideal for limited space environments.

Optical fibers may be multi-mode or single-mode in nature. Single-mode fiber has been optimized to allow only one light path while multi-mode fiber allows various paths. The physical characteristics of the multi-mode fiber's layer control the speed of the various modes. By bending the light at different rates, the signal's parts arrive simultaneously and appear to be a single pulse to the receiver. Single-mode fiber has a higher capacity but costs more to produce and use than multi-mode fiber.

Types of fiber optic cable are differentiated by mode, composition (glass or plastic) and core / cladding size. The size and purity of the core determines the amount of light that can be transmitted. Common types of fiber optic cables include:

1. 8.3 micron core / 125 micron cladding single-mode.
2. 62.5 micron core / 125 micron cladding single-mode.
3. 50 micron core / 125 micron cladding single-mode.
4. 100 micron core / 140 micron cladding single-mode.

A common LAN installation of fiber optic cable starts at a used device that contains two optical interfaces (incoming and outgoing). The interface is connected directly to fiber cables, which have been terminated which biconic or other mechanical connectors. With Multiple lengths of fiber optic cable, when necessary, are spliced together using electric fusion, a chemical epoxy process, or mechanical connectors.

Optical interface devices convert computer signals and light pulses to and from the optical fibers. The light pulses are generated by light emitting diodes (LEDs) on multi-mode fiber or injection laser diodes (ILDs) on single-mode fiber. They are reconverted to electric signals by P intrinsic N diodes or avalanche photodiodes.

Cost: Historically, bulk fiber and connectors have been relatively expensive compared to copper wire, but these costs are falling rapidly. However the extreme cost of installation far outpaces the cost of materials.

Ease of Installation: The nature of fiber optic cable poses installation problems. Every fiber junction, splice, or connection must be made with extreme care to ensure that the light path is unobstructed. Installers must also be careful not to excessively stretch or bend the fiber.

Capacity: Optical fibers support extremely high bandwidths because they are limited by the high-frequency photon properties of light rather than by lower-frequency properties of electrical systems. Current technologies allow data rates from 100 Mbps to over 2 Gbps. The data rate of a given fiber optic system is depended upon cables the fiber composition (glass or plastic), the mode, and the wavelength (and therefore the frequency) of the light transmistted. The most common LAN installations include glass multi-mode fiber and 850-nm wavelength LEDs. This configuration can sustain a transmission rate of 100 Mbps at distances of approximately 20 km.

Attenuation: Fiber optic cables have extremely low attenuation rates. The amount of attenuation varies depending upon the operating wavelength, but effective ranges are usually measured in kilometers. Therefore, fiber optic cable attenuates much less than any copper wire transmission medium.

Immunity from EMI: Due to the use of the light spectrum, fiber optic cables do not leak signals and are immune to electromagnetic interference and eavesdropping. Also, the light spectrum does not require electrical grounds so fiber optic cables do not suffer from potential shifts to electrical ground nor do they produce sparks. These characteristics make fiber ideal for hazardous, high voltage, or eavesdropping-sensitive environments.

1.16 Transmission Media Connections

When building a network, we need a number of hardware devices to connect each computer to a media segment. These devices include:

1. Transmission media connectors.
2. Network interface boards.
3. Modems.

We also connect multiple separate segments of transmission media to form one large network. For this purpose, we use the following network devices:

1. Repeaters.
2. Hubs.
3. Bridges.
4. Multiplexers.

Figure 1.16.1: T-Connector and RJ-45

In LAN technologies the speed and performance is very important, so we can generally examine topologies, kinds of cables, reaching the environment and some kinds of equipment to connect cables.

1.17 Topologies

In LAN technology we can use many kinds of topologies and in large LAN environments the numbers of topologies are more than the others. Some of these topologies are:

1.17.1 Bus

Generally Ethernet connections that are done by coaxial cables use this topology. In bus topology, use of cable is less and it is very easy to spread this cable and also this kind of construction is very useful for constructing a backbone. Backbone construction is very useful to reach far places by network connections and people choose this kind of topology because with this topology lot of people can connect to this network easily. But there is a disadvantage of this topology. It is not tolerable to the errors in the network. In case of a small failure in coaxial cables, all the users are affected with this failure and an error in a PC's Ethernet card can affect other PC's more efficiently. So it can not be a good choice.

1.17.2 Star

In star technology, connections between computers are done by using boxes called hub (Appendices 2, Figure 1). In star technology, use of cables is very common and also it is expensive than the other technologies. But in case of failures in connections only one user is affected because of this failure. Other users are not affected, so other people do their work properly. Hubs are connected in two ways that one of them is cascade connection and the other is stack connection. It is the most useful connection for switched environments.

1.17.3 Distributed Star, Tree

Increasing number of hub connections makes people use two or more (must be less than four) hubs. For Ethernet, the number of used hubs can be four. For fast Ethernet it can be two.

1.17.4 Ring (token ring and FDDI/CDDI):

It is useful to make backbone connections and with using double ring system it is also tolerable to errors. It is usually used in factories network connections and in campuses.

1.18 Wireless

In movable areas and in decorative places wireless connections can be used. It is used easily in buildings and also in far fields. Infrared and laser technologies are used in these connections. But there is a disadvantage of these connections. Connection distances are not very far and its price is very expensive.

1.19 Communication Environment and Network Cards

In communication environments, it is very popular to use Ethernet in these days. It works in 10 Mbps. In past, people were using Token Ring cards, because it was very tolerable to errors. With star topology and use of UTP cables, there have become similar tolerances to Ethernet standards tool. And it has become popular.

In higher speed standards, 100 Mbps FDDI, CDDI, 100 Base TX, TX Fast Ethernet, 100 Base VG, 155 Mbps ATM cards are used. FDDI and CDDI technologies are very standard and they are very tolerable to errors. But these cards are very expensive about 1500$ - 2000$. ATM is a new developing technology and its developments continue till now. These cards are very expensive too. 100 Base TX and 100 Base VG standard is similar to token ring special technique. So the numbers of firms producing this standard are less. And there are some connection problems between these standards. Some main tests showed us that the performance of 100 Base TX cards is better.

1.19.1 Active Cable Connection Equipment

People make nearest LAN groups to enlarge LAN environments and to increase the number of users and then these LAN groups connect each other. Repeater, bridge, switch router are the useful equipment help to connect LAN groups.

1.19.2 Repeater

Repeaters are the first part of the (OSI) Open system Interconnect equipment. In another view repeaters are not interested about the contents of the data it only increases the rage of the signal and transmits the other part more strongly ON a classic Ethernet repeater all ports are on the same cable. So in Ethernet repeater connections, data coming from all computers go to all other computers and endpoints.

Only one of the end points get the data and the others stop the data at the entrance of the connection. In repeater technology just one computer can connect the others. Other computers can not connect each other at the same time. Other people have to wait the end of this connection. Generally, hub concept is very similar to repeater concepts. A repeater that contains lots of ports can be named as hub a chassis that contains some repeater, switch, FDD concentrator bridge router; terminal server can be called as hub.

1.19.3 Bridge

Bridges is the equipment that works on data-link level. IN another view these equipment analyze the address part of the data (MAC address). They check the address if it already exists in the target. Bridge equipment really consists of two ports so it behaves like a bridge between two cables. Bridges have the capability of learning which address is where. They do that by reading some addresses in data and they write these addresses into schedules.

1.19.4 Switch

Switch system work like a bridge system. They work in data-link levels. This system is different in some ways from bridge system. It has more than two ports so it can connect more segments at the same time. Switch can understand easily by controlling the serial numbers on Ethernet cards written on a schedule.

On switch system, ports are isolated from each other. All the connections are broken of from each other, so if two computers are connected, first their lines should be connected on the switch. When the communication finishes, other computers can connect to each other. By this way, a group of two computers becomes a parallel network we can see this easily in. There are two ways to connect segments to each other.

Switches that use this method just read the beginning address of the data package and without waiting the end of data it easily makes connection between two lines

1.19.5 Store-And-Forward

By this method, switches take the all package data inside and check the addresses then they decide which lines to connect. At first glance, we can think that cut-through switches are more useful. But it is not like this. In the static interference atmospherics it does not check the Frame-Check sequence (FCS), so it uses the connection erroneous and uselessly.

If the users want to connect just one server, there is no need to use switch. If the line going through the server is busy, then other people who want to connect to the same server have to wait.

1.19.6 FDDI / CDDI Uplinks

The difficulties in connecting to a server can be surpassed by connecting the server system to an uplink or backbone line. In Figure 5 we can see how to connect a 100 Mbps FDDI backbone. IN this position, lots of data coming from 10 Mbps can reach to the target by using 100 Mbps FDDI / CDDI lines very quickly. So other coming databases do not have to wait more.

There is no need for an extra equipment or extra number of ports on FDDI / CDDI line. It is enough just to attach one Dual attached FDDI / CDDI line. It is enough just to attach one Dual attached FDDI/ CDDI network card. In addition to this fact, FDDI / CDDI technology has known standards and it's very tolerable to the errors. But, in another way, FDDI / CDDI cards are more expensive than the other cards.

1.19.7 FDDI / CDDI Concentrator

If the number of PC's and the number of switches are too many, switches can be connected each other by Dual Attached Station (DAS) or from a FDDI / CDDI Concentrator, they can be connected as Single Attached Station (SAS).

1.19.8 FDDI / CDDI Switch

If we change the middle 100 Mbps FDDI / CDDI backbone with a FDDI / CDDI switch (which can make parallel backbones), we can get a higher performance connection environment.

1.19.10 ATM Uplink

In connections, 155 Mps ATM technologies can be used instead of 10 Mbps Ethernet switch uplink connection. ATM is a new technology, so maybe it can not be found suitable card and program for it.

For connecting lots of PC's into a server, we have to increase the number of ATM ports. Lots of switch systems consist of one uplink port. With ATM, we can reach the higher performance, 155 Mbps and 622 Mbps and in the future 2.4 Gbps, but network cards are expensive.

1.19.11 Fast Ethernet (100BaseTX) Uplink

In connections, 100 Base TX technologies can be used instead of 100 Mbps Ethernet switch uplink connection. Fast Ethernet cards are very cheap. Wasting of time is less in Fast Ethernet switch system. Before using this technology, all system must be checked. To connect too many server systems, it is enough to increase number of 100 Base TX. By this way, performance will increase. In other way, a Fast Hub (100 Mbps speed) can be connected to uplink line. But, by using Fast Hub, if the numbers of users increase, then we can have some difficulties.

1.19.12 Fast Ethernet Hub / Repeater

Fast Ethernet "repeater" system is a technology that it can bring 100 Mbps speed to "desktop" computer in a cheaper way and that it gains popularity rapidly. In present days, more graphics, colors using multi-media is popular, so taking 100 Mbps-band breadths to the last user is necessary. There are some restrictions. First, the cable must be category-5 UTP or STP, or it should be fibre.

Only two repeater systems can connect each other and the distance between two computers must not be higher than 205 meters.

1.19.13 Fast Ethernet Switch

We can enlarge our network by using too fast Ethernet repeaters. And it increases performance Switch takes place between these Fast Ethernet repeaters Connections on UTP cables must not be over 100 meters and connections that are on fibre cables must not be over 400 meters. Full-duplex connections on fibre cables must not be over 2 kilometers.

1.20 ATM Switch

ATM is the most popular technology in these days. ATM switch systems can make connections 155,622 Mbps speed. ATM switches are preferable, because they are aptness to multi-media (data, sound, and frame)

Ethernet package length	: 1,500 bytes
FDDI package length	: 4,500 bytes
Token Ring package length	: 16,000 bytes

In these lengths of package' communication delay time called "latency" is very much. In ATM switch, the length of the cell is 53 byte and the delay time between packages' beginning and packages' end is very less. So the quality of sound and vision is very well.

To use ATM, every computer has to have an ATM card. ATM technologies are very expensive, so people generally prefer Ethernet Token-Ring Fast Ethernet that contains

ATM uplink. In this position, ATM switch acts as a switch. So the users working on tips are out of sound and vision quality.

1.20.1 Router

Router systems are the systems that take place on third step of OSI. This equipment has the capability to understand the network protocol and network addresses. For this reason, Router systems can permit Router managers to control the system. In fast LAN environments, traffic optimization can be not very important but, for LAN safety and Wide Area Network connections, traffic optimization is very important. To control the traffic optimization, Virtual LAN technology is used. To inspect broadcast traffic connections between VLAN, Router systems are very useful.

1.21 Performance Investigation of the Department LAN

1.21.1 The Statement of the Problem

Communication with computers using networks is very popular in our world now. Also the speed of the communication is another important point so the importance of a LAN segment also increases. In this section it is explained that how computers work together in a Departmental LAN? And how their performance changes, due to the varying number of clients to a file server in this environment?

Firstly, it is supposed that every workstation runs a client program, which reads data from a file server that is the same for all clients. The client program is also the same for all workstations. We are interested in the response time for a client to read a number of blocks from Turing file server. This time will depend on the current number of active clients, which access concurrently the Turing file server. The aim of my work was to experimentally find the dependence of the client response time on the current number of active clients with some parameters of the access in my Turing server account. These parameters include the block size, the number of blocks to read from the file server, the idle time of a client between two successive accesses to the file server Turing. It is supposed that, in every run all the active clients start accessing the Turing file server exactly at the same time and finish after reading the given number of blocks from the file server Turing. In these read operations I used 10 files, with the same size but with the different file names.

1.21.2 Network Control and Performance

In order that a computer network may be adequately controlled, it is important to obtain a good idea of its actual performance. This may be achieved empirically, partly by making network measurements at various times and places, partly by more systematic monitoring of important parts of the network. Various sorts of control, including bow control and congestion control, help to keep the information traffic across the network in reasonable order, and prevent it from getting out of hand.

Idea of network performance, it is necessary to supplement empirical studies of network behavior by theoretical studies. These use mathematical models to throw light on the performance of part or whole of a net- work, and the resulting calculations on the models are carried out, using judicious combination of analytical and simulation methods. In this way, using also the results of empirical studies, more or less accurate predictions can be made of how a network will behave if certain changes are made to its physical characteristics, to its configuration, and to its traffic. Such predictions can be used both to improve, lhe day-to-day operation of a network and to make valuable suggestions for the improvement of its architectural design d f the protocols that it uses.

1.21.3 Workstation

A type of computer used for engineering applications (CAD/CAM), desktop publishing, software development, and other types of applications that require a moderate amount of computing power and relatively high quality graphics capabilities.

Workstations generally come with a large, high-resolution graphics screen, at least 64 MB (megabytes) of RAM, built-in network support, and a graphical user interface. Most workstations also have a mass storage device such as a disk drive, but a special type of workstation, called a diskless workstation, comes without a disk drive. The most common operating systems for workstations are UNIX and Windows NT.

In terms of computing power, workstations lie between personal computers and minicomputers, although the line is fuzzy on both ends. High-end personal computers are equivalent to low-end workstations. And high-end workstations are equivalent to minicomputers.

Like personal computers, most workstations are single-user computers. However, workstations are typically linked together to form a local-area network, although they can also be used as stand-alone systems.

1.22 Network Computers (NC)

A few years ago, it seemed that the world was ready for the age of a marvelous new cretion called the network computer (NC). A network computer is a computer-like device with a very fast processor and no CD, hard drive, or floppy drive. When the user logs on from the network computer. If the user starts an application, a Java-based application downloads to the network computer possibly with some server-based processing for certain tasks.

The user could save any files to a well-protected and fault-tolerant storage device on the server or elsewhere on the network. When the user turns off the network computer, the complete configuration disappears from memory. But it returns when the user logs on again. In fact, another user could log on to the same network computer and receive a completely different configuration. The new user could even receive a completely different operating system. Meanwhile, the users' files are kept safe with the ISP. All software is managed, configured, and updated from the server, and the network computer is so simple that it isn't likely to break. If it does break, you just buy a new one because it is so inexpensive. In any ease, you don't have to disassemble, reassemble, or configure the network computer because there is nothing to configure.

This amazing vision captivated market watchers when it was first proposed, but so far the revolution of the network computer hasn't happened. One reason why the network computer hasn't caught on is the fact that hardware prices have fallen so sharply. You can now buy a complete computer for what a network computer cost a few years ago. Another reason may be that, although lava development is proceeding very rapidly, we haven't yet reached the point where a complete Java-based operating system is viable for the mainstream. However, the network computer is only one of several thin-client solutions that have made their way to the market. You'll learn about another thin-client option (the terminal client) in the next section.

1.23 Network Functionality

A wide range of local area network (LAN) systems has now been developed, well over 50 of these systems are now available commercially, and more of them are being introduced almost every month. This chapter surveys a representative selection of them, without making any claim to be comprehensive.

The rest of the section describes some important examples of the nearly 200 commercially available LAN systems, which are surveyed briefly in Thurber (1982a) and more fully in Thurber (1982b), with periodical updates of information in Thurber (1982c). It staffs with ring-based and Ethernet-like systems, then proceeds to broadband systems, and after that to some integrated LAN systems, providing a very wide range of services for business offices and other organizations; finally, it considers briefly some miscellaneous LANs.

It should be noted that the claims made by the manufacturers and vendors of these and other network systems and products should be evaluated very carefully by prospective users, in relation to the specific needs and existing equipment and methods of their organizations, in relation to the estimated costs and previous operating experience of the systems and products, and in relation to the likely evolution of computing and information technologies during the next few years.

Chapter II: LAN Structures

2.1 Review and Classification of Local Area Network Technologies

A considerable variety of lan technologies are available, these technologies have been surveyed and compared by cotton(1979),for example ,who gives over thirty literature references. They can be classified in four ways:

1. By *configuration* or *topology,* for example: star, ring, bus, mesh (fully connected), as shown in Figure 1.2.
2. By *medium,* the method by which data are transported within the network, for example: twisted pair wires, cable, radio; digital base band signaling, using only one frequency; digital broadband systems, using several frequencies shared by a channel; modulated signaling.
3. By *sharing technique,* the way in which many users are allocated bandwidth in the network, for example: dedicated (non-shared), time or frequency division multiplexing, statistical multiplexing, contention.
4. By *user services* and *protocols,* this can be provided by intelligent devices, attached to the network or its interfaces, regardless of the internal network transmission techniques.

Any sharing technique can be used with any technology (Clark et al, 1978), who describes a number of interesting combinations. Some of the arguments for and against some of the most common variants of some of the technologies are now summarized; for further details, see Cotton (1979).

Local non-switched networks, using dedicated lines: are most suitable where only relatively few users need interconnection or where most users need to communicate only with one other user, as in the original time-sharing computer systems.

Local circuit switching: can be achieved, either through a public telephone exchange or through a branch exchange on the user's premises. Any user can be dialled cQnveniently, and costs are fairly small for low speeds, up to about 1200 bits/second.

Local message-switched: networks tend to have reliability problems, especially when based on central switches, but can be attractive.

Local packet-switched networks: are very feasible, though sometimes more expensive than other approaches. Most of the LAN systems, described in this chapter, indeed in this book, are in this category.

Ring networks: very efficiently share available transmission bandwidth, and can be implemented at high data rates with very simple transmission facilities; despite initial misgivings about their possible unreliability, they have turned out to be very reliable

2.2 LAN Integration

A LAN is a high-speed data network(meduim allows a high bit transmission rate) that covers a relatively small geographic area(ex within a building). It typically connects personal computers, workstations, printers, servers, and other devices, LANs are connected by permanent cables that allow rapid data transfer. A LAN will generally comprise several personal computers, shared peripheral devices such as printers and scanners, and a central file server with high capacity disk storage. A network server stores data and programs that can be used and shared by any computer linked to the LAN (subject to users having access rights), Most LANs, as mentioned above. Node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data.

2.3 LAN Operation

A LAN requires special operating system software to allow the various devices connected to the LAN to communicate with each other.As Lan follows the rule of server-client networkes,the server must have the power to operate strongly within the network.This strongness and effictevness of the server lies in the precense of a strong operating system ex:- macintosh ,windows 2000 may be also used.

Local area network (LAN) could use any topology for connection in figure 1.1 bus topology is used to connect the pc's together ,and the information and data are stored in the file system(FS) ,see figure, these file servers contain the software necessary to implement a wide area networks(WAN) through connections of LAN'S together ,taking into attention that any cooruptions in the FS may cause a troubleshoot(problems) in connecting LAN'S.

2.4 LAN Hardware Structure

Network Cards. A wide variety of network cards—officially called Network Interface Cards and nicknamed NICs—is available. Most do at least an adequate job. If you're a novice networker, the primary things to look for are:

- **Connection Jack:** Be sure the NIC's jack matches the type of cable you're using. If you're using 10BaseT cable, for instance, the NIC you buy should have an RJ-45 compatible connector.

- **Plug and Play Compatibility:** This feature allows Windows 95/98 to automatically configure the card, saving you a lot of time in the process.

- **Interrupt Addresses:** Interrupts on any machine are at a premium, so you'll want to determine which ones the NIC has available. Generally, the more you pay, the more latitude you'll have. ISA-bus cards are usually fast enough for a 10BaseT network; if you're running 100BaseT you'll probably want to go with PCI-bus card for speed. If you've only got one interrupt left and must add two cards, use two PCI-bus network cards; part of the PCI spec is that cards can share interrupt.

2.5 Devices Connected to LAN

Devices commonly used in LANs include repeaters, hubs, LAN extenders, bridges, LAN switches, and routers. Respective to the OSI model, these devices operate at the following layers:

- **OSI Layer 1 (physical):** Hubs, repeaters (hubs are considered to be multiport repeaters)
- **OSI Layer 2 (data link):** Bridges, switches
- **OSI Layer 3 (network):** Routers

2.6 Intelligent Hubs

A *hub* is a physical layer device that connects multiple user stations, each via a dedicated cable. Electrical interconnections are established inside the hub. Hubs are used to create a physical star network.while maintaining the logical bus or ring configuration of the LAN. In some respects, a hub functions as a multiport repeater.

Hubs operate at the physical layer (Layer 1) of the OSI model. A hub is used to connect devices so that they are on one shared LAN, as shown in Figure 2-9. Because only two devices can be directly connected with LAN cables, a hub is needed to interconnect two or more devices on a single LAN. The cable termination points are the hub and the LAN device (host).

Intelligent hubs contain logic circuits that will shut down a port if the traffic originating from that port indicates that bad, or malformed, frames are the rule rather than the exception.

2.7 Repeaters

A *repeater* is a physical layer device used to interconnect the media segments of an extended network. A repeater essentially enables a series of cable segments to be treated as a single cable. Repeaters receive signals from one network segment and amplify, retime, and retransmit those signals to another network segment.

These actions prevent signal deterioration caused by long cable lengths and large numbers of connected devices. Repeaters are incapable of performing complex filtering and other traffic processing. In addition, all electrical signals, including electrical disturbances and other errors, are repeated and amplified.

The total number of repeaters and network segments that can be connected is limited due to timing and other issues. Figure illustrates a repeater connecting two network segments.

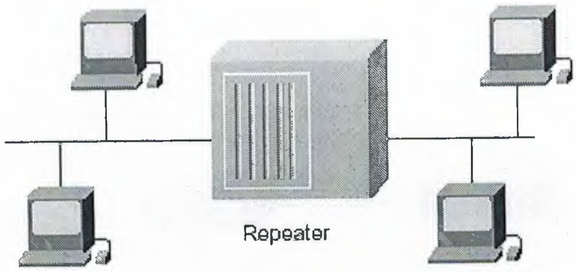

Figure 2.7.1: A Repeater Connects Two Network Segments

2.8 Bridges

This section focuses on transparent bridges, which can also be referred to as learning or Ethernet bridges. Bridges have a physical layer (Layer 1), but are said to operate at the data link layer (Layer 2) of the OSI model. Bridges forward data frames based on the destination MAC address.

Bridges also forward frames based on frame header information. Bridges create multiple collision domains and are generally deployed to provide more useable bandwidth. Bridges don't stop broadcast traffic; they forward broadcast traffic out every port of each bridge device. Each port on a bridge has a separate bandwidth (collision) domain, but all ports are on the same broadcast domain.

Bridges were also deployed in complex environments, which is where broadcast storms became such a problem. Routers were added to the complex bridged environments to control broadcasts. VLANs were devised when switches were deployed in enterprise environments andbrought back the old problem of broadcast storms.

Bridges, like repeaters, do not modify traffic. Unlike repeaters, bridges can originate traffic in the form of spanning tree bridge protocol data units (BPDUs). Bridges maintain a MAC address table, sometimes referred to as a *content addressable memory (CAM)* or bridging table, which maintains the following information:

• MAC Addresses.

• Port Assignment.

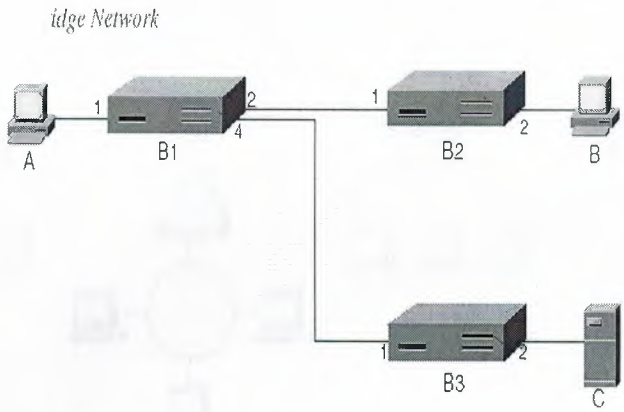

Figure 2.8.1: A Bridged Network

The original all-ports broadcast of A's first frame to B ensures that B3 knows how to send to frames to A. An attempt by C to communicate with B results in B3 broadcasting the frame on all ports (except number 2), so the frame reaches B1 on port 4. While B1 forwards this frame to B2, it also learns what to do with frames destined for C.

2.9 LAN Extender

A *LAN extender* is a remote-access multilayer switch that connects to a host router. LAN extenders forward traffic from all the standard network layer protocols (such as IP, IPX, and AppleTalk) and filter traffic based on the MAC address or network layer protocol type. LAN extenders scale well because the host router filters out unwanted broadcasts and multicasts. However, LAN extenders are not capable of segmenting traffic or creating security firewalls. Figure below illustrates multiple LAN extenders connected to the host router through a WAN.

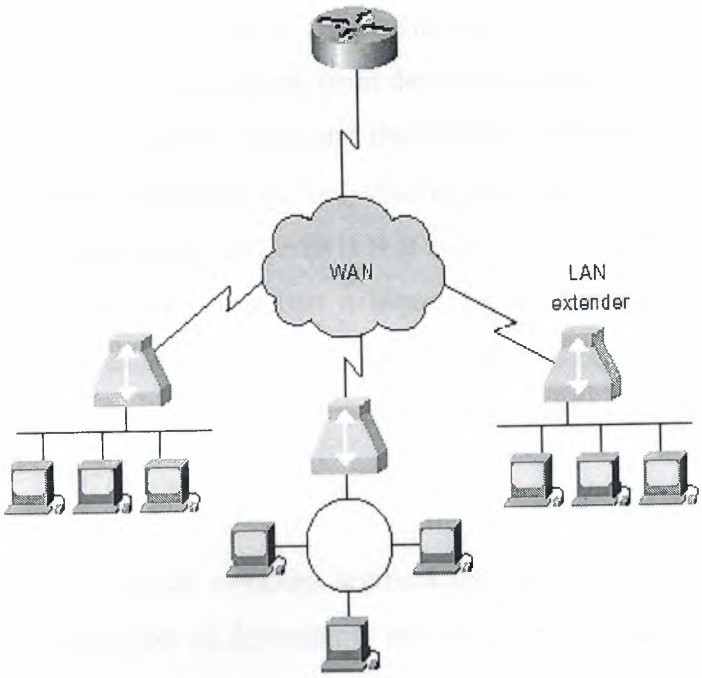

Figure 2.9.1: Multiple LAN Extenders Can Connect to the Host Router Through a WAN

2.10 LAN Media-Access Methods(MAC)

Media contention occurs when two or more network devices have data to send at the same time. Because multiple devices cannot talk on the network simultaneously, some type of method must be used to allow one device access to the network media at a time. This is done in two main ways: carrier sense multiple access collision detect (CSMA/CD) and token passing.

In networks using *CSMA/CD* technology such as Ethernet, network devices contend for the network media. When a device has data to send, it first listens to see if any other device is currently using the network. If not, it starts sending its data. After finishing its transmission, it listens again to see if a collision occurred. A collision occurs when two devices send data simultaneously. When a collision happens, each device waits a random length of time before resending its data. In most cases, a collision will not occur again between the two devices. Because of this type of network contention, the busier a network becomes, the more collisions occur. This is why performance of Ethernet degrades rapidly as the number of devices on a single network increases.

In *token-passing* networks such as Token Ring and FDDI, a special network packet called a token is passed around the network from device to device. When a device has data to send, it must wait until it has the token and then sends its data. When the data transmission is complete, the token is released so that other devices may use the network media. The main advantage of token-passing networks is that they are deterministic. In other words, it is easy to calculate the maximum time that will pass before a device has the opportunity to send data. This explains the popularity of token-passing networks in some real-time environments such as factories, where machinery must be capable of communicating at a determinable interval.

For CSMA/CD networks, switches segment the network into multiple collision domains. This reduces the number of devices per network segment that must contend for the media. By creating smaller collision domains, the performance of a network can be increased significantly without requiring addressing changes.

2.11 LAN Topologies

The physical layout of the LAN is called Network Topology. Common LAN topologies are Ring, Bus, Tree, and Star.LAN topologies define the manner in which network devices are organized,and their architecture in which they are implemented in real life. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star.

1.11.1 Bus Topology

A bus topology is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three most widely used LAN implementations, Ethernet/IEEE 802.3 networks.

2.11.2 Star Topology

A star topology is a LAN architecture in which the endpoints on a network are connected to a common central hub, or switch, by dedicated links. Logical bus and ring topologies are often implemented physically in a star topology, which is illustrated in Figure below.

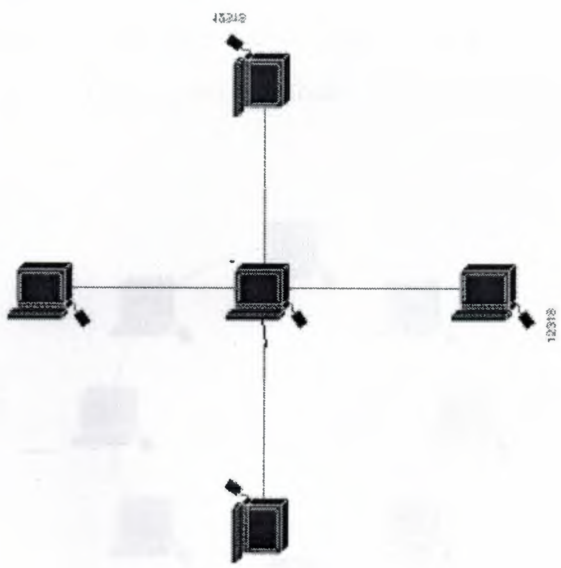

Figure 2.11.2.1: A Star Connection

All stations are attached by cable to a central point, usually a wiring hub or other device operating in a similar function. Several different cable types can be used for this point-to-point link, such as shielded twisted-pair (STP), unshielded twisted-pair (UTP), and fiber-optic cabling. Wireless media can also be used for communications links.

The advantage of the star topology is that no cable segment is a single point of failure impacting the entire network. This allows for better management of the LAN. If one of the cables develops a problem, only that LAN-attached station is affected; all other stations remain operational.

2.11.3 Ring Topology

A ring topology is a LAN architecture that consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop. Both Token Ring/IEEE 802.5 and FDDI networks implement a ring topology. Figure depicts a logical ring topology,in ring topology one of the pc's connected on the network transmittes a signal, this signal circles through the closed loop and is then copied by the intended destination network node. The signal is then absorbed by the original station that transmitted the signal.

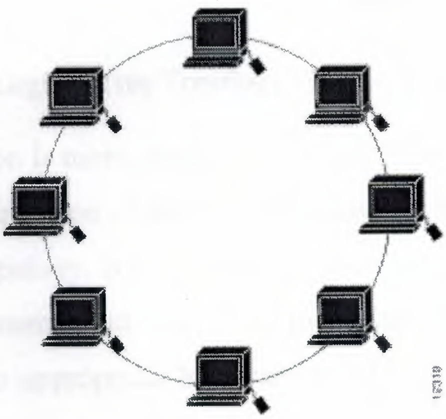

Figure 2.11.3.1: Some Networks Implement a Logical Ring Topology.

Token Ring (IEEE 802.5) best represents a ring topology. Although the physical cabling is considered to be a star topology, Token Ring is a ring in logical topology, as demonstrated by the following figures. Although physical topology is a physical layer attribute, the media access method used at the data link layer determines the logical topology. Token Ring defines a logical ring and contention, as Ethernet defines a logical bus. Even when attached to a hub, when one Ethernet device transmits, everyone hears the transmission, just as though on a bus.

2.11.4 Tree Topology

A tree topology is a LAN architecture that is identical to the bus topology, except that branches with multiple nodes are possible in this case. Figure below llustrates a logical tree topology.

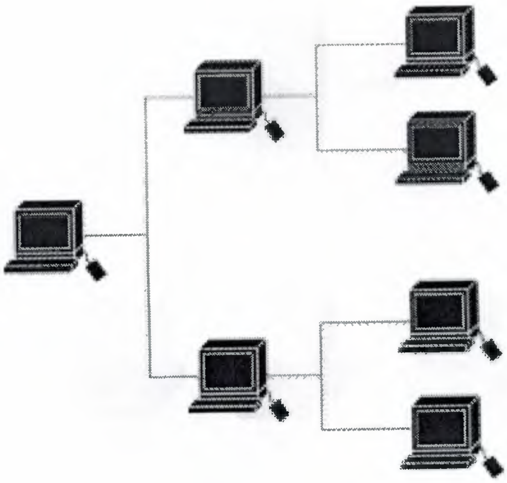

Figure 2.11.4.1: A Logical Tree Topology Can Contain Multiple Nodes.

The Tree Topology connection is more complicated, since it has branches that are identical to Bus Topologies. The transmission of data by any station in the network is controlled by the Central Hub in a Star Topology. Bus Topology is used to connect the equipment in the PLC local area network presented in this paper.In a Bus Topology network, all PLC stations are attached through appropriate hardware interface cards called iaIsolated Link Couplersld. There are no switches or repeaters. Therefore, fewer hardware components are required for Bus Topology local area networks.

2.12 LAN Transmission Methods

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single packet is sent to one or more nodes. The three classification of local area network transmission methods,are explained below,showing how data is transfered from one machine into another.

2.12.1 Unicast

With unicast transmissions, a single packet is sent from the source to a destination on a network. The source-node addresses the packet by using the network address of the destination node. The packet is then forwarded to the destination network and the network passes the packet to its final destination. Figure below is an example of a unicast network.

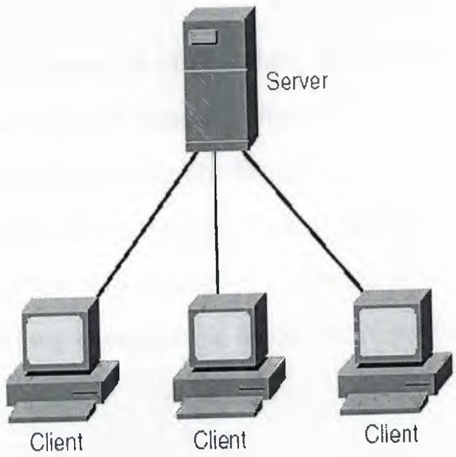

Figure 2.12.1.1: A Unicast Network

2.12.2 Multicast

With a multicast transmission, a single data packet is copied and forwarded to a specific subset of nodes on the network. The source node addresses the packet by using a multicast address. For example, the TCP/IP suite uses 224.0.0.0 to 239.255.255.255. The packet is then sent to the network, which makes copies of the packet and sends a copy to each segment with a node that is part of the multicast address. Figure below is an example of a multicast network.

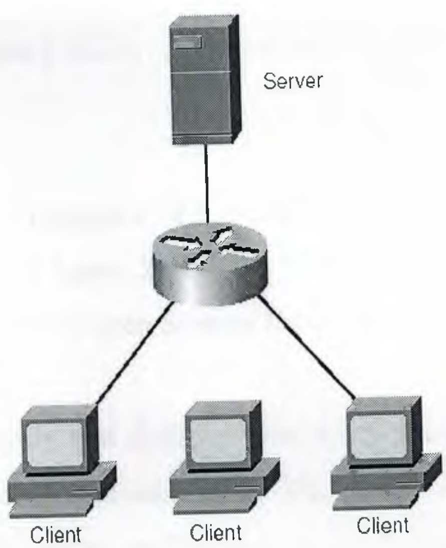

Figure 2.12.2.1: A Multicast Network

2.12.3 Broadcast

A *broadcast transmission* consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address.Broadcasts are found in LAN environments. Broadcasts do not traverse a WAN unless the Layer 3 edge-routing device is configured with a helper address (or the like) to direct these broadcasts to a specified network address. This Layer 3 routing device acts as an interface between the local-area network (LAN) and the wide-area network (WAN).

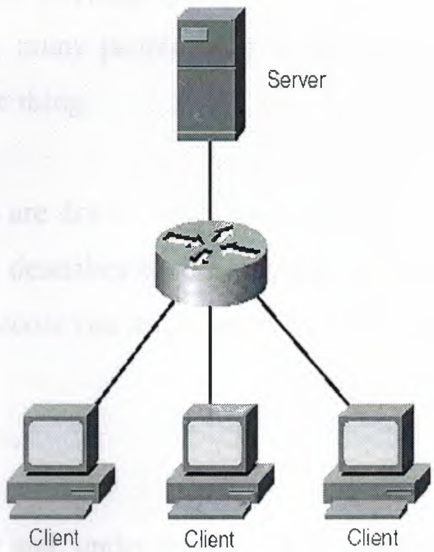

Figure 2.12.3.1: A Broadcast Network

2.13 The OSI Model

If you spend much time in the company of network technicians you will eventually hear them say something like “That’s Layer 2 only” or “That’s our new Layer 4 switch”. The technicians are referring to the OSI (Open System Interconnection) Refer-ence Model.

This model defines seven Layers that describe how applications run-ning upon network-aware devices may communicate with each other. The model is generic and applies to all network types, not just TCP/IP, and all media types, not just Ethernet.

It is for this reason that any network tech-nician will glibly throw around the term"Layer 4" and expect to be understood.

It should be noted, however, that most protocols in day-to-day use work on a slightly modified layer system. TCP/IP, for example, uses a 6- rather than a 7-layer model. Nevertheless, in order to ease the exchange of ideas, even those who only ever use TCP/IP will refer to the 7-layer model when discussing networking principles with peers from a different networking background.

Confusingly, the OSI was a working group within the ISO (International Standards Organisation) and, therefore, many people refer to the model as the ISO 7-layer model. They are referring to the same thing.

Traditionally, layer diagrams are drawn with Layer 1 at the bottom and Layer 7 at the top. The remainder of this article describes each layer, start-ing from the bottom, and explains some of the devices and protocols you might expect to find in your data centre operating at this layer.

2.13.1 Layer 1

Layer 1 is the Physical Layer and, under the OSI Model, defines the physical and electrical characteristics of the network. The NIC cards in your PC and the interfaces on your routers all run at this level since, eventually, they have to pass strings of ones and zeros down the wire.

2.13.2 Layer 2

Layer 2 is known as the Data Link Layer. It defines the access strategy for sharing the physical medium, including data link and media access issues. Protocols such as PPP, SLIP and HDLC live here. On an Ethernet, of course, access is Governed by a device's MAC address, the six-byte number that is unique to each NIC. Devices which depend on this level include bridges and switches, which learn which segment's devices are on by learning the MAC addresses of devices attached to various ports.

This is how bridges are eventually able to segment off a large network, only forwarding packets between ports if two devices on separate segments need to communicate. Switches quickly learn a topology map of the network, and can thus switch packets between communicating devices very quickly. It is for this reason that mi-grating a device between different switch ports can cause the device to lose network connectivity for a while, until the switch, or bridge, re-ARPs.

2.13.3 Layer 3

Layer 3 is the Network Layer, providing a means for communicating open systems to establish, maintain and terminate network connections.

The IP protocol lives at this layer, and so do some routing protocols. All the routers in your network are operating at this layer.

2.13.4 Layer 4

Layer 4 is the Transport Layer, and is where TCP lives. The standard says that "The Transport Layer relieves the Session Layer [see Layer 5] of the burden of ensuring data reliability and integrity". It is for this reason that people are becoming very excited about the new Layer 4 switching technology.

2.13.5 Layer 5

Layer 5 is the Session Layer. It provides for two communicating presentation entities to exchange data with each other. The Session Layer is very important in the E-commerce field since, once a user starts buying items and filling their "shopping basket" on a Web server, it is very important that they are not load-balanced across different servers in a server pool.

This is why, clever as Layer 4 switching is, these devices still operate software to look further up the layer model. They are required to under-stand when a session is taking place, and not to interfere with it.

2.13.6 Layer 6

Layer 6 is the Presentation Layer. This is where application data is either packed or unpacked, ready for use by the running application. Protocol conversions, encryption/ decryption and graphics expansion all takes place here.

2.13.7 Layer 7

Finally, Layer 7 is the Application Layer. This is where you find your end-user and end-application protocols, such as telnet, ftp, and mail (pop3 and smtp).

LAYER7	Application
LAYER6	Presentation
LAYER5	Session
LAYER4	Transport
LAYER3	Network
LAYER2	Data Link
LAYER1	Physical

Figure 2.13.7.1: The 7-Layer OSI Model

2.14 Localnet

Sytek Inc. in the USA, whose British agent is Network Technology Limited, has developed local Net as a low cost, high performance LAN, based on a synergistic combination of analog, digital and data communications technologies (network Technology, 1982; Thurber, 1982a; Biba, 1981a and 1981b). It uses industry Standard broadband cable television distribution facilities, allowing over 20,000 users to be supported simultaneously. A wide variety of user equipments can be interconnected, with end-to-end data security, flexibility of configuration, and ease of installation.

System 20. The first group of products in the Local Net family. Was designed to meet the immediate and near-future needs of a variety of users, in government, finance, industry, education, etc. It is implemented as a modular growth-oriented family of network products. It's claimed to be cost-effective, reliable, and compatible with a broad range of devices and interface standards. As it occupies only a relatively small part of the cable bandwidth, its services can coexist with other broadband services, such as high-speed data links, voice and video.

Local net extensions and improvements provide substantially increased capabilities for network interconnection, user device interfaces, security and privacy, and network management and control.

2.15 Advantages and Disadvantages of LAN

Some of the advantages and disadvantages of LAN networks, are listed below:

2.16 Local Area Network (LAN) Support Specialist I 4826(3291)

Employees at this level are microcomputer-literate, entry-level specialists in networking. They learn network operations and perform simpler systems duties (such as data gathering, monitoring operations, or network documentation) as well as install equipment and software. They work under direct supervision of a designated technical supervisor.

- Provides basic network support services to users (such as, the installation of personal computers.
- Workstations onto the network, configuring network interface cards and client software, and installing and supporting network printers and queues).
- Executes well-defined backup, recovery, and security procedures to ensure continual availability of the network
- Provides assistance to network users in resolving routine network problems.
- Maintains and reviews logs and audit trails to detect intrusion, virus, or other problems and begins corrective action.

Chapter III: ATM

3.1 ATM General

Asynchronous Transfer Mode or ATM is a network transfer technique capable of supporting a wide variety multimedia application with diverse service and performance requirements. It supports traffic bandwidths ranging from a few kilobytes per second to several hundred megabits per second. And traffic types ranging from continuous, fixed-rate traffic to highly bursty traffic.

ATM is a form of packet-switching technology. That is, ATM networks transmit their information in small, fixed-length packets called "cells", each of which contains 48 octets (or bytes) of data and 5 octets of header information. The small, fixed cell size was chosen to facilitate the rapid processing of packets in hardware and to minimize the amount of the time required to fill a single packet.

ATM is also connection-oriented. In other words, a virtual connection must be established before a "call" can take place, where a call is defined as the transfer of information between two or more end points.

Another important characteristic of ATM is that its network functions are typically implemented in hardware. With the introduction of high speed fiber optic transmission lines, the communication bottleneck has shifted from the communication links to the processing at switching nodes and at terminal equipment. Hardware implementation is necessary to overcome this bottleneck, because it minimizes the cell processing overhead, thereby allowing the network to match link rates on the order of Gbit/s

Finally, as its name indicates, ATM is asynchronous. Time is slotted into cell-sized intervals, and slots are assigned to calls in an asynchronous, demand-based manner. Because slots are allocated to calls on demand ATM can easily accommodate traffic whose bit rate fluctuates over time. Moreover, in ATM also gains bandwidth efficiency by being able to statistically multiplex bursty traffic sources.

Since bursty traffic does not require continuous allocation of the bandwidth at its peak rate, statistical multiplexing allows a large number of bursty sources to share the network's bandwidth. Since its birth in the mid-1980s, ATM has been fortified but a number of robust standards and realized by a significant number of network equipment manufacturers.

International standards-making bodies such as the ITU and independent consortia like the ATM forum have developed a significant body of standards and implementation agreements for ATM

3.2 ATM Standards

The telecommunication standardization sector of the ITU, the international standards agency commissioned by the United Nations for the global standardization of telecommunication, has developed standards for ATM networks. Other standards bodies and consortia have also contributed to the development of ATM.

3.3 Protocol Reference Model

The purpose of the protocol reference model is to clarify the functions that ATM networks perform by grouping them into a set of interrelated, function-specific layers and planes. The reference model consists of a user plane, a control plane and a management plane. Within the user and control planes is a hierarchical set of layers.

The user plane defines a set of functions for the transfer of user information between communication end-points; the control plane defines the control functions such as call establishment, call maintenance, and call release; and the management plane defines the operations necessary to control information flow between planes and layers, and to maintain accurate and fault –tolerant network operation.

Within the user and control planes, there are three layers: the physical layer, the ATM layer, and the ATM adaptation layer (ALL).

The physical layer performs primarily bit level functions, the ATM layer is primarily responsible for the switching of ATM cells, and the ATM adaptation layer is responsible for the conversion of higher layer protocol frames into ATM cells. The functions that the physical, ATM, and adaptation layers perform are described in more detail in the following.

3.4 Physical layer

The physical layer is divided into two sub layers: the physical medium sub layer and the transmission converge sub layer

Physical Medium (PM) Sub layer: The physical medium sub layer performs medium-dependent functions. For example, it provides bit transmission capabilities including bit alignment, line coding and electrical/optical conversion. The PM sub layer is also responsible for bit timing, i.e.., the insertion and extraction of bit timing information. The PM sub layer currently supports two types of interface: optical and electrical

Transmission Convergence (TC) Sub **layer:** Above the physical medium sub layer is the transmission converge sub layer, which is primarily responsible for the framing of data transported over the physical medium. The ITU_T recommendation specifies two options for TC sub layer transmission frame structure cell-based and synchronous digital hierarchy (SDH). In the cell-based case, cells are transported continuously without any regular frame structure. Under SDH, cells are carried in a special frame structure based on the North American SONET (Synchronous Optical Network) protocol.

Regardless of which transmission frame structure is used, the TC sub layer is responsible for the following four functions: Cell rate decoupling, header error control, cell delineation, and transmission frame adaptation. Cell rate decoupling is the insertion of idle cells at the sending side to adapt the ATM cell stream's rate to the rate of the transmission path.

Header error control is the insertion of an 8-bit CRC polynomial in the ATM cell header to protect the contents of the ATM cell header. Cell delineation is the detection of cell boundaries. Transmission frame adaptation is the encapsulation of departing cells into an appropriate framing structure

3.5 ATM Layer

The ATM layer lies a top the physical layer and specifies the functions required for the switching and flow control of ATM cells. There are two interfaces in an ATM network: The user network interface (UNI) between the ATM end point and the ATM switch, and the network-network interface (NNI) between two ATM switches.

Although a 48 octet cell payload is used at both interfaces, the 5 octet cell header differs slightly at these interfaces. The VCI and VPI field share identifier values for virtual channel (VC) and virtual path (VP), respectively. A virtual channel connects two ATM communication end-points. A virtual path connects two ATM devices, which can be switches or end-points, and several virtual channels may be multiplexed onto the same virtual path.

The 2-bit PT field identifies whether the cell payload contains data or control information. The CLP bit is used by the user for explicit indication of cell loss priority. If the value of the CLP is 1 the cell is subjected to discarding in case of congestion. The HEC field is an 8 bit CRC polynomial that protects the contents of the cell header.

The GFC field, which appears only at the UNI, is used to assist the customer premises network in controlling the traffic flow for different qualities of service. At the time of writing the exact procedures for use of this field have not been agreed upon.

3.6 ATM Layer Functions

The primary function of the ATM layer is VPI/VCI translation. As ATM cells arrive at ATM switches, the VPI and VCI values contained in their headers are examined by the switch to determine which out port should be used to forward the cell. In the process, the switch translates the cell's original VPI and VCI values into new outgoing VPI and VCI values, which are used in turn by the next ATM switch to send the cell toward its intended destination.

The table used to perform this translation is initialized during the establishment. An ATM switch may either be a VP switch, in which case it only translates the VPI values contained in cell headers, or it may be a VP/VC switch, in which case it translates the incoming VCI value into an outgoing VPI/VCI pair.

Since VPI and VCI values do not represent a unique end-to-end virtual connection. They can be reused at different switches through the network. This is important, because the VPI and VCI fields are limited in length and would be quickly exhausted if they were used simply as destination address.

The ATM layer supports two types of virtual connections: switched virtual connection (SVC) and permanent, or semi permanent, virtual connections (PVC). Switched virtual connections are established and torn down dynamically by an ATM signaling procedure. That is they only exist for the duration of a single call.

Permanent virtual connections, on the other hand, are established by network administrators and continue to exist as long as the administrator leaves them up, even if they are not used to transmit data. Other important functions of the ATM layer include cell multiplexing and demultiplexing, cell header creation and extraction, and generic flow control.

Cell multiplexing is the merging of cells from several calls onto a single transmission path, cell header creation is the attachment of a 5- octet cell header to each 48 octet block of user payload, and generic flow control is used at the UNI to or event short-term overload conditions from occurring within the network

3.7 ATM Layer Service Categories

The ATM Forum and ITU-T have defined several distinct service categories at ATM layer. The categories defined by the ATM forum include constant bit rate (CBR), real-time variable bit rate (VBR-rt), non real-time variable bit rate (VBR-nrt), available bit rate (ABR), and unspecific bit rate (UBR). ITU-T defines four service categories, namely, deterministic bit rate (DBR), statistical bit rate (SBR), available bit rate (ABR) and ATM block transfer (ABT). The first of the three ITU-T service categories correspond roughly to the ATM Forum's CBR, VBR and ABR classifications, respectively.

The fourth service category, ABT, is solely defined by ITU-T and is intended for bursty data application. The UBR category defined but the ATM Forum is for calls that request no quality of service guarantees at all. The constant bit rate CBR (or deterministic bit rate DBR) service category provides a very strict QoS guaranty. It is targeted at real-time applications, such as voice and raw video, which mandate severe restrictions on delay, delay variance (jitter) and cell loss rate.

The only traffic description required by the CBR service are the peak cell rate and the cell delay variation tolerance. A fixed amount of bandwidth, determined primarily by the call's peak cell rate, is reserved for each CBR connection. The real-time variable bit rate VBR-rt (or statistical bit rate SBR) service category is intended for real time bursty application, which also require strict QoS guarantees.

The primary difference CBR and VBR-rt is in the traffic descriptions they use. The VBR-rt service requires the specification of the sustained cell rate and bursty tolerance in addition to the peak cell rate and the cell delay variation tolerance. The ATM Forum also defines a non-real-time VBR-nrt service category, in which cell delay variance is not guaranteed. The available bit rate (ABR) service category is defined to exploit the network's unutilized bandwidth. It is intended for non-real time data application in which the source is amenable to enforced adjustment of its transmission rate.

A minimum cell rate is reserved for the ABR connection and therefore guaranteed by the network. When the network has unutilized bandwidth, ABR sources are allowed to increase their cell rates up to an allowed cell rate (ACR), a value which is periodically updated by the ABR flow control mechanism. The value of ACR always falls between the minimum and the peak cell rate for the connection and is determined by the network

The ATM forum defines another service category for non-real-time application called the unspecified bit rate (UBR) service category. UBR service is entirely best effort; the call is provided with no QoS guarantees. .The ITU-T also defines an additional service category for non-real-time data applications. The ATM block transfer (ABT) service category is intended for the transmission option (ABT/IT), the block of data is sent at the same time as the reservation request.

If bandwidth is not available for transporting block, then it is simply discarded; and the source must retransmit it. In the ABT service with delayed transmission (ABT/DT); the source waits for a confirmation from the network that enough bandwitdh is available before transmitting the block of than data. In both cases, the network temporarily resource reserves bandwidth according to the peak. Cell rate for each block. Immediately after transporting the block, the network releases the reserved bandwidth

3.8 ATM Adaptation Layer

The ATM adaptation layer (AAL), which resides a top ATM layer, is responsible for mapping the requirements of higher layer protocols onto the ATM network. It operates in ATM devices at the edge of the ATM network and is totally up sent in ATM switches. The adaptation layer is divided into two sub layers: The convergence sub layer (CS), which performs error detection and handling, timing and clock recovery and the segmentation and reassembly (SAR) sub layer, which performs segmentation of convergence sub layer protocol data units (PDUs) into ATM cell-sized SAR sub layer service data units data units (SDUs) and vice versa in order to support different service requirements, the ITU-T proposed for AAL-specific services classes.

Note that while these ALL service classes are similar in many ways to the ATM layer service categories defined in the pervious section, they are not the same; each exists at a different layer of the protocol reference model, and each requires a different set of functions. ALL service class A corresponds to constant bit rate (CBR), services with a timing the relation required between source and destination. The connection mode is connection – oriented. CBR audio and video belong to this class. Class B corresponds to variable bit rate (VBR) services. This class also requires timing between sources and destination, and its mode is connection-oriented. VBR audio and video are examples of class B services. Class C also corresponds to VBR connection –oriented services but the timing between source and destination needs not be related. Class C includes connection-oriented data transfer such as X.25, signaling and future high speed data services. Class D corresponds to connectionless services. Connectionless data services such as those supported by LANs and WANs are examples of class D services.

Four AAL types, each with a unique SAR supplier and CS sub layer, are defined to support the four service classes. ALL type 1 supports constant bit rate services (Class A), and AAL type 2 supports available bit rate services with a timing relation between source and destination (Class B). ALL type 3 /4 was originally specified as two different AAL type (Type 3 and Type 4), but due to their inherent similarities, they were eventually merged to support both Class C and Class D services. AAL Type 5 also supports class C and Class D services

3.8.1 ALL Type5

Currently the most widely used adaptation layer is AAL type 5. AAL type 5 supports connection-oriented and connectionless services in which there is no timing relation between source and destination (class C and class D). Its functionality was intentionally made simple in order to support high speed data transfer. AAL type 5 assumes that the layers above the ATM adaptation layer can perform error recovery. Retransmission and sequence numbering when require and those it does not provide this functions. Therefore, only none assured operation is provided; lost or corrupted AAL type 5 packet will not be corrected by retransmission.

The SAR supplier of AAL type 5 performs segmentation of CS-PDU into a size suitable for the SAR-SDU pay load. Unlike other AAL types, Type 5 devotes the entire 48-octet payload of the ATM cell to the SAR-SDU; there is no overhead. An AAL specific flag in the ATM Payload Type (PT).

Field of the cell header is set when the last cell of a CS-PDU is sent. The assembly of the CS-PDU frames at the destination is controlled by using this flag.

The CS-PDU format for AAL type 5 contains the user data payload, along with any necessary padding bits (PAD) and a CS-PDU trailer, which are added by the CS supplier when it receives the under information from the higher layer. The CS –PDU is padded using 0 + 47 bytes of PAD field to make the land of the CS_PDU and integral multiple of 48 bytes (the size of the SAR -SDU) at the receiving end, reassembled PDU is passed to the CS sub layer from the SAR sub layer, CRC values are then calculated and compared.

If there is no error, the PAD field is removed by using the value of length field (LF) in the CS -PDU trailer, and user data is passed to the higher layer. If an error is detected, the erroneous information is either delivered to the use or discarded according to user‘s choice. The use of the CF field is for further study

3.9 ATM Signaling

ATM follows the principle of out-of-band signaling that was established for N-ISDN. In other words, signaling and data channels are separate. The main purposes of signaling are:

1) To establish, maintain and release ATM virtual connections.
2) To negotiate the traffic parameters of new connections

The ATM signaling standards support the creation of point to point as well as multicast connections. Typically certain VCI and VPI values are reserved by ATM networks for signaling messages. If additional signaling VCs are required, they may be establish through the process of meta-signaling.

Summary and Conclusion

A Local Area Network (LAN) links computers in a building, or across a school, office or campus. The LAN allows data and applications to be shared on multiple computers. A LAN also allows applications and/or files to be accessed on a central server via wired or wireless connections. With a wired LAN, computers are connected by a solid and fixed network of wires. It can be difficult to move and expensive to change.

A wireless LAN enables a local network of computers to exchange data or other information without the use of cables. It can either replace or extend a wired LAN, and data can be transmitted through the air, through walls, ceilings and even cement structures, without wired cabling. With a wireless LAN in place, laptop or handheld computers may be carried from place to place while remaining connected. Any device within range of an access point can potentially connect to the wireless LAN. This provides greatly increased freedom and flexibility compared to a wired network.

With a wireless LAN, additional users and access points can be added as necessary. Students and teachers can stay connected as they move throughout the school and, depending on how it is configured, access information anywhere in the school or in the school grounds.

The most common wireless standard, 802.11b, has a data transfer rate of 11 megabits per second (Mbps), much slower than current wired LANs, which operate at 100Mbps. Newly installed wired networks now operate at 1000Mbps (1Gb).

With a wireless LAN, bandwidth is sufficient to allow the use of a wide range of applications and services. However, it has a limited ability to deliver multimedia applications at sufficient quality, and a wired LAN is likely to be necessary to access these. Ongoing advances in wireless standards continue to increase the data rate achievable with new equipment. 802.11b devices are often branded with a WiFi mark to indicate interoperability.

As a conclusion, I would like to say a few words about done work. I investigated performance analyses of the departmental LAN in EMU for ten computers. The results are shown in graphs and in tables. I did these graphs for clear understanding of the results. I also wrote a general description of all the graphs. The performance analysis of a Departmental LAN is very important thing to investigate before doing any experiments in a LAN segment.

I can say at end of this work I learned more about performance investigation of the Departmental LAN. I learned a lot of new things about network and transmission media. Another important point I acquire, how I should organize my time and my life. I have to work more and more to be successful in my job.

References

1. GOVELL EDUCATION COURSE 200 "Networking Technologies" Novell, inc 1994
2. GILBERT HELD "Local Area Network Performance: Issues and Answers" John Willy Copyrigh 1994
3. ALEXANDER KOSTIN "Investigation of the concurrent access of the varying member of client to a file server in a local area network" Cmpe-333 Computer Networks lecture experiment sheet, 1996
4. Internet pages
5. Computer center