



NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

**Internet Protocols and Local Area Network
Management Systems**

**Graduation Project
COM 400**

Student : BASIL RIYAL(990973)

Supervisor:Mr. Halil Adahan

Nicosia – 2003



ACKNOWLEDGMENTS

With all the respect, I would like to acknowledge my father, MR Ghassan Riyal, which without his support and love, I would not have the opportunity to achieve the success in my life and studies, and god gives him a long and beautiful life.

I would like also to acknowledge one of my best instructors, MR khalil Adahan, who helped me a lot not only concerning my project but in important subjects for engineering that we would not have learned a lot without him.

My special appreciations go to every individual and friend who contributed in this effort and who created for me the best atmosphere to work successfully overcoming all difficulties that I faced during my life study.

ABSTRACT

I chose talking about networks from any other subjects from the knowledge, that networks are widely used, anywhere and anytime, as we all know that networks make the world very small, by the ability of contacting any person needed, even if he is very far from you. And I specialized in network management because it is an essential, and important activity in our life, because networks are taking an essential part of everyday activities in the entire world, management systems are needed for every action and duty, not only in network administrating but also used in business, studies, and every daily activity, also note that network and internet protocols are developing very quickly and everyday, so we as an engineers either cope with this fast developments or we parish, so working in the future as network administrator brings me into a sea of knowledge, and ability to prove myself in my future career, if god wishes.

LIST OF ABBREVIATIONS

10Base2 - Ethernet specification for thin coaxial cable, transmits signals at 10 Mbps (megabits per second) with a distance limit of 185 meters per segment.

10Base5 - Ethernet specification for thick coaxial cable, transmits signals at 10 Mbps (megabits per second) with a distance limit of 500 meters per segment.

10BaseF - Ethernet specification for fiber optic cable, transmits signals at 10 Mbps (megabits per second) with a distance limit of 2000 meters per segment.

10BaseT - Ethernet specification for unshielded twisted pair cable (category 3, 4, or 5), transmits signals at 10 Mbps (megabits per second) with a distance limit of 100 meters per segment.

100BaseT - Ethernet specification for unshielded twisted pair cabling that is used to transmit data at 100 Mbps (megabits per second) with a distance limit of 100 meters per segment.

Asynchronous Transfer Mode (ATM) - A network protocol that transmits data at a speed of 155 Mbps and higher. It is most often used to interconnect two or more local area networks.

Backbone - A cable to which multiple nodes or workstations are attached.

Bridge - Devices that connect and pass packets between two network segments that use the same communications protocol.

Cable - Transmission medium of copper wire or optical fiber wrapped in a protective cover.

Client/Server - A networking system in which one or more file servers (Server) provide services; such as network management, application and centralized data storage for workstations (Clients).

CSMA/CA - Carrier Sense Multiple Access Collision Avoidance is a network access method in which each device signals its intent to transmit before it actually does so. This prevents other devices from sending information, thus preventing collisions from occurring between signals from two or more devices. This is the access method used by LocalTalk.

CSMA/CD - Carrier Sense Multiple Access Collision Detection is a network access method in which devices that are ready to transmit data first check the channel for a carrier. If no carrier is sensed, a device can transmit. If two devices transmit at once, a collision occurs and each computer backs off and waits a random amount of time before attempting to retransmit. This is the access method used by Ethernet.

Coaxial Cable - Cable consisting of a single copper conductor in the center surrounded by a plastic layer for insulation and a braided metal outer shield.

Concentrator - A device that provides a central connection point for cables from workstations, servers, and peripherals. Most concentrators contain the ability to amplify the electrical signal they receive.

Ethernet - A network protocol invented by Xerox Corporation and developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps (megabits per second).

Fiber Optic Cable - A cable, consisting of a center glass core surrounded by layers of plastic, that transmits data using light rather than electricity. It has the ability to carry more information over much longer distances.

File Server - A computer connected to the network that contains primary files/applications and shares them as requested with the other computers on the network. If the file server is dedicated for that purpose only, it is connected to a client/server network. An example of a client/server network is Novell Netware. All the computers connected to a peer-to-peer network are capable of being the file server. Two examples of peer-to-peer networks are LANtastic and Windows for Workgroups.

Hub - A hardware device that contains multiple independent but connected modules of network and internetwork equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat but merely split signals sent through them).

LAN (Local Area Network) - A network connecting computers in a relatively small area such as a building.

Network Interface Card (NIC) - A board that provides network communication capabilities to and from a computer.

Node - End point of a network connection. Nodes include any device attached to a network such as file servers, printers, or workstations.

Node Devices - Any computer or peripheral that is connected to the network.

Peer-to-Peer Network - A network in which resources and files are shared without a centralized management source.

Protocol - A formal description of a set of rules and conventions that govern how devices on a network exchange information.

Repeater - A device used in a network to strengthen a signal as it is passed along the network cable.

Router - A device that routes information between interconnected networks. It can select the best path to route a message, as well as translate information from one network to another. It is similar to a superintelligent bridge.

Star Topology - LAN topology in which each node on a network is connected directly to a central network hub or concentrator.

Star-Wired Ring - Network topology that connects network devices (such as computers and printers) in a complete circle.

Twisted Pair - Network cabling that consists of four pairs of wires that are manufactured with the wires twisted to certain specifications. Available in shielded and unshielded versions.

WAN (Wide Area Network) - A network connecting computers within very large areas, such as states, countries, and the world.

Workgroup - A collection of workstations and servers on a LAN that are designated to communicate and exchange data with one another.

Workstation - A computer connected to a network at which users interact with software stored on the network.

Asynchronous Transfer Mode (ATM) - A network protocol that transmits data at a speed of 155 Mbps and higher. It is most often used to interconnect two or more local area networks.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	i
ABSTRACT	ii
LIST OF ABBREVIATIONS.....	iii
TABLE OF CONTENTS.....	vi
INTRODUCTION.....	1
Chapter 1: GENERAL NETWORK PRINCIPLES.....	2
1.1 Overview.....	2
1.2 Purposes of Networking.....	2
1.3 User Requirements.....	4
1.4 User Interfaces.....	6
1.4 Network Application.....	8
1.5 Network Technologies.....	9
1.6 Network Structures.....	10
1.7 Equipment Linked To Networks.....	12
1.8 Data Transmission.....	13
1.9 Network Architecture Standards and Protocols.....	13
1.10 Network Control and Performance.....	14
1.11 Network Computers (NC).....	15
1.12 General Network Design Principles.....	16
1.12.1 Core Layer.....	17
1.12.2 Distribution Layer.....	17
1.12.3 Access Layer.....	17
Chapter 2: LOCAL AREA NETWORK.....	18
2.1 Overview.....	18
2.2 Review and Classification of Local Area Network Technologies.....	19
2.3 What Is a LAN?	20
2.4 How Does LAN Operate?	21
2.5 LAN Applications.....	21
2.6 LAN Network Operating System.....	22
2.6.1 Peer-to-Peer.....	23
2.6.2 Client/Server.....	24
2.7 LAN Hardware Design	25
2.7.1 LAN Cabling Standards.....	25

2.7.2 Network Cards.....	26
2.7.3 Backbones.....	27
2.8 Devices Connected to LAN.....	27
2.8.1 Hubs.....	27
2.8.2 Repeaters.....	28
2.8.3 LAN Switches.....	29
2.8.4 Bridging.....	30
2.8.5 Routers.....	31
2.8.6 LAN Extender.....	32
2.9 LAN Topologies and Media.....	33
2.9.1 Bus Topology.....	34
2.9.2 Star Topology.....	34
2.9.3 Star-Wired Ring.....	35
2.9.4 Ring Topology.....	36
2.9.5 Tree Topology.....	37
2.10 LAN Cabling.....	38
2.10.1 Twisted Pair.....	38
2.10.2 Coaxial Cable.....	40
2.10.3 Fiber Optic Cable.....	41
2.10.4 Wireless LANs.....	42
2.11 Data Communication Principles.....	46
2.11.1 LAN Media-Access Methods(MAC).....	46
2.11.2 LAN Transmission Methods.....	47
2.11.3 The OSI Model.....	49
2.12 Some Advantages and Disadvantages of Local Area Network.....	51
2.13 Implementing and Designing a High-Speed, Self Configured LAN.....	53
2.14 Other Implemented Data Networks.....	56
Chapter 3: LOCAL AREA NETWORK DESIGN AND MANAGEMENT SYSTEM.....	57
3.1 Overview.....	57
3.2 Role of The Network Engineer.....	57
3.3 Network Management.....	58
3.4 Local Area Network Management.....	58
3.5 Network Management Functions.....	59
3.5.1 Fault Management.....	59
3.5.2 Configuration management.....	60

3.5.3 Security management.....	61
3.5.4 Performance Management.....	64
3.5.5 Accounting Management.....	64
3.6 The Network Management System.....	65
3.6.1 The Network Management Platform.....	65
3.6.2 Network Management Architecture.....	67
3.7 Network Management Protocols.....	68
3.8 Internet Protocols.....	69
3.8.1 Network Protocol.....	69
3.8.2 Network Subnets.....	70
3.8.3 The TCP/IP.....	71
3.8.4 THE TCP/IP LAYERS.....	71
3.8.4.1 Network Access Layer.....	71
3.8.4.2 Internet Layer.....	71
3.8.4.3 Transport Layer.....	71
3.8.4.4 Application Layer.....	72
3.8.5 The Network Access Layer.....	72
3.8.5.1 Ethernet.....	72
3.8.5.1.1 Fast Ethernet.....	73
3.8.5.1.2 Gigabit Ethernet.....	73
3.8.5.2 Token Ring.....	73
3.8.5.3 FDDI.....	74
3.8.5.4 ATM.....	74
3.8.6 The Internet Layer.....	74
3.8.6.1 Internet Protocol (IP).....	74
3.8.6.2 Internet Control Message Protocol (ICMP).....	76
3.8.6.3 Routing Internet Protocol (RIP).....	77
3.8.7 Transport Layer.....	77
3.8.7.1 Transmission Control Protocol (TCP).....	77
3.8.7.2 User Datagram Protocol (UDP).....	79
3.8.8 The Application Layer.....	79
3.8.8.1 File Transfer Protocol (FTP).....	79
3.8.8.2 Hypertext Transfer Protocol (HTTP).....	80
CONCLUSION.....	81
REFERENCES.....	82

INTRODUCTION

Network management is a specialized, and important in our life, because networks are taking an essential part of everyday activities in the entire world, management systems are needed for every action and duty, not only in network administrating but also used in business, studies, and every daily activity, now talking about local area networks, All LANs require regular administration and management in order to function efficiently and effectively. A Network Administrator is required to perform a range of duties in order to achieve this efficiency and effectiveness. These include maintaining system security, implementing backup strategies, installing software, upgrading software, managing data storage and ensuring provision of virus protection.

Considering the second subject in my project, which is internet protocols, which is also important subject because data communication has become a fundamental part of computing. World-wide networks gather data about such diverse subjects as atmospheric conditions, crop production, and airline traffic. Groups establish electronic mailing lists so they can share information of common interest. Hobbyists exchange programs for their home computers. In the scientific world, data networks are essential because they allow scientists to send programs and data to remote supercomputers for processing, to retrieve the results, and to exchange scientific information with colleagues.

Recently, however, a new technology has emerged that makes it possible to interconnect many disparate physical networks and make them function as a coordinated unit. The new technology, called internetworking, or internetting, accommodates multiple, diverse underlying hardware technologies by adding both physical connections and a new set of conventions. The Internet technology hides the details of network hardware and permits computers to communicate independent of their physical network connections.

CHAPTER ONE

GENERAL PRINCIPLES OF NETWORKING

1.1 Overview

This chapter explains the most important general principles that are used in most Forms of computer networks, including local area networks, personal computer networks and linked local area networks. It considers only those principles that are widely used.

As we all know networking is taking an essential part of our career, entertainment and many other roles in our life. But why? Is the question to be asked, and you could find the answer after reading the 1st chapter of this project. But what I could add now is that recently people on earth are lazy and they require help to accomplish their jobs easily, fastly and efficiently, so from here comes the need of networks and communications between people.

Firstly, there are brief discussions of the purposes and user requirements of networking(here I will talk about the ability of making the user more dissolved with the usage of networking and being satisfied of network usage). This chapter then considers in turn user interfaces to computer networks, network architecture (which is the building and main parts of computer network system), devices and other equipment linked to networks, data transmission (it's an important part of networks which talks about the data that is transferred through networks), network standards and protocols, network control and performance.

1.2 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.

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

Other purposes of implementing network for normal users include:

- Implementation of administrative and financial database.
- Staff access to company records.
- Automation of letter, report or specification writing.
- E-mail for staff.
- Staff scheduling.
- General information automation (including library, plans, graphics and images).
- Learning or training aids (interactive software).

Computer skills training rooms (word processing, publishing, CADD, spreadsheets, databases).

- Printer sharing.
- File transfer.
- Internet access (graphical, text, news).
- Access to centralized information sources (e.g. CD-ROM stacks).
- Automate software updates.
- Centralize application software.

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:

- relationship building i.e. personally connecting with others.
- relationship maintenance i.e. timely reconnecting and communicating.
- information sharing i.e. adding value to the relationship.

1.3 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.

Last but not least are the ergonomic requirements of networking, that the equipment used shall provide a pleasant environment and interface for the user, which is neither tiring nor, in the long run, a health hazard or source stress.

1.4 User Interfaces

A typical user interface to a computer network, whether it is a terminal or a more elaborate 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.

Examples of User Interface

Acme windows are 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.

X Windows or 8½ [Sche86, Pike91]. 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.

Macintosh, 8½, and Sam. 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 Application

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 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 file 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, fiber 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 proposed modifications or new features, and learning from practical experience of networks.

1.6 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 "subnet" as explained in figure 1.1. 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 others; 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 way 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, belonging to the different networks that are being brought together there.

There are configurations of interconnected networks of various types; for example, it shows not only interconnected Neighboring: WAN, but very important, the linkages between different LANS, separated from each other by intervening WAN.

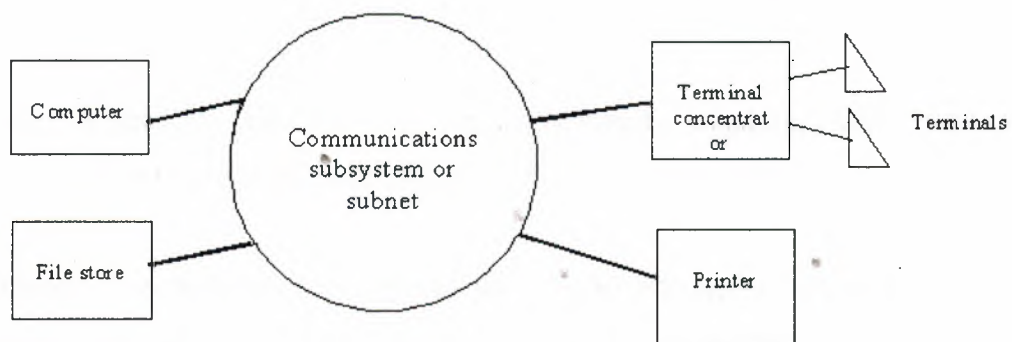


Fig 1.1 Example of a computer network, sharing attached devices, subnet and interfaces between devices and subnet source: Based on author's drawing.

1.7 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 be linked 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, and 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 is 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 magnetic 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.

1.8 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.

1.9 Network Architecture Standards and 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 organized. 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 overcome 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.

1.10 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 flow 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 network, 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, the 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.

1.11 Network Computers (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, a complete Java-based operating system downloads to 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 Java 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.

1.12 GENERAL NETWORK DESIGN PRINCIPLES

Good network design is based on many concepts that are summarized by the following key principles:

i. Principle 1

Examine single points of failure carefully. There should be redundancy in the network so that a single failure does not isolate any portion of the network. There are two aspects of redundancy that need to be considered: backup and load balancing. In the event of a failure in the network, there should be an alternative or backup path. Load balancing occurs when two or more paths to a destination exist and can be utilized depending on the network load. The level of redundancy required in a particular network varies from network to network.

ii. Principle 2

Characterize application and protocol traffic. For example, the flow of application data will profile client-server interaction and is crucial for efficient resource allocation, such as the number of clients using a particular server or the number of client workstations on a segment.

iii. Principle 3

Analyze bandwidth availability. For example, there should not be an order of magnitude difference between the different layers of the hierarchical model. It is important to remember that the hierarchical model refers to conceptual layers that provide functionality. The actual demarcation between layers does not have to be a physical link. It can be the backplane of a particular device.

iv. Principle 4

Build networks using a hierarchical or modular model. The hierarchy allows autonomous segments to be internetworked together.

There exist a high-level view of the various aspects of a hierarchical network design. A hierarchical network design presents three layers core, distribution, and access, with each layer providing different functionality.

1.12.1 Core Layer

The core layer is a high-speed switching backbone and should be designed to switch packets as fast as possible. This layer of the network should not perform any packet manipulation access lists and filtering that would slow down the switching of packets.

1.12.2 Distribution Layer

The distribution layer of the network is the demarcation point between the access and core layers and helps to define and differentiate the core. The purpose of this layer is to provide boundary definition and is the place at which packet manipulation can take place. In the campus environment, the distribution layer can include several functions, such as the following:

- Address or area aggregation
- Departmental or workgroup access
- Broadcast/multicast domain definition
- VLAN routing
- Any media transitions that need to occur
- Security

1.12.3 Access Layer

Is the layer where access is held and distributed according to defined rules, in this layer the access to the hardware and software components may be allowed to the various machines connected to the network

CHAPTER TWO

LOCAL AREA NETWORKS

2.1 Overview

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. Without making any claim to be comprehensive. Those systems, that are based on personal computer networks and “micro nets”.

The present chapter begins by reviewing briefly some of the available LAN technologies. These LAN technologies describe the latest local area network development and how it is implemented considering some structures.

The rest of the chapter describes in more detailed aspects, the hardware structure of LAN , including cabling and essential devices used for not only local area networks but also other networking kinds that are used for small and wide communications, example. wide area networks, metropolitan area networks, in the commercially available LAN systems, providing a very wide range of services for business offices and other organizations, this chapter also mentions the methods of communicating-media access methods-, the OSI model and if you go through this chapter you will obviously find that most important subjects in the local area network are categorized in a unique way. Finally, it considers the standards which employees the local area network.

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.

2.2 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).
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.

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 dialed conveniently, 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.

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 in practice.

Ethernets and other similar bus networks are suitable for serving many users at a single site, where no pair of stations is more than a few miles apart. They can provide gateway access to other networks. They are also very reliable and have good performance. Cable bus systems allow many different services, such as data, voice and television traffic, to be supported on the same cable.

2.3 What Is a LAN?

A LAN is a high-speed data network (medium allows a high bit transmission rate) that covers a relatively small geographic area. 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.

2.4 How Does LAN Operate?

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 networks, the server must have the power to operate strongly within the network. This strongness and effectiveness of the server lies in the presence of a strong operating system ex: -windows NT, windows 2000 may be also used.

Local area network (LAN) could use any topology for connection, bus topology is used to connect the pc's together, and the information and data are stored in the file system (FS), see figure 2.1, 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 corruptions in the FS may cause a troubleshoot (problems) in connecting LAN'S.

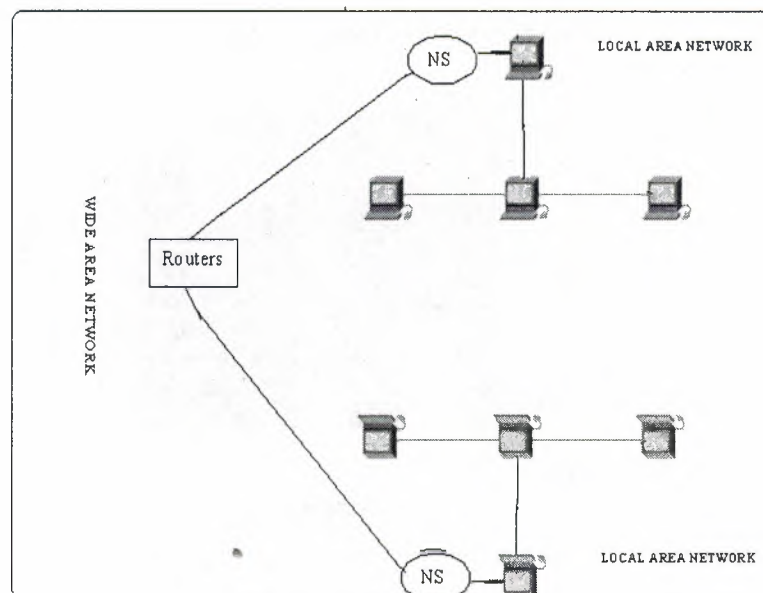


Fig 2.1 LAN Operation

2.5 LAN Applications

The types of applications for which LANs are used are quite similar to applications on stand alone personal computers, with word processing, spreadsheets, and database management the most widely used applications. Database management and word processing were the only applications expected to be used more than two-thirds of planned LANs. Usages total to more than 100% for both current and planned LAN installations since a single LAN may be used for multiple applications.

Fig 2.2 and 2.3 show the types of applications used on existing LANs and expected to be used on planned LANs.

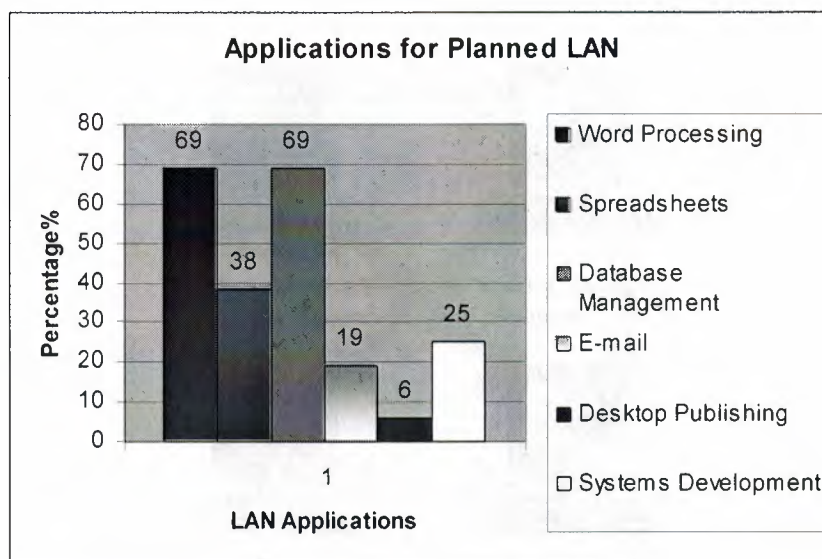
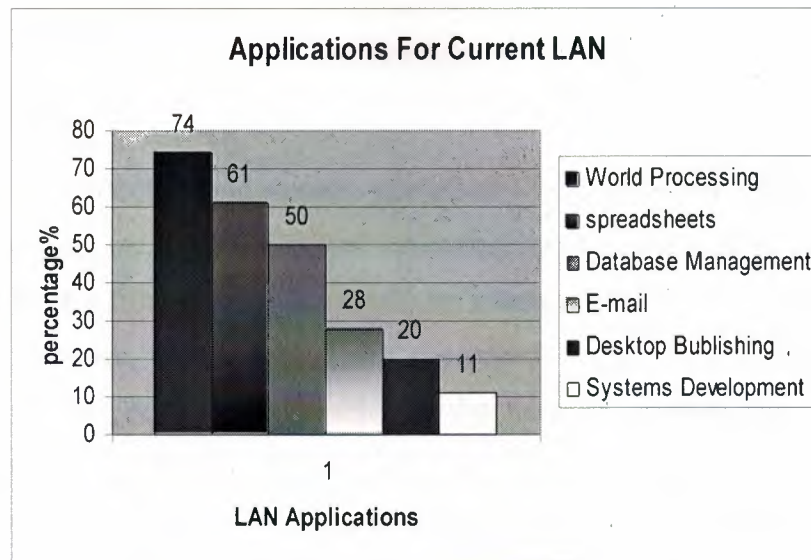


Fig 2.2, Fig 2.3 LAN Applications

2.6 LAN Network Operating System.

Unlike operating systems, such as DOS and Windows95, that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly.

The two major types of network operating systems are:

- Peer-to-Peer
- Client/Server

2.6.1 Peer-to-Peer

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source (See fig. 2.4). In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. AppleShare and Windows for Workgroups are examples of programs that can function as peer-to-peer network operating systems.

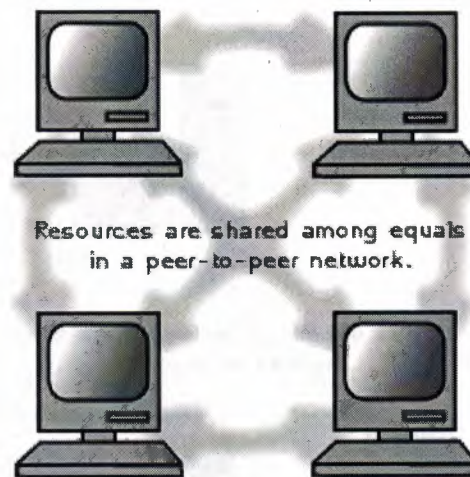


Fig. 2.4: Peer-to-peer network

Advantages of a Peer-To-Peer Network:

- Less initial expense - No need for a dedicated server.
- Setup - An operating system (such as Windows 95) already in place may only need to be reconfigured for peer-to-peer operations.

Disadvantages of a Peer-to-Peer Network:

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

2.6.2 Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers (See fig. 2.5). The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. Novell Netware and Windows NT Server are examples of client/server network operating systems.

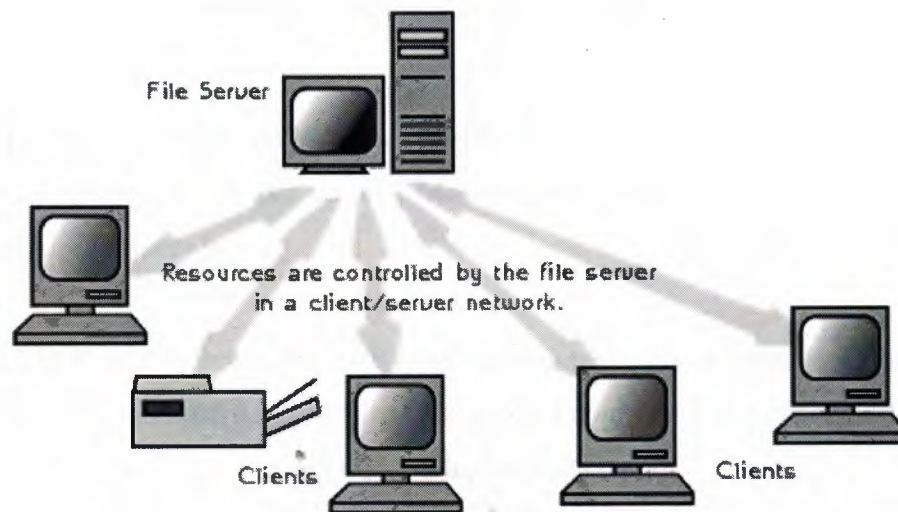


Fig. 2.5 Client/server network

Advantages of a Client/Server Network:

1. Centralized - Resources and data security are controlled through the server.
2. Scalability - Any or all elements can be replaced individually as needs increase.
3. Flexibility - New technology can be easily integrated into system.
4. Interoperability - All components (client/network/server) work together.

5. Accessibility - Server can be accessed remotely and across multiple platforms.

Disadvantages of a Client/Server Network:

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

2.7 LAN HARDWARE DESIGN

2.7.1 LAN Cabling Standards

We recommend Category 5 cables for new users. Officially called Ethernet 10/100BaseT, they're the most common type of network cable and provide a good upgrade path should you need it. Cat 5 allows either 10- or 100-megabyte communication. These terms have simple meanings, so don't let them put you off.

- The "10" or "100" in 10/100BaseT refers to network connection speed i.e. 10 Megabits or 100 Mega-bits per second. Most networks actually top out at less, though most users would never know.
- The "T" in BaseT refers to the wire type, twisted-pair, which consists of pairs of thin wires twisted around each other. It also refers to the connector, commonly called an RJ-45, which resembles a big-ger and wider telephone connector.
- "Base" means that the cable is used for baseband (i.e., simple, single frequency) rather than broad-band (multiplex or analog) networks.

Cables can be purchased in different lengths and often different colors. They come with a male RJ-45 plug at each end. Cards and hubs have female RJ-45 jacks.

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

Table 2.1: Ethernet Cable Summary

2.7.2 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:

1. 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.
2. Plug and Play compatibility. This feature allows Windows 95/98 to automatically configure the card, saving you a lot of time in the process.
3. 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.

2.7.3 Backbones

In larger enterprises, some sort of information backbone, or data highway, allows high speed, high quality internetworking with good reliability. Backbones connect LANs, WANs and other forms of network segments together in one large network. The decision to build a backbone depends on the present and future needs of the enterprise. But once it is implemented, growth becomes less painful. One common backbone is the Fiber Distributed Data Interface, or FDDI standard. This backbone is also available in a copper version (CDDI).

FDDI is considered an implementation of a "metropolitan" LAN, or MAN. It is a dual-ring topology that can span up to 200 kilometers at 100 Mbps. It is commonly used to connect LANs together where higher bandwidths are required. Two rings of fiber carry data. All nodes attach to at least the primary ring, with some or all attached to the secondary ring. The idea is that if one ring breaks, the other automatically picks up the load. If both rings break at the same point, they automatically join together in one long ring.

2.8 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.

2.8.1 Hubs

A hub is a physical layer device that connects multiple user stations, each via a dedicated cable. The purpose of a hub is to regenerate and retime network signals. This is done at the bit level to a large number of hosts using a process known as concentration. You will notice that this definition is very similar to the repeater's, which is why a hub is also known as a multi-port repeater.

The difference is the number of cables that connect to the device. Two reasons for using hubs are to create a central connection point for the wiring media, and increase the reliability of the network. The reliability of the network is increased by allowing any single cable to fail without disrupting the entire network. This differs from the bus topology where having one cable fail will disrupt the entire network. Hubs are considered Layer 1 devices because they only regenerate the signal and broadcast it out all of their ports (network connections). A hub is used in as ethernet conjunction with 10BaseT and 100BaseT cables. The cables run from the network's computers to ports on the hub. Using a hub makes it easier to move or add computers, find and fix cable problems, and remove computers temporarily from the network (if they need to be upgraded, for instance).

There are different classifications of hubs in networking. The first classification is active or passive hubs. Most modern hubs are active; they take energy from a power supply to regenerate network signals. Some hubs are called passive devices because they merely split the signal for multiple users, like using a "Y" cord on a CD player to use more than one set of headphones. Passive hubs do not regenerate bits, so they do not extend a cable's length, they only allow two or more hosts to connect to the same cable segment.

Another classification of hubs is intelligent or managed(dump). This classification is explained below:

Intelligent Hubs

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. This console ports in the intelligent hubs, enables the hub to be programmed to manage network traffic.

Managed Hubs

Are hubs managed by supervisor, and dont process by its own. hubs simply take an incoming networking signal and repeat it to every port without the ability to do any management.

2.8.2 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, retiming, 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 2.6 illustrates a repeater connecting two network segments.

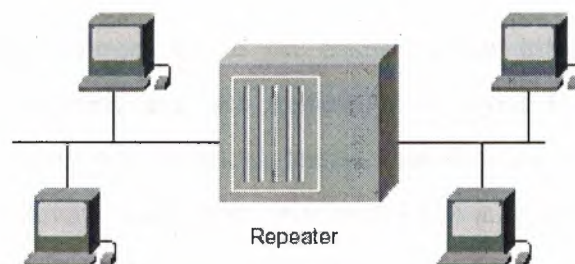


Figure 2.6 A Repeater Connecting Two Network Segments

2.8.3 LAN Switches

A switch is a Layer 2 device just as a bridge is. In fact a switch is called a multi-port bridge, just like a hub is called a multi-port repeater. The difference between the hub and switch is that switches make decisions based on MAC addresses and hubs don't make decisions at all. Because of the decisions that switches make, they make a LAN much more efficient. They do this by "switching" data only out the port to which the proper host is connected. In contrast, a hub will send the data out all of its ports so that all of the hosts have to see and process (accept or reject) all of the data. Switches at first glance often look like hubs.

Both hubs and switches have many connection ports, since part of their function is connectivity concentration (allowing many devices to be connected to one point in the network). The difference between a hub and a switch is what happens inside the device.

The purpose of a switch is to concentrate connectivity, while making data transmission more efficient. For now, think of the switch as something that is able to combine the connectivity of a hub with the traffic regulation of a bridge on each port. It switches frames from incoming ports (interfaces) to outgoing ports, while providing each port with full bandwidth (the transmission speed of data on the network backbone).

2.8.4 Bridging

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. Later, VLANs were devised when switches were deployed in enterprise environments and brought back the old problem of broadcast storms. Note that 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 2-11 Simple Bridge Network

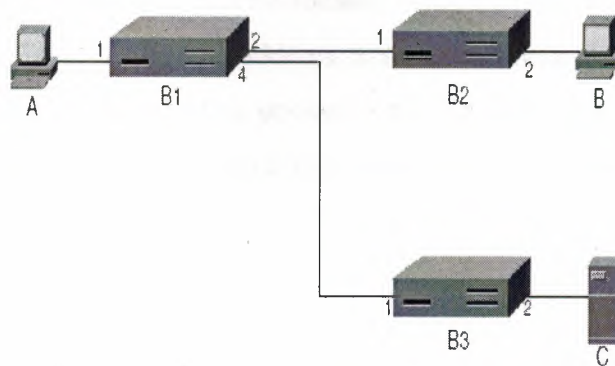


Fig 2.7: Simple Bridge Network

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.

2.8.5 Routers

A router is a Layer 3 device. Working at Layer 3 allows the router to make decisions based on groups of network addresses (Classes) as opposed to individual Layer 2 MAC addresses. Routers can also connect different Layer 2 technologies, such as Ethernet, Token-ring, and FDDI. However, because of their ability to route packets based on Layer 3 information, routers have become the backbone of the Internet, running the IP protocol.

The purpose of a router is to examine incoming packets (Layer 3 data), choose the best path for them through the network, and then switch them to the proper outgoing port. Routers are the most important traffic-regulating devices on large networks. They enable virtually any type of computer to communicate with any other computer anywhere in the world, While performing these basic functions, routers can also execute many other tasks.

In networking, there are two addressing schemes: one uses the MAC address, a data link (Layer 2) address; the other uses an address located at the network layer (Layer 3) of the OSI model. An example of a Layer 3 address is an IP address. A router is a type of internetworking device that passes data packets between networks, based on Layer 3 addresses. A router has the ability to make intelligent decisions regarding the best path for delivery of data on the network.

2.8.6 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 2.8 illustrates multiple LAN extenders connected to the host router through a WAN.

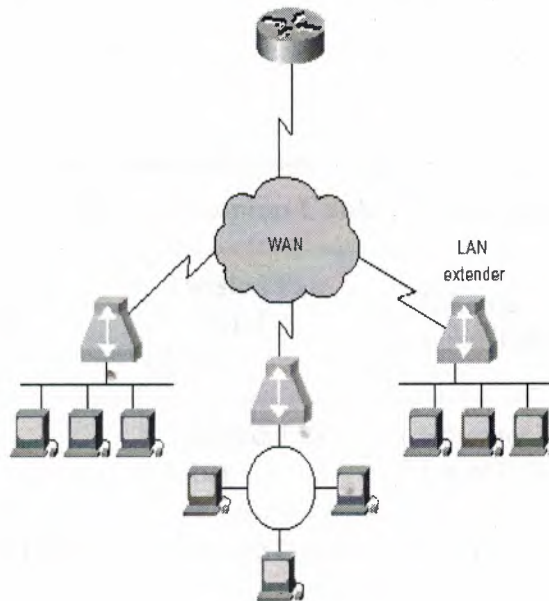


Fig 2.8 Multiple LAN Extenders Can Connect to the Host Router Through a WAN

2.9 LAN TOPOLOGIES AND MEDIA

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.

Considerations When Choosing a Topology.

1. **Money.** A linear bus network may be the least expensive way to install a network; you do not have to purchase concentrators.
2. **Length of cable needed.** The linear bus network uses shorter lengths of cable.
3. **Future growth.** With a star topology, expanding a network is easily done by adding another concentrator.
4. **Cable type.** The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

Physical Topology	Common Cable	Common Protocol
Linear Bus	Twisted Pair Coaxial Fiber	Ethernet LocalTalk
Star	Twisted Pair Fiber	Ethernet LocalTalk
Star-Wired Ring	Twisted Pair	Token Ring
Tree	Twisted Pair Coaxial Fiber	Ethernet

Table 2.2

2.9.1 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, including 100BaseT, implement a bus topology, which is illustrated below.



Fig 2.9: Some networks implement a local bus topology

With the Bus topology, all workstations are connect directly to the main backbone that carries the data. Traffic generated by any computer will travel across the backbone and be received by all workstations. This works well in a small network of 2-5 computers, but as the number of computers increases so will the network traffic and this can greatly decrease the performance and available bandwidth of your network.

Advantages of Bus Topology

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

Disadvantages of Bus Topology

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

2.9.2 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(2.10).

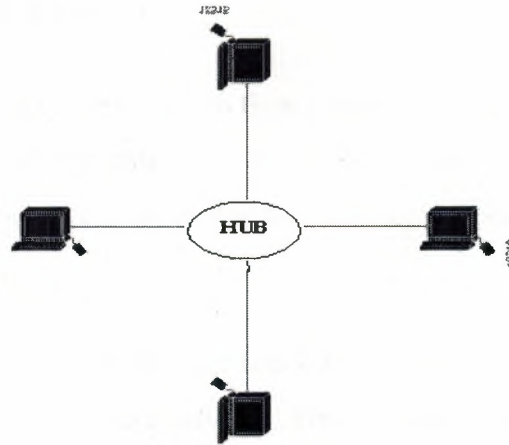


Fig 2.10 star LANS

All stations are attached by cable to a central point, usually a wiring hub or other device operating in a similar function. In the star topology, the information or data is sent through cables as signals to the central hub, which gives the access ability to all workstations connected to the hub.

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.

2.9.3 Star-Wired Ring

A star-wired ring topology may appear (externally) to be the same as a star topology. Internally, the MAU (multistation access unit) of a star-wired ring contains wiring that allows information to pass from one device to another in a circle or ring. The Token Ring protocol uses a star-wired ring topology.

Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network then connecting or removing devices.
- Easy to detect faults and to remove parts.
- no cable segment is a single point of failure impacting the entire network.

Disadvantages of a Star Topology

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

Mentioning the last 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.

2.9.4 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 2.11 depicts a logical ring topology, in ring topology one of the pc's connected on the network transmits 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.

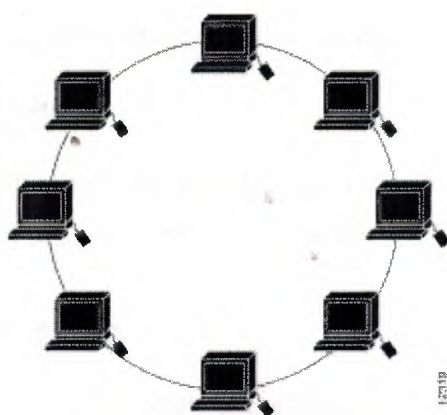


Figure 2.11 : Some networks implement a logical ring topology.

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. Figures 2.11 is an examples of ring topology.

2.9.5 Tree Topology

A tree topology is a LAN structure that is identical to the bus topology, except that branches with multiple nodes are possible in this case. Figure 2.12 illustrates a logical tree topology. The protocols used with star configurations are usually Ethernet or LocalTalk. Token Ring uses a similar topology, called the star-wired ring.

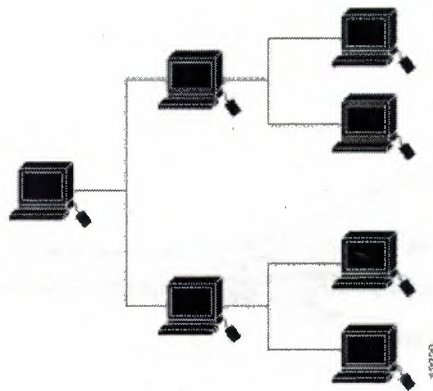


Fig 2.12 : A logical tree topology can contain multiple nodes.

Advantages of a Tree Topology

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

Disadvantages of a Tree Topology

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

2.10 LAN CABLING

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

2.10.1 TWISTED PAIR

Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for small networks (See fig. 2.13).

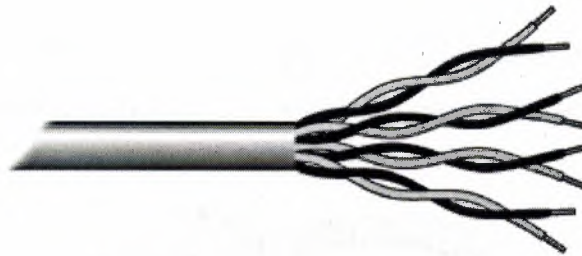


Fig 2.13: Unshielded twisted pair

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

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

Table 2.3: Categories of Unshielded Twisted Pair

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2.14). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



Fig 2.14: Unshielded Twisted Pair

Shielded Twisted Pair (STP) Cable

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

2.10.2 Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig 2.15). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.



Fig 2.15: Coaxial Cable

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

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

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

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 2.16). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.



Fig 2.16: connector for coaxial cabling

2.10.3 Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 2.17). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

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



Fig.2.17 Fiber optic cable

Facts about fiber optic cables:

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

Fiber Optic Connector

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

The advantages of Structured cabling are:

- 1. Consistency** – A structured cabling systems means the same cabling systems for data, voice and video.
- 2. Support for multi-vendor equipment** – A standard-based cable system will support applications and hardware even with mix & match vendors.
- 3. Simplify moves/adds/changes** – Structured cabling systems can support any changes within the systems.
- 4. Simplify troubleshooting** – With structured cabling systems, problems are less likely to down the entire network, easier to isolate and easier to fix.
- 5. Support for future applications** – Structured cabling system supports future applications like multimedia, video conferencing etc with little or no upgrade pain.

2.10.4 Wireless LANs

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data.

Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.



Fig 2.18

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

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

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

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

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.

A wireless LAN is made up of two key components:

- An access point, or base station, that is usually physically connected to a LAN.
- A wireless card that is either built into or added to a handheld, laptop or desktop computer.

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.

Some differences between wired and wireless LAN:

	Wires	Wireless
Installation and Management	If you have computers in several rooms you will have to drill holes through walls - often into the attic and down again is the best option. If you have a	Nothing to install or manage - however it should be noted that thick walls, trees, etc. will have an impact on the range of the wireless connection. Not a great issue though
Tidyness	Wires are a pain to keep tidy	Nothing to keep tidy!
Reliability	Wires can be pulled, tampled on, chewed by cats, rodents(!), etc.	Nothing to go wrong
Portability	None/very limited	Take your computer (e.g. laptop, tablet or PDA) anywhere around your house/office/garden - or even the pub over the road
Speed	100Mb/sec is the current de-facto for home/office usage and 100Mb/sec or 1GB/sec for servers. Although up to 10GB/sec is now available	10Mb/sec is the most common. D-Link and a few other companies now do 22Mb/sec (which is slightly faster, but not true 22Mb/sec). 'Standards' are out that go faster than this (e.g. 53Mb/sec but this is not yet fully standardised and people are being warned not to move over to the 802.11g standard just yet...
Cost	Quite cheap	Now quite cheap now that the take up of it is booming - a couple of years ago this was very expensive
Security	Totally secure if your LAN is not connected to the Internet or other external source (i.e. it is a 'closed system') as someone would have to physically connect their computer to it in order to connect to anything	<p>If not configured for security someone could be sitting outside your house/office with a laptop and could log onto your network.</p> <p>Secure once set up correctly:</p> <ul style="list-style-type: none"> • Limit or exclude access by MAC addresses - every network card in the world has a unique MAC address • Encrypt data being transmitted so that others cannot evesdrop and capture data • Hide node IDs in order to ensure privacy (i.e. make each node/device invisible to others not on the network)

Table 2.4

2.11 DATA COMMUNICATION PRINCIPLES

2.11.1 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.

2.11.2 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 transferred from one machine into another.

Unicasting

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 2.19 is an example of a unicast network.

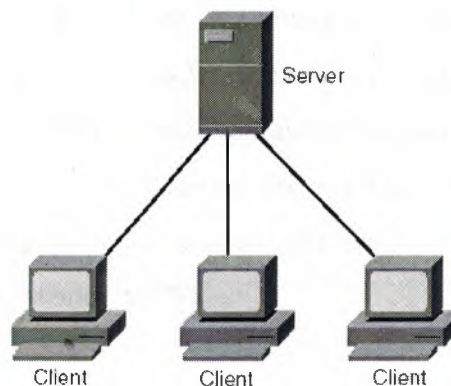


Fig 2.19: unicast network

Multicasting

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 2.20 is an example of a multicast network.

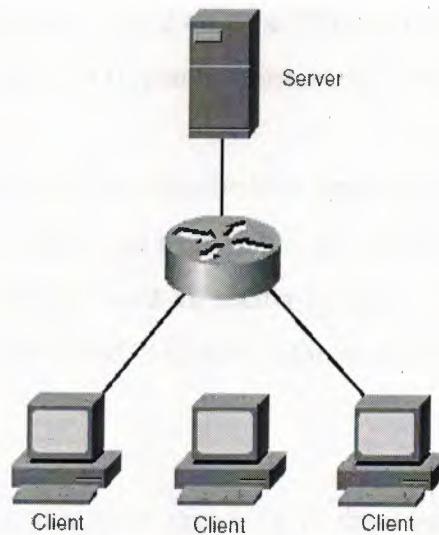


Fig 2.20: Multicast Network

Broadcasting

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).



Fig 2.21: Broadcasted transmission

2.11.3 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) Reference Model.

This model defines seven Layers that describe how applications running 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 technician 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, starting from the bottom, and explains some of the devices and protocols you might expect to find in your data centre operating at this layer.

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.

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 migrating a device between different switch ports can cause the device to lose network connectivity for a while, until the switch, or bridge, re-ARPs.

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.

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.

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 understand when a session is taking place, and not to interfere with it.

considerable savings when compared to buying individual components

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.

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).

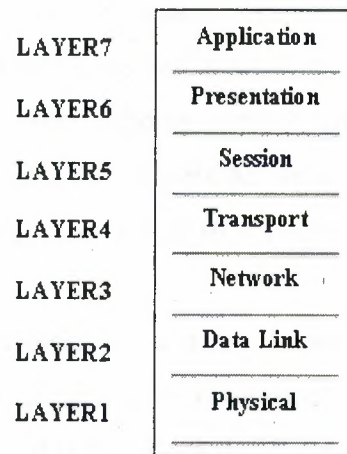


Fig 2.22 The OSI model

2.12 Some Advantages And Disadvantages Of Local Area Network

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

Advantages of Local Area Network

1. **Speed.** Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to floppy disks, then carrying or sending the disks from one computer to another. This method of transferring files (referred to as sneaker-net) is very time-consuming.
2. **Cost.** Networkable versions of many popular software programs are available at considerable savings when compared to buying individually licensed copies.

Besides monetary savings, sharing a program on a network allows for easier upgrading of the program. The changes have to be done only once, on the file server, instead of on all the individual workstations.

3. **Security.** Files and programs on a network can be designated as "copy inhibit," so that you do not have to worry about illegal copying of programs. Also, passwords can be established for specific directories to restrict access to authorized users.
4. **Centralized Software Management.** One of the greatest benefits of installing a network at a school is the fact that all of the software can be loaded on one computer (the file server). This eliminates that need to spend time and energy installing updates and tracking files on independent computers throughout the building.
5. **Resource Sharing.** Sharing resources is another area in which a network exceeds stand-alone computers. Most schools cannot afford enough laser printers, fax machines, modems, scanners, and CD-ROM players for each computer. However, if these or similar peripherals are added to a network, they can be shared by many users.
6. **Electronic Mail.** The presence of a network provides the hardware necessary to install an e-mail system. E-mail aids in personal and professional communication for all school personnel, and it facilitates the dissemination of general information to the entire school staff. Electronic mail on a LAN can enable students to communicate with teachers and peers at their own school. If the LAN is connected to the Internet, students can communicate with others throughout the world.
7. **Flexible Access.** School networks allow students to access their files from computers throughout the school. Students can begin an assignment in their classroom, save part of it on a public access area of the network, then go to the media center after school to finish their work. Students can also work cooperatively through the network.
8. **Workgroup Computing.** Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently. For example, educators located at various schools within a county could simultaneously contribute their ideas about new curriculum standards to the same document and spreadsheets.
9. **Shared access to devices and applications.**

Disadvantages of Local Area Network

- 1. Expensive to Install.** Although a network will generally save money over time, the initial costs of lan installation can be prohibitive. Cables, network cards, and software are expensive, and the installation may require the services of a technician.
- 2. Requires Administrative Time.** Proper maintenance of a network requires considerable time and expertise. Many schools have installed a network, only to find that they did not budget for the necessary administrative support.
- 3. File Server May Fail.** Although a file server is no more susceptible to failure than any other computer, when the files server "goes down," the entire network may come to a halt. When this happens, the entire school may lose access to necessary programs and files.
- 4. Cables May Break.** The Topologies present information about the various configurations of cables. Some of the configurations are designed to minimize the inconvenience of a broken cable; with other configurations, one broken cable can stop the entire network.

2.13 Implementing and Designing a High-Speed, Self Configured LAN.

Autonet

Autonet is a self-configuring local area network composed of switches interconnected by 100 Mbit/second, full-duplex, point-to-point links. The switches contain 12 ports that are internally connected by a full crossbar. Switches use cut-through to achieve a packet forwarding latency as low as 2 microseconds per switch. Any switch port can be cabled to any other switch port or to a host network controller.

A processor in each switch monitors the network's physical configuration. A distributed algorithm running on the switch processors computes the routes packets are to follow and fills in the packet forwarding table in each switch. This algorithm automatically recalculates the forwarding tables to incorporate repaired or new links and switches, and to bypass links and switches that have failed or been removed. Host network controllers have alternate ports to the network and fail over if the active port stops working.

With Autonet, distinct paths through the set of network links can carry packets in parallel. Thus, in a suitable physical configuration, many pairs of hosts can communicate simultaneously at full link bandwidth. The aggregate bandwidth of an Autonet can be increased by adding more links and switches. Each switch can handle up to 2 million packets/second. Coaxial links can span 100 meters and fiber links can span two kilometers. A 30-switch network with more than 100 hosts is the service network for Digital's Systems Research Center.

Design Decision

This section summarizes the major decisions that characterize the Autonet design. Point-to-Point Links at 100 Mbit/s Ethernet uses a broadcast physical medium. Each packet sent on an Ethernet segment is seen by all hosts attached to the segment. The minimum size of an Ethernet packet is determined by the need to detect collisions between packets.

Reliable collision detection requires that each packet last a minimum time. At high bit rates this time translates into unacceptably large minimum packet sizes. Most 100 Mbit/s and faster networks, including Autonet, use point-to-point links to get away from these limitations. Using point-to-point links also can produce a design that is relatively independent of the specific link technology. As long as a link technology has the needed length, bandwidth, and latency characteristics, then it can be incorporated into the network with appropriate interface electronics.

We settled on 100 Mbit/s for the link bandwidth in Autonet because that speed represents a significant increase over Ethernet, while still being well within the limits of standard signalling technology. We chose the AMD TAXI chip set [3] to drive the links, leaving the subtleties of phase-locked loops and data encoding on the link to others. The overall Autonet design should scale to ten times faster links.

We engineered Autonet to tolerate transmission delays sufficient for fiber optic links up to 2 km in length. The first link we have implemented uses 75 ohm coaxial cable, with full-duplex signalling on a single cable. Electrical considerations limit these coax links to a maximum length of 100 m.

If both link types were implemented they could be mixed in a single installation: coaxial links might be used within a building because of their lower cost; fiber optic links might be used between buildings because of their longer length limit.

Automatic Operation

One of the virtues of Ethernet and FDDI is that in normal operation no management is required to route packets. Even when multiple networks are interconnected with bridges, a distributed algorithm executed by the bridges determines a forwarding pattern to interconnect all segments without introducing loops. The bridge algorithm also automatically reconfigures the forwarding pattern to include new equipment and to avoid broken segments and bridges.

Autonet also operates automatically. This function is provided by software executing on the control processor in each switch that monitors the physical installation. Whenever a switch or link fails, is repaired, is added, or is removed, this software triggers a distributed reconfiguration algorithm. The algorithm adjusts the packet routes to make use of all operational links and switches and to avoid all broken ones. Of course, human network management is still required to repair broken equipment and adjust the physical installation to reflect substantially changed loads.

Deadlock-Free, Multipath Routing

Because Autonet uses flow controlled FIFOs for buffering and does not discard packets in normal operation, deadlock is possible if packets are routed along arbitrary paths. Deadlocks can be dealt with by detecting and breaking them, or by avoiding them. For Autonet we chose the latter approach. Detecting deadlocks reliably and quickly is hard, and discarding an individual packet to break a deadlock complicates the switch hardware. Our scheme uses deadlock-free routes while still allowing packet transmission on all working links. The scheme has the property that it allows multiple paths between a particular source and destination, and takes advantage of links installed as parallel trunks.

Hardware-Supported Broadcast

Because Ethernet naturally supports broadcast, high-level protocols have come to depend upon low-latency broadcast within a LAN. Autonet switch hardware can transmit a packet on multiple output ports simultaneously. This capability is used to implement LAN-wide broadcast with low latency by flooding broadcast packets on a spanning tree of links.

Since a broadcast packet must go everywhere in a network, the aggregate broadcast bandwidth is limited to the link bandwidth. As we found out, supporting broadcast complicates the problem of providing deadlock-free routing. Having low-latency broadcast, however, simplifies the problem of mapping destination UIDs to short addresses.

2.14 OTHER IMPLEMENTED DATA NETWORKS

Metropolitan Area Network

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

One example of a MAN is the MIND Network located in Pasco County, Florida. It connects all of Pasco's media centers to a centralized mainframe at the district office by using dedicated phone lines, coaxial cabling, and wireless communications providers.

Wide Area Network

Wide Area Networks (WANs) connect larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of network. Using a WAN, schools in Florida can communicate with places like Tokyo in a matter of minutes, without paying enormous phone bills. A WAN is complicated. It uses multiplexers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN or a MAN.

CHAPTER THREE

LOCAL AREA NETWORK DESIGN AND MANAGEMENT SYSTEMS

3.1 Overview

Organizations invest significant amounts of time and money in building complex data networks. Rather than a company's dedicating one or more network engineers to maintenance alone, it would be more cost-effective if the system could look out for itself for the most part and, in the process, perform routine tasks for engineer. These arrangements would free the engineers to work on the future developments of the network.

From this need was born the concept of network management. Network management is the process of controlling a complex data network to maximize its efficiency and productivity. To better define the scope of network management, the international organization for standardization (ISO) network management forum divided network management into five functional areas:

- Fault management.
- Configuration management.
- Security management.
- Performance management.
- Accounting management.

3.2 Role of The Network Engineer

Due to the importance of functioning data network, usually one or more network engineers have responsibility for installing, maintaining, and troubleshooting the network. For these technical experts, the solution to a network problem could be as simple as answering a confused user's question or as complicated as identifying and replacing failed or malfunctioning equipment or initiating disaster-recovery procedures following a catastrophic event.

complexity of the network engineer's job increases. Engineers need to know large amount of information about the data network. The sheer volume of this information can quickly become unmanageable, particularly as the network grows and changes. To help the engineers do their jobs, the concept of network management evolved. The overall goal of network management is to help network engineers deal with the complexity of a data network and to make sure that data can go across it with maximum efficiency and transparency to the user.

3.3 Network Management

Network management means different things to different people. In some cases, it involves a solitary network consultant monitoring network activity with an outdated protocol analyzer. In other cases, network management involves a distributed database, autpolling of network devices, and high-end workstations generating real-time graphical views of network topology changes and traffic. In general, network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks.

3.4 Local Area Network Management

This document discusses the tasks associated with management of Local Area Networks (LANs). All LANs require regular administration and management in order to function efficiently and effectively. A Network Administrator is required to perform a range of duties in order to achieve this efficiency and effectiveness. These include maintaining system security, implementing backup strategies, installing software, upgrading software, managing data storage and ensuring provision of virus protection.

3.5 NETWORK MANAGEMENT FUNCTIONS

The international organization for standardization (ISO) network management as mentioned above divided network functions into Fault, configuration, security,

performance, and accounting.

3.5.1 Fault Management

Fault management is a process of locating problems, or faults; on the data network. it involves the following.

- 1- discover the problem.
- 2- Isolate the problem.
- 3- Fix the problem (if possible).

Using fault management techniques, the network engineer can locate and solve problems more quickly than could be done without them.

For example, in a typical setup a user logs into a remote system by way of several network devices, suddenly the connection drops. The user reports the problem to you, the network engineer. you would begin by isolating the problem. Without an effective fault management tool, you first would want to determine whether the problem results from user error, such as entering an invalid command or trying to access an unreachable system. If you find no user errors, you would have to check each device between the user and the remote system, beginning with the device closest to the user. Let's say that you find no connectivity on this first device, as shown in fig. 3.1.

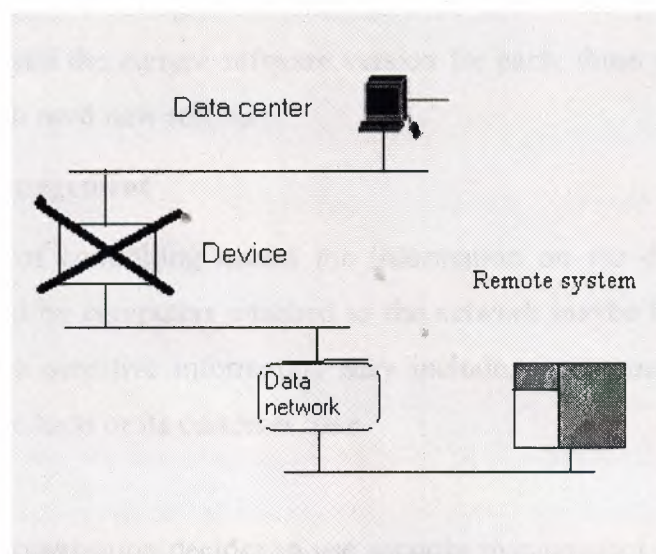


Fig 3.1: Fault Management

Entering the data center, you find that all the lights on the device are off. Investigating further, you notice signs of construction in the area and that the plug for the device is on the floor. You conclude that someone must have unplugged the device accidentally.

After reinserting the plug, this time into a wall outlet away from the construction area, you then would verify that the device now is working normally.

With the aid of a fault management tool, you could have isolated the problem much more quickly. In fact, such a tool might have enabled you to isolate and fix the problem before the user report it.

3.5.2 Configuration Management

The configuration of certain network devices control the behavior of the data network. Configuration management is the process of finding and setting up (Configuring) these critical devices.

Assume that a quirk in version A of the software in an ethernet bridge is causing network performance problems. To fix the anomaly, the bridge manufacturer has released a software upgrade, version B, that will require your installation new firmware in each of the 100 bridges on the network. Accordingly, you have planned the phased deployment to bring all the bridges on the network to version B, first, however, you would need to determine the current software version installed at each bridge. But lacking an effective configuration management tool, you would have to physically inspect each bridge. A configuration management tool could provide a list of all bridges, showing you the current software version for each, thus making it easier for you to locate which need new software.

3.5.3 Security Management

It is the process of controlling access to the information on the data network. Some information stored by computers attached to the network maybe inappropriate for all users to view. Such sensitive information may include, for example, details about a company's new products or its customer base.

Suppose that an organization decides to use security management techniques to allow remote access to its network through dialup lines on a terminal server for a group of engineers. Once engineers connect to the terminal server, they can log in to their computer to do their work.

After a few weeks, the administrator of one of the payroll computers on the network comes to you with a report showing many unsuccessful remote login attempts originating from the terminal server used by the engineers. The terminal server does allow access to any computer on the network leaving the destination host security preventing the access to sensitive information. Thus no engineers have gained access to the payroll computer, but the mere fact that someone is trying is a security concern.

Your first step may be to use a configuration management tool to limit the computer's accessibility from the terminal server. However, to discover who is attempting to gain access to this payroll computer, you will have to periodically log in to the terminal server and record which engineers are using it. Ideally, you can correlate the times at which the unsuccessful remote login attempts are being made with who is logged in on the terminal server. Security management would give you a way to monitor the access points on the terminal server and record which engineers is using the device on a periodic basis.

Security management also could provide you with audit trails and sound alarms to alert you of potential security breaches.

Network Security

There are two forms of security:

1. Physical security (to avoid theft, fire, water and wilful physical damage).
2. Data security (to avoid loss / corruption of data and applications and to maintain privacy).

1-Physical Security

It is important to store vital network components such as servers, hubs and routers in secure locations such as a strongroom. Most of this equipment needs little or no administration and should be safely stored to avoid theft or damage from fire. Components such as cabling should be concealed in conduit wherever possible and should not be easily visible when run outside buildings. Similarly, components such as main power switchboards should always be kept locked.

2-Data Security

If data security has not been investigated thoroughly before configuring the system, difficulties and frustrations may arise. A system could be developed so it is easy to "break" into through a very lax security framework, allowing students to access parts of the system and cause data damage. On the other hand, it could be too difficult to navigate because of the overuse of passwords and tight restrictions. Effective data security involves the allocation of trustee rights to users or groups of users for specific parts of each server and the allocation of passwords where appropriate. Networkaware menu systems that restrict access to sensitive areas of the system (such as MS-DOS), providing Read-Only access to application areas on the servers and the protection and regular changing of sensitive passwords can ensure effective and secure use of your network system. As a general rule, only allocate each user the minimum rights necessary.

3-Computer Viruses

Computer viruses are a separate concern for network administrators. As these can potentially be devastating to a computer network, it is imperative that measures be taken to avoid infection. The best way to avoid infection is the education of users. Understanding what a virus is and how it spreads, and adopting work practices among users to ensure infection cannot occur is the first step.

Virus protection software is the safety net in case a virus manages to get through good work practices.

Methods of How Viruses Spread

All viruses hide somewhere on a floppy disk or a hard disk. Most viruses fall into the following categories.

1. Boot Sector / Partition Table Viruses

These live in the boot areas of disks and load into memory whenever the computer is booted. They infect each diskette placed in the drive.

2. Executable File Viruses

These attach themselves to executable files (programs) and function whenever the infected program is loaded. They infect other uninfected programs when they are loaded.

3. Multi-Partite Viruses

These viruses are made up of separate components and can be almost undetectable whilst at the same time infecting every file on your computer.

4. Macro Viruses

These are embedded in macros defined within certain word processing documents or spreadsheet files. They are transferred by the sharing of the infected documents.

5. How to Avoid Viruses

Viruses are getting “smarter” everyday, becoming harder to detect and there are thousands of different viruses in circulation. It is almost impossible to totally avoid viruses however, these suggestions should help.

1. Ensure that complete and regular backups are maintained for all computer systems.
2. Use an up-to-date virus scanning program on both file servers and workstations.
3. Be wary of all disks that have come from external sources (even from home).
4. Do NOT participate in copyright infringement.
5. Write-protect all original program diskettes before using them.
6. Install virus scanning software that automatically scans for viruses.

3.5.4 Performance Management

Performance management involves measuring the performance of hardware, software, and media. Examples of measured activities are overall throughput, percentage utilization, error rates, and response time. Using performance management information, the engineer can ensure that the network will have the capacity to accommodate the users' needs.

Suppose that a user complains about poor file transfer performance to a site across the network. Without a performance management tool, you would first have to look for

network faults. If you find no fault, your next step would be to evaluate the performance of each link and device between the user's terminal and the destination across the network. During your investigation, you might discover that the average utilization of one link is very close to its capacity. You might then decide that the solution to the file transfer performance problem is to upgrade the current link or to install a new one to add capacity. If a performance management tool had been available, you might have been able to detect early on that the link was nearing capacity, perhaps even before the performance was impacted.

3.5.5 Accounting Management

Accounting management involves tracking each individual and group user's utilization of network resources to better ensure that users have sufficient resources. It also involves granting or removing permission for access to the network.

Suppose that you need to upgrade a department file server's network interface because it reached its packet-processing capacity. Without an accounting management tool, you would not know which users have clients that access the file server. Thus you ask the users to see who has client computers that access the file server on a regular basis. As a result of your investigation, you discover that the departmental documentation group has many clients who use a desktop publishing system on the file server. After some rudimentary analysis, you conclude that this traffic contributes nearly half of the load on the file server's network interface.

You might decide that giving this documentation group its own file server would alleviate a large amount of the network traffic that this interface card has to handle, removing the need to upgrade the interface card and allowing the rest of the department to remain unchanged. Further, you might decide to locate the new file server on the same network segment as the documentation group, which could reduce network traffic throughout the department. With an accounting management tool, however, you would quickly learn that the documentation group accesses the file server with many clients on a regular basis-so you would have been able to handle the situation sooner.

3.6 THE NETWORK MANAGEMENT SYSTEM

3.6.1 The Network Management Platform

Historically network management revolved around multiple systems, each managing one specific set of components on the data network. A typical network management center could have a separate system for managing modems, multiplexers, hubs, bridges, routers, and other types of network components. Restrictions of money, physical space, and technical expertise all led to the desire to have the network components managed by a single system that would also show their interconnections on a network map. Out of this need came the network management platform.

A network management platform is a software package that provides the basic functionality of network management for many different network components. The goal of the network management platform is to provide generic functionality for managing a variety of network devices (see Fig. 3.2). This basic functionality includes.

1. A graphical user interface (GUI).
2. A network map.
3. A database management system (DBMS).
4. A standard method to query devices.
5. A customizable menu system.
6. An event log.

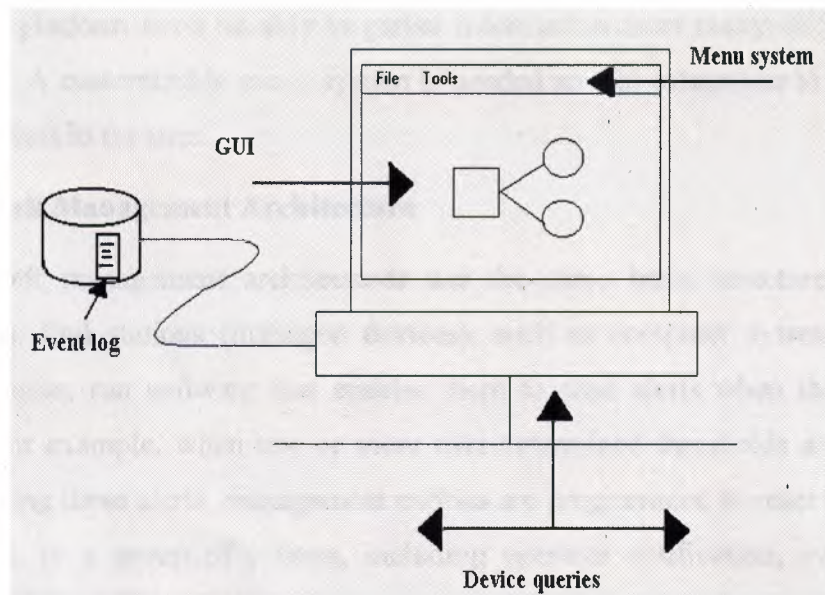


Fig 3.2 The basic components of a network management platform.

The GUI is useful for a variety of reasons, including giving the user easier access to the features of the platform. The GUI should conform to a common look-and-feel standard, such as Microsoft Windows, OSF Motif, or Sun Microsystems Openwork. By using a standard GUI, the platform will behave in a manner that is documented and conformed to by different vendors.

As we will discuss in the next section, the overall network management system will most likely comprise a platform and applications from a variety of vendors. If all vendors build their applications using a common look and feel, it makes the system easier to use and manipulate.

The map is useful for nearly every area of network management. Fault management tools can help isolate the cause of the fault, using colors on the map. Configuration management tools can show the physical and logical configuration of the network pictorially. Performance management tools can graphically show the current performance of devices and links by color or different pictures. If the network management platform provides a way to automatically discover the devices in the network (called auto discovery) and then draw the network graphically (called auto mapping), this is an added benefit. The standard method to query devices is essential

because the platform must be able to gather information from many different vendor components. A customizable menu system is needed so that extensions to the platform appear seamless to the user.

3.6.2 Network Management Architecture

Most network management architectures use the same basic structure and set of relationships. End stations (managed devices), such as computer systems and other network devices, run software that enables them to send alerts when they recognize problems (for example, when one or more user-determined thresholds are exceeded). Upon receiving these alerts, management entities are programmed to react by executing one, several, or a group of actions, including operator notification, event logging, system shutdown, and automatic attempts at system repair.

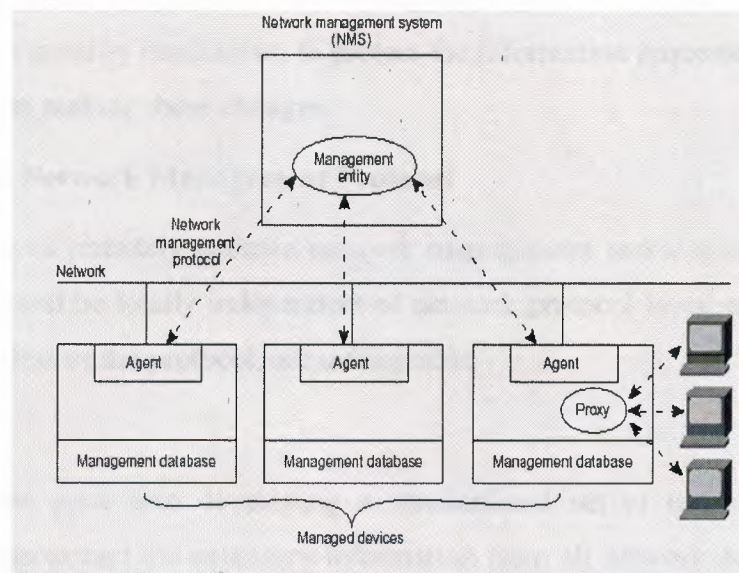


Figure 3.3: A Typical Network Management Architecture Maintains Many Relationships

Management entities also can poll end stations to check the values of certain variables. Polling can be automatic or user-initiated, but agents in the managed devices respond to all polls. Agents are software modules that first compile information about the managed devices in which they reside, then store this information in a management database, and finally provide it (proactively or reactively) to management entities within network management systems (NMSs) via a network management protocol. Well-known network management protocols include the Simple Network Management Protocol

(SNMP) and Common Management Information Protocol (CMIP). Management proxies are entities that provide management information on behalf of other entities. Figure 6-1 depicts a typical network management architecture.

3.7 Network Management Protocols

An essential factor in achieving the goals of network management is the ability to acquire information from and effect change to network devices.

Likewise, the requirements in network management protocols could fall into those categories.

A Simple Network Management Protocol

Would define common data formats and parameters and allow for easy retrieval of information. A more complex network management protocol would add some change capability and a security mechanism to protect the information requested and to prevent just anyone from making these changes.

-An Advanced Network Management Protocol

Would be able to remotely execute network management tasks, similar to a remote procedure call, and be totally independent of network protocol layer, so all networking devices, regardless of the protocol, are manageable.

Much work has gone into developing a standardized set of network management protocols to help extract the necessary information from all network devices. The most common network management protocols are SNMP (Simple Network Management Protocol) and whenever SNMPV2 (version 2) and CMIS/CMIP (Common Management Information Services/common Management Information Protocol). A quick answer is that SNMP is a bit beyond the simple tool, with adequate monitoring capabilities and some change capabilities. SNMPV2 greatly enhances the SNMP feature set. CMIS/CMIP approaches the advanced tool, but implementation issues have limited its use. The bounded nature of the standard network management protocols today is a key point in the development of network management applications.

3.8 INTERNET PROTOCOLS

3.8.1 Network Protocol

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

3.8.2 Network Subnets

Although the individual subscribers do not need to tabulate network numbers or provide explicit routing, it is convenient for most Class B networks to be internally managed as a much smaller and simpler version of the larger network organizations. It is common to subdivide the two bytes available for internal assignment into a one byte department number and a one byte workstation ID.

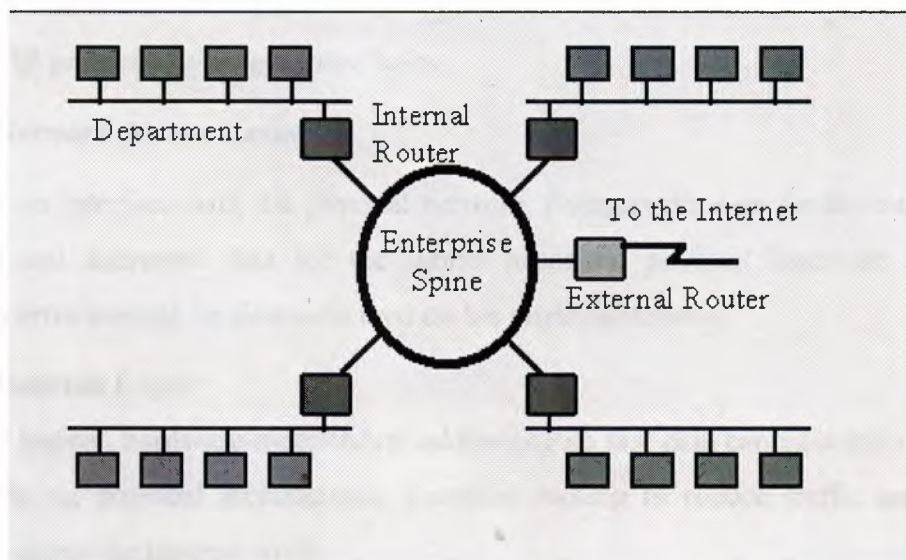


Fig 3.4: Network Subnet

The enterprise network is built using commercially available TCP/IP router boxes. Each router has small tables with 255 entries to translate the one byte department number into selection of a destination Ethernet connected to one of the routers. Messages to the PC Lube and Tune server (130.132.59.234) are sent through the national and New England regional networks based on the 130.132 part of the number. Arriving at Yale, the 59 department ID selects an Ethernet connector in the C& IS building. The 234 selects a particular workstation on that LAN. The Yale network must be updated as new

Ethernets and departments are added, but it is not effected by changes outside the university or the movement of machines within the department.

3.8.3 The TCP/IP

TCP/IP is a set of protocols developed to allow cooperating computers to share resources across a network. It was developed by a community of researchers centered around the ARPAnet. Certainly the ARPAnet is the best-known TCP/IP network. However as of June, 87, at least 130 different vendors had products that support TCP/IP, and thousands of networks of all kinds use it.

3.8.4 THE TCP/IP LAYERS

The TCP/IP protocol system or can be called as network protocol suit- is subdivided into layered components that each perform specific duties, these layers contain protocols that are used by the TCP/IP together, as one mechanismic operation,see fig, the TCP/IP protocol layers are listed below.

3.8.4.1 Network Access Layer

Provides an interface with the physical network. Formats the data for the transmission medium and addresses data for the subnet based on physical hardware addresses. Provides error control for data delivered on the physical network.

3.8.4.2 Internet Layer

Provides logical, hardware-independent addressing so that data can pass among subnets with differing physical architectures. Provides routing to reduce traffic and support delivery across the internet work.

3.8.4.3 Transport Layer

Provides flow control, error control, and acknowledgment services for the internet work, and Serves as an interface for network applications.

3.8.4.4 Application Layer

Provides applications for network troubleshooting, file transfer, remote control, and Internet activities. Also supports the network Application Programming Interfaces (APIs) that enable programs written for a particular operating environment to access the network.

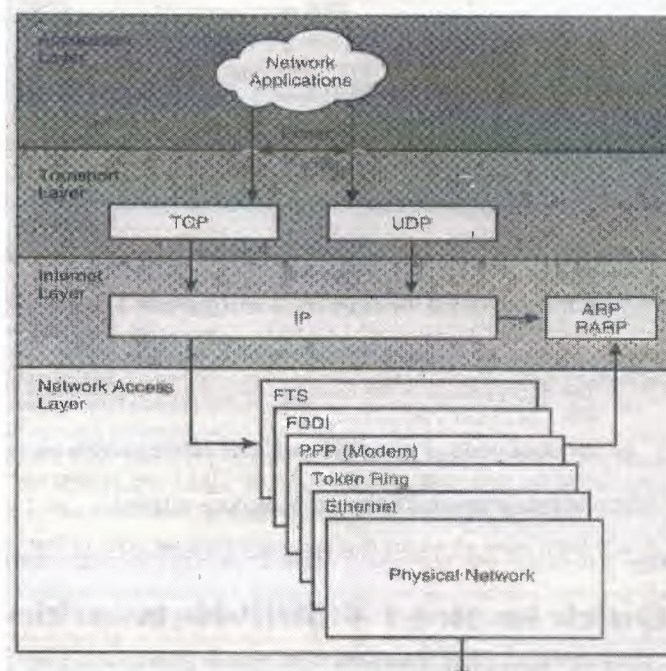


Fig 3.5: The TCP/IP Model

NOTE: The protocols below are the most important and the most used TCP/IP protocols, as we all know that it is a very huge and wide subject.

3.8.5 The Network Access Layer

3.8.5.1 Ethernet

The Ethernet protocol is by far the most widely used. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already

transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.

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

3.8.5.2 Fast Ethernet

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

3.8.5.3 Gigabit Ethernet

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

3.8.5.4 Token Ring

In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at

transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring in school environments has decreased.

3.8.5.5 FDDI

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

3.8.5.6 ATM

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

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

3.8.6 The Internet Layer

3.8.6.1 Internet Protocol (IP)

The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols.

IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork; and providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes.

IP Addressing

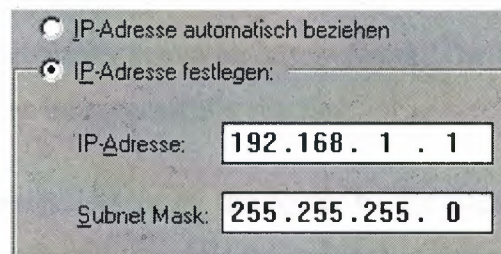
As with any other network-layer protocol, the IP addressing scheme is integral to the process of routing IP datagrams through an internetwork. Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for subnetworks.

Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts. The network number and the host number. The network number identifies a network and must be assigned by the Internet Network Information Center (InterNIC) if the network is to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the InterNIC and can itself assign address space as necessary. The host number identifies a host on a network and is assigned by the local network administrator.

IP Address Format

The 32-bit IP address is grouped eight bits at a time, separated by dots, and represented in decimal format (known as dotted decimal notation). Each bit in the octet has a binary weight (128, 64, 32, 16, 8, 4, 2, 1).

The minimum value for an octet is 0, and the maximum value for an octet is 255.



The image shows a screenshot of a network configuration window. At the top, there are two radio buttons: 'IP-Adresse automatisch beziehen' (unselected) and 'IP-Adresse festlegen:' (selected). Below the selected option, there are two input fields. The first is labeled 'IP-Adresse:' and contains the text '192.168.1.1'. The second is labeled 'Subnet Mask:' and contains the text '255.255.255.0'.

Figure 3.6: Illustrates the Basic Format of an IP Address.

3.8.6.2 Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is a internet-layer protocol that provides message packets to report errors and other information regarding IP packet processing back to the source. ICMP is documented in RFC 792.

ICMP Messages

ICMPs generate several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement and Router Solicitation. If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages.

When an ICMP destination-unreachable message is sent by a router, it means that the router is unable to send the package to its final destination. The router then discards the original packet. Two reasons exist for why a destination might be unreachable. Most commonly, the source host has specified a nonexistent address. Less frequently, the router does not have a route to the destination.

Destination-unreachable messages include four basic types: network unreachable, host unreachable, protocol unreachable, and port unreachable. Network-unreachable messages usually mean that a failure has occurred in the routing or addressing of a packet. Host-unreachable messages usually indicates delivery failure, such as a wrong subnet mask. Protocol-unreachable messages generally mean that the destination does not support the upper-layer protocol specified in the packet. Port-unreachable messages imply that the TCP socket or port is not available.

An ICMP echo-request message, which is generated by the ping command, is sent by any host to test node reachability across an internetwork. The ICMP echo-reply message indicates that the node can be successfully reached.

An ICMP Redirect message is sent by the router to the source host to stimulate more efficient routing. The router still forwards the original packet to the destination.

ICMP redirects allow host routing tables to remain small because it is necessary to know the address of only one router, even if that router does not provide the best path. Even after receiving an ICMP Redirect message, some devices might continue using the less-efficient route.

An ICMP Time-exceeded message is sent by the router if an IP packet's Time-to-Live field (expressed in hops or seconds) reaches zero. The Time-to-Live field prevents packets from continuously circulating the internetwork if the internetwork contains a routing loop. The router then discards the original packet.

3.8.6.3 Routing Internet Protocol (RIP)

RIP works well in small environments but has serious limitations when used in larger internetworks. For example, RIP limits the number of router hops between any two hosts in an internet to 16. RIP is also slow to converge, meaning that it takes a relatively long time for network changes to become known to all routers. Finally, RIP determines the best path through an internet by looking only at the number of hops between the two end nodes. This technique ignores differences in line speed, line utilization, and all other metrics, many of which can be important factors in choosing the best path between two nodes. For this reason, many companies with large internets are migrating away from RIP to more sophisticated routing protocols.

3.8.7 Transport Layer

3.8.7.1 Transmission Control Protocol (TCP)

The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.

With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers. This service benefits applications because they do not have to chop data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery.

TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. Bytes not acknowledged within a specified time period are retransmitted. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission. TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence number it can receive without overflowing its internal

buffers. Full-duplex operation means that TCP processes can both send and receive at the same time.

Finally, TCP's multiplexing means that numerous simultaneous upper-layer conversations can be multiplexed over a single connection.

TCP Connection Establishment

To use reliable transport services, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using a "three-way handshake" mechanism.

A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well. This is necessary so that packets are not transmitted or retransmitted during session establishment or after session termination.

Each host randomly chooses a sequence number used to track bytes within the stream it is sending and receiving. Then, the three-way handshake proceeds in the following manner. The first host (Host A) initiates a connection by sending a packet with the initial sequence number (X) and SYN bit set to indicate a connection request.

The second host (Host B) receives the SYN, records the sequence number X, and replies by acknowledging the SYN (with an $ACK = X + 1$). Host B includes its own initial sequence number ($SEQ = Y$). An $ACK = 20$ means the host has received bytes 0 through 19 and expects byte 20 next. This technique is called forward acknowledgment. Host A then acknowledges all bytes Host B sent with a forward acknowledgment indicating the next byte Host A expects to receive ($ACK = Y + 1$). Data transfer then can begin.

3.8.7.2 User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless transport-layer protocol (Layer 4) that belongs to the Internet protocol family. UDP is basically an interface between IP and upper-layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another.

Unlike the TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP. Because of UDP's simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP. UDP is useful in situations where the reliability mechanisms of TCP are not necessary, such as in cases where a higher-layer protocol might provide error and flow control.

UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Trivial File Transfer Protocol (TFTP).

3.8.8 The Application Layer

3.8.8.1 File Transfer Protocol(FTP)

The file transfer protocol (FTP) allows a user on any computer to get files from another computer, or to send files to another computer. Security is handled by requiring the user to specify a user name and password for the other computer. Provisions are made for handling file transfer between machines with different character set, end of line conventions, etc. This is not quite the same thing as more recent "network file system" or "netbios" protocols, which will be described below. Rather, FTP is a utility that you run any time you want to access a file on another system. You use it to copy the file to your own system. You then work with the local copy. (See RFC 959 for specifications for FTP.)

3.8.8.2 Hypertext Transfer Protocol (HTTP)

Web servers and browsers communicate using the Hypertext Transfer Protocol. The purpose of HTTP is to support the transfer of HTML documents. HTTP is an application-level protocol. The HTTP client and server applications use the reliable atcpa transport protocol to establish a connection.

HTTP has the following duties.

1. To establish a connection between the browser (the client) and the server.
2. To negotiate settings and establish parameters for the session.
3. To provide for the orderly transfer of HTML content.
4. To close the connection with the server.

Although the nature of Web communication has become extremely complex, most of that complexity relates to how the server builds the HTML content and what the browser does with the content it receives. The actual process of transferring the content through HTML is relatively uncluttered.

CONCLUSION

Network management protocols allow a manager to monitor and control gateways and hosts. A network management client program executing on the manager's workstation contacts one or more servers running on the computers to be controlled. Because an internet consists of heterogeneous machines and networks, TCP/IP management software executes as application programs and uses internet transport protocols (e.g., UDP) for communication between clients and servers.

The TCP/IP protocol suite has two co-recommended draft standard network management protocols: CMOT and SNMP. CMOT uses the ISO CMIS/CMIP protocols over a TCP connection. SNMP defines a simple management protocol that provides two basic operations: fetch a value from a variable or store a value into a variable. In SNMP, all operations occur as side-effects of storing values into variables.

Initially, both SNMP and CMOT used a common definition of variables to be controlled. The set of variables was known as the common Management Information Base, or MIB. MIB variables are described using ASN.1, a formal language that provides a concise encoded form as well as a precise human-readable notation for names and objects. ASN.1 uses a hierarchical namespace to guarantee that all MIB names are globally unique while still allowing subgroups to assign parts of the namespace. Recently, the two groups have each proposed their own MIB extensions.

REFERENCES

- [1] http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/
- [2] <http://www.wlana.org/>
- [3] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212495,00.html
- [4] Network and System Integration for Dummies (With CD-ROM) Author: Michael
- [5] Practical Storage Area Networking by Dan Pollack, Daniel Pollack
- [6] TCP/IP Illustrated 3 Volume Set by W. Richard Stevens, et al (Hardcover)
- [7] Business Data Networks and Telecommunications (4th Edition) by Raymond R. Panko
- [8] Mastering Network Security by Chris Brenton, Cameron Hunt
- [9] Designing Storage Area Networks Author: Tom Clark, Thomas Clark
Computer Networks, Fourth Edition by Andrew S. Tanenbaum;
- [10] Communications Systems and Networks Author: Ray Horak, Mark A. Miller
(Editor), Harry Newton