COMPUTER NETWORKS IN DATA COMMUNICATION

BY

ADEGBEHINGBE EMMANUEL

87/750

A THESIS SUBMITTED TO THE DEPARTMENT OF MATHEMATICS/ COMPUTER SCIENCE, FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE: BACHELOR OF TECHNOLOGY (HONOURS) IN MATHEMATICS / COMPUTER SCIENCE.

SEPTEMBER 1992.

DEDICATION

THIS THESIS IS DEDEICATED TO MY GRANDMOTHER; LATE MRS MARYAM ADEGBEHINGBE.

CERTIFICATION

I hereby certify that I have supervised, read and approved this project work which I found to be adequate in scope and guality for the partial fulfilment of the award of a Bachelor's Degree in Mathematics / Computer science (B.Tech)

MR. T. BANKEFA
Project Supervisor

Date

MR. T. BANKEFA
H.O.D Maths / Computer Sc.

Date

External Examiner
A.D. AKINDÉ

15-10-92
Date

ACKNOWLEDGEMENT

I want to express my appreciation to MR. T. Bankefa for his invaluable counsel and his numerous contributions towards the succesful completion of my project.

My brother, Architect Dola Akeredolu, was an ardent cheer leader, supporter, and friend throughout the project. His contributions show in many subtle ways and were indeed instrumental in achieving the final result.

The staff at National oil, Marina, Lagos was instrumental in the development of this project. Miss Amaka, Mr. Ladi Cole, and Mr Okunade were actively involved throughout the course of the project.

I would also acknowledge the contribution of my parents Mr. and Mrs Adegbehingbe for their support. I would also express my thanks to Mr. and Mrs Apalowo, Mr. and Mrs Gbadamosi, and Mr. Femi Ogunleye. And a very special thanks to Messrs Jegede Femi and Awoniyi Tunji for their counsel.

The task of writting this project requires cooperation, contribution and sacrifice in part of numerous indivduals.I wish to express my deep gratitude to the following people, Adebanjo Adebayo, Akinbode Akinwale, Akinnadeju Oludele, Onipede Dare, Bash Idris, Akinbode Akinbayo, Femi Ojo, Akpan, Akerele Tola, Jagunna Wale, Thompson Bamisebi, Awosanya kemi, Idowu Ronke, Bunmi Egberongbe, Toyin Adewumi, Ogundare Sunday, Atubu Emmanual and my dearest brothers Adetona Adebayo and Tokunbo Adeoba.

ABSTRACT

This project is designed to provide the background knowledge required for the study of computer information systems, and to introduce the concepts and approaches required for the design and analysis of computer networks. Also the descriptive and analysis treatment of various aspects of network is examined.

Chapters one to three provide an introduction to the basic components of network, such as transmission links, transmission codes, and error checking. Chapter four deals with the ways of sharing a meduim, and the way in which a medium gains access to medium. Chapter five looks at the network routing: the issues involved in supplying the basic network services, while chapter six goes on to describe the interface to such a network services. Chapter seven also goes on to describe how networks can be connected on to another, allowing users to communicate not just within one network, but across several networks.

Chapter eight is devoted to the subject of security in computer networks, because as computers become more pervasive and important,the information that they process and pass from one to another across network become more critical. Chapter nine and ten describe and discuss the implementation and implications of enterprisewide computer networks in an

organisation, and it also goes on to describe the network of the future; the Cableless LAN. In chapter ten, a case study of National OIL and Chemical marketing PLC was used to discuss the impacts of enterprisewide network in an organisation.

TABLE OF CONTENTS

CHAPTER 3

THE BASICS OF DATA COMMUNICATION

CHAPTER 6

NETWORK SERVICE AND INTERFACE

CHAPTER 7

INTERNETWORKING

CHAPTER 7

INTERNETWORKING

CHAPTER 8

SECURITY IN COMPUTER NETWORKS

CHAPTER 9

IMPLEMENTING ENTERPRISEWIDE NETWORKING

CHAPTER 10

IMPLICATIONS OF COMPUTER NETWORKING IN

AN ORGANISATION

(ACASE STUDY OF NATIONAL OIL)

CHAPTER 1

INTRODUCTION TO COMPUTER NETWORKS

Computer networks are general - purpose distributed computer systems. These are systems based on a set of seperate computers that are capable of autonomous operation, linked by a computer networks. General - purpose distributed system are designed to enable the individual computers, of which they are composed, to use shared resources in the network, providing computing facilities that are at least as flexible and widley - applicable as conventional, centralised or ' mainframe' computers. Users of a computer network system are given the impression that they are using a single integrated computing facility, although the computers may be in different locations.

1.1 PROPERTIES OF COMPUTER NETWORK

The properties that distinquish a distributed computer network from other types of multiple computer systems include the hardware or processing logic, the data, the processing mode itself and the operating system. Succinctly put, computer network is characterized by several features:

- a number of general - purpose component,
- physical distribution of resources
- high level operating systems,
- system transparency, and
- co-operative autonomy.

1.1.1 NUMBER OF GENERAL PURPOSE COMPONENTS

Computer networks usually contain a number of general - purpose physical and logical components that can be assigned to specific tasks on a dynamic basics. In this way the system is then able to be be dynamically reconfigured on a short term basic with respect to those resources that provide any specific services rquired by the system at any given time.

For example if the purpose of the system is to provide at service that requires a general - purpose processor, the system must then have a multipilicity of general - purpose processors. This recofiguration or assignment of resources is ususally possible without affecting the operation of those resources which are not directly involved. It is most common in computer networks to deal with symmetric structues that are made up of a number of very simlar general - purpose computers, since the hardware design cost of specialized individual processors for the network is generally prohibitive. Hence identional hardware is often used for each processor, with different software being used to generate the specialization needed for each function. This simplifies the overall network design, since each processor need only to store the program and data needed for its processes rather than the entire program for all processes, and the hardware reproduction cost of the system can be lowered beacuse less memory is needed per processor.

1.1.2 PHYSICAL DISTRIBUTION OR RESOURCES

Computer networks have a physical distribution of system resources which interact through an interconnection network. The essential use in interconnection network is being the establishment of a two- partly protocol to transfar messages. This two party protocol means that the two communicating processor must cooperate to successfully complete the transfer. The term cooperative in this context to denote multiple systems which are designed to achieve a common purpose to serve a single organization or interchange data in an agreed fashion.

1.1.3 HIGH LEVEL OPERATING SYSTEM

Computers networks usually have a set of high level' proceedures to integrate the control of the distributed components. With such a sysyem the individual processors may have their own operating system, but a well defined set of polices govern the integrated operation of the total configuration. Other properties that must charactise the 'system control procedures' are the support of an effective transfer bandwith between the processors in the system, the ability of a processor to continue to operate and effectively utilze its local resources when disconnected from the network and to be easily re-integrated into the system without affecting other operations in progress, and the support of process and processor interactions at a finegrain level where approprate.

Within a distributed networks, the operating system in the processing units should be able to handle a 'communication mointor' a 'communicator supervisor' and an 'input/output interfaces' within the device support communication amongs the units. The communication monitor continue to initiate and terminate communications for processes and passes information to the communicator supervisor. The communication supervisor then verifies the availability of the required network resources, estabilished and abolishes logical networks on existing hardware resources, estabilishes and abolished logical networks request. Finally the 1/0 interface receives and transmits the network data through some kind of transmission medium.

1.1.4 SYSTEM TRANSPARENCY

Ideally any computer network should be totally transparent to its users, in other words, it should not be obvious to a person sitting at a terminal whether the computing facilities being addressed are located within the terminal itself or in some distant processor, nor should he or she be aware of how the communications actually occur.

System transparency is then necessary in a compter network to permit a user to request services by name only. This means that a user must be able to request an action by specifying what is to be done, not be required to specify which physical or logical component is to provide that service.

1.1.5 COOPERATIVE AUTONOMY

There are many different forms of computer networks, all differing in the amount of 'logical coupling' between the units in the system. We use the term coupling to refer to the ammount of cooperation between the different parts of the system in performing some large tasks. True networks must demonstrate cooperative autonomy in the seperation and interaction of both physical and logical resources.

1.2 TYPES OF COMPUTER NETWORKS

To differentiate distributed computer networks, it is possible to distingiush basically two types of networks for interconnecting installations, based initially on the average distance a message must travel in the network. These two structures are usually referred to as a local Area Network and Wide Area Network. It can be noted that the seperation distance is not the only distinquishing feature of the two types of systems. Howevere, most of the other differences can be traced back to the limitations their seperation brings to the physical construction of such systems.

1.2.1. LOCAL AREA NETWORK

A local area network (LAN) is a data communication network that spans a physical limited area and provides high bandwidth communications over an inexpensive medium. Most

LANs rely on a switching communication network that is usually owned by one owner. The major purpose of the LAN is as a data communications system to allow communications between a number of independent computer related devices such as computers, terminal, mass storage devices, printers, plotters, or copying machines.

1.2.2 WIDE AREA NETWORK

The second category of distributed network is the long distance or wide Area Network (WAN). It usually relies on public communication carries (such as telephone lines). This type of network is operated as a public utility for its subscribers, providing services such as a voice, data, video. Computer systems based on long distance networks tend to consist of highly autonomous computers that only communicate intrequenthy.

CHAPTER 2

INTRODUCTION TO DATA COMMUNICATION

Data communication allows computer systems to communicate not only locally but also over great distances with other remote devices via telephone networks, dedicated networks and private networks.

This means that for example, that a computer terminal in London can communicate with a host computer in lagos as long as they are compatible. (see figire 2.1)

2.1 HISTORY

In the early days of data transfer, data was punched onto a batch of cards, then batch processed. This type of system required a lot of preparation by the operator as each card as to puched and then transported to the host computer to be stored. This is a very time - consuming task.

An alternative methods was introduced that stored the data on papertape or a cassette. This process was also inefficient as the data still had to be transported to, and placed on the host computer resulting in the host computer never totally up to date.

Todays form of data communication solves this problem by transmitting data between the host computer and its remote terminals in real time. Another advantage of having a direct connection is that the operator has less handling to perform, therefore it is no longer necessary for an operator to constantly stay at his terminal in order to transmit data. (see figure 2.2).

2.2 TYPES OF DATA COMMUNICATION

Generally there are two basic types of data communication systems

- Interactive,
- Non-interactive.

2.2.1 INTERACTIVE

Interactive systems are used where an immediate response or action is necessary. Examples of this type include word processing system, databases e.t.c.

2.2.2 NON - INTERACTIVE

This type of communication is used when an immediate response is not feasible. Examples include telex systems and devices that transfer their data to a host computer for storage purposes.

2.3 EXAMPLES OF DATA COMMUNICATION SYSTEMS

There is a multitude of data communication techniques, some are discused below.

2.3.1 Data communication using A Dedicted Data Networks

This involes data communication between devices using a dedicated data networks. A company contains a number of departments performing differing functions, yet each

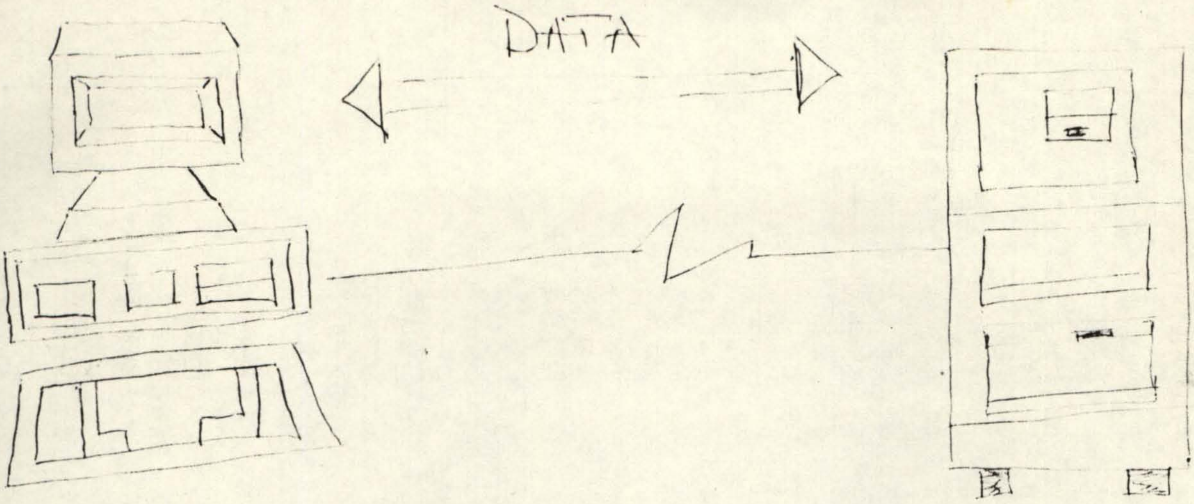


Figure 2.2 Current Data Communication

requires some form of computing facility that includes, in certain caces, access to information contained in other departments.

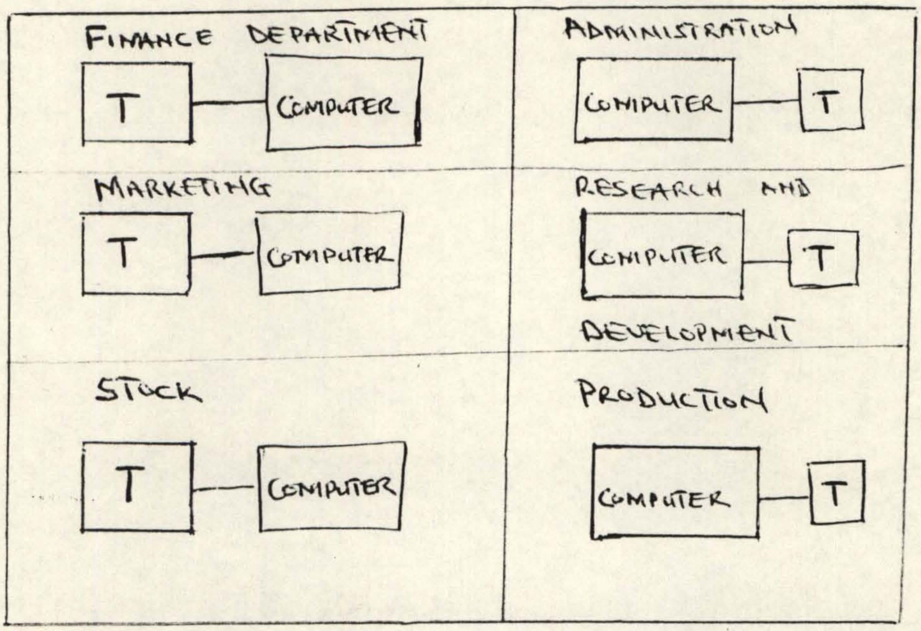
One way of providing this facility is to install a computer in each department (see figure 2.3), however, the biggest disadvantage of this method other than the enormous cost, is that other departments are not able to access any information that they might require.

The second way, that sovles both the cost and access problems, is to install a central computer and have connections to each department via remote terminals (see figure 2.4). Using this method all of the data concerning the company is centralised in one system making it not only accessible to each department but also easy to update.

2.3.2 DATA COMMUNICATION USING TELEX NETWORK

The fuction of the Telex Network is to provide communication in textual format. The telex network transfers the data in a character-by-character basis.

It is an example of non-interactive communication as the transmitting device is usually not provided with any indication from the receiving device as to whether the transmitted data has arrieved. Also compared with other forms of data communication, are the relatively show operating speed.



T = TERMINAL

Figure 2·3 Company With A Computer In Every Department.

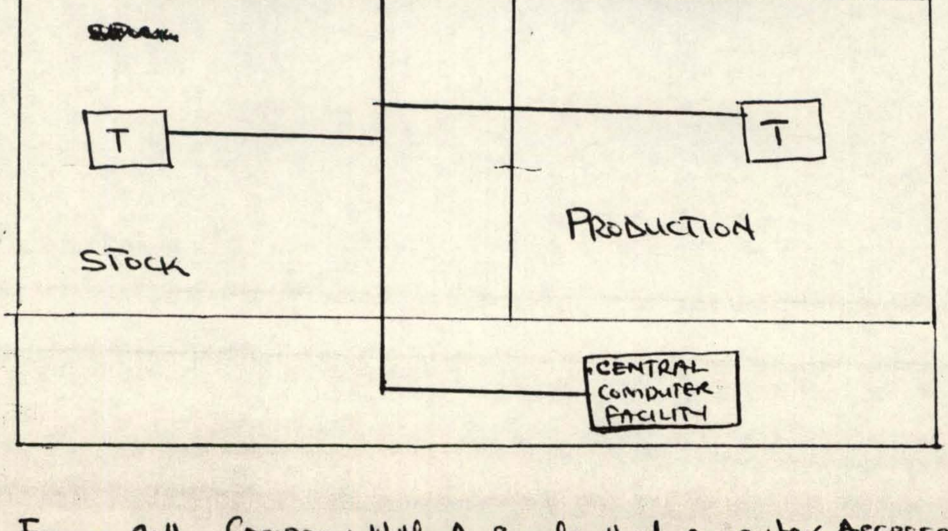


Figure 2·4 Company With A Single Host Computer Accessed Via Terminals, located in Each Department

2.3.3 DATA COMMUNICATION USING THE TELEPHONE NETWORK

The telephone network is like the telex network as it is a worldwide facility comprised of a number of interconnected networks. However, that is where the comparison ends as it is not only much larger but also more versatile than its telex counter part.

The main disadvantage of the telphone network, when compared with a dedicated data network is that it was not originally designed to perform data communication but has been adapoted to do so with the aid of an especially designed piece of equipment known as MODEM. This converts the digit output from a computer system into an analogue signal (and vice-versa) that can be transfered over telephone lines.

An example where the telephone network can be used to good advantage for data communication purposees is given below; Assume that a journalist is on location in London reporting for his newspaper on an important event in Lagos. If it is to make the next edition of the newspaper, the journalist must contact his office and provide them with a story, either by dictating the rlevant facts over the telephone or by using the telephone data communication facility. The lather, and more efficient methods is only possible if the journalist is equipped with a portable word processor and an Acoustic MODEM, and if there is access to a standard telephone set. If this is the case, once the story is completed on the word processor it can be transmitted to the newspapers computer system via the telephone line,where it will be recieved in its original format. (see figure 2.5).

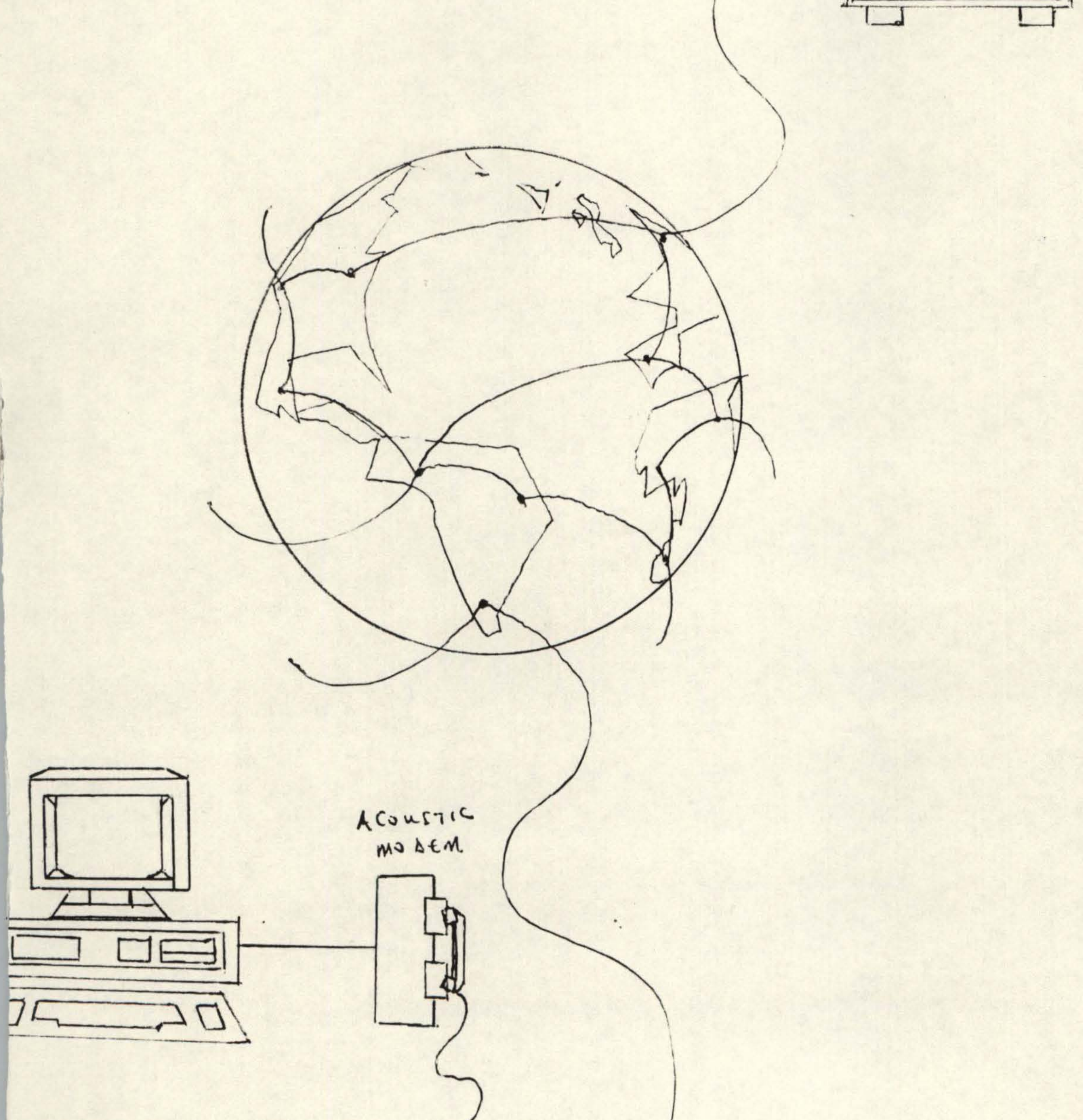


Figure 2.5.1 An Example of Data Communication Making Use of the Telephone Network

CHAPTER 3

THE BASICS OF DATA COMMUNICATION

This chapter will provide an introduction to the basic elements that comprise a functional communication link.

3.1 THE COMMUNICATION LINK

The basic link is that between the communication devices connected via a transmission line (see figure 3.1). This line consists of a single wire and, as such can only transmit data one element at a time. A computer station always output data in a parallel format, normally a 5,6,7, or 8 bit code. To succesfully transimit data, it has to be converted into serial bit stream.

It is important to note that a communicating Devices is commonly known as DTE (DATA TERMINAL EQUIPMENT) and where applicable, will be referred to as such throughout the rest of this project.

Transmission lines only transmit analogue signals, as the output from the Data Communication Controller is the form of a digital signal. It is therefore, necessary to convert this signal into its equivalent analogue format.

This conversion function is performed by the equipment known as the MODEM or DCE (DATA CIRCUIT - TERMINATION EQUIPMENT). The name MODEM is derived from the terms MODulation and DEModulation.

Modulation is the process of converting a digital signal into its analogue equivalent, and Demodulation, the process of converting an analogue signal into its digital equipment.

3.2 TRANSMISSION CODES

The communication between computers and human beings is by means of characters that are esembled into text of some sort.

Data communication provides an operational interfaces between two remote stations. The data exchanged by these two stations can be divided into two groups;

- Data characters
- Control chatracters

To successfully transmit data it has to be converted into unique bit combination that recognised, and can be divided by the receiving station. This unique bit combination is more commonly known as the transimission code.

Figure 3.2 shows the ASC11 character set. The letters 'ASCII' stand for the American Standard Code for Information Interchange. There are many other national and international codes that are either identical to ASC11, or are very close and differ only in the representation of a few graphic symbols. There are also others, such as 150 - 8859 - 1 that are more extensive.

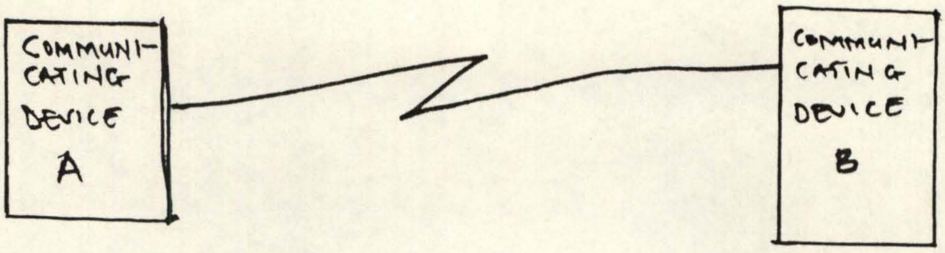


FIGURE 3·1 TRANSMISSION LINE

		0	1	2	3	4	5	6	7
0	0	NULL	DEL		0	@	P	\	p
1	1	SOH	DC1	!	1	A	Q	a	q
2	2	STX	OC2	"	2	B	R	b	r
3	3	ETX	DC3	#	3	C	S	c	s
4	4	EOT	DC4	$	4	D	T	d	t
5	5	ENQ	NAK	%	5	E	u	e	u
6	6	ACK	SYN	&	6	F	V	f	v
7	7	BEL	ETB	'	7	G	W	g	w
8	8	BS	CAN	(	8	H	X	h	x
9	9	HT	EM	)	9	I	Y	i	y
10	A	LF	SUB	*	:	J	Z	j	z
11	B	VT	ESC	+	;	K	[	K	{
12	C	FF	FS	+	<	L	\	L	/
13	D	CR	GS	-	=	M	]	M	}
14	E	SO	RS	•	>	N	^	n	~
15	F	SI	US	/	?	O	_	o	DEL

Figure 3·2 The ASCII Character Set

We can see from figure 3.2 that there are 128 characters arranged in eight columns of 16. The columes are numbered 0 to 7 from left to right, and the rows 0 to 15 from top to bottom. To find the binary representation of a particular character, we multiply the column number by 16 and add the row of the 4th colume. 4 * 16 + 11 = 75 (decimal) = 1001011 (binary).

There are 94 printable characters, plus the space character, in columes 2 to 7. These are the ones with single character entry in the table. The 33 locations that do not represent printable characters are called control characters. The control characters are codes that are reserved for special functions.

Another important feature of the ASC11 character set is its use of only half the availabe values #00 to # 7f. Characters are usually represented in a bytes, giving 256 possible values. The other are values from #80 to #ff are not allowed. Fundamentally ASC11 uses a seven - bit code, the 8bit, #80, is used as a parity bit. The function is for error checking, the idea of parity is to make the number of bits in an eight-bit byte even. Thus, our character "k" has the Y - bit binary pattern 1001011. This has 4 one bits, and thus the number is already even, so the parity bit is 0, and the full eight bit pattern is 01001011. On the other hand, "L" has the pattern 1001100, this has three one bits, and so the parity bits must be 1 to make the representation even parity; 11001100.

The use of this is that, if transmission errors occurs, they will affect individual isolated bits. If an eight - bit byte is received and an error has currupted one bit of the data, then the parity will be wrong, and the character will be rejected as an error.

3.3 TRANSMISSION METHODS

Data can be transfered using either of the following methods

- Asynchronous Transmission
- Synchronous Transmission

3.3.1 ASYNCHRONOUS TRANSMISSION

The data to be transmitted is clocked out of the reqister by the internal clock circuit of the transmitting device and into DCE where it is modulated before being placed on the transmission line. (see figure 3.3). On arrival at the recieving DCE, the data is demodulated then passed to the DTE. The DTE then clocks the received data into the shift register. However, before the data can be clocked in the clock circuit of the receiving DTE must be initialized. The initialization is a function of the transmitted data, or more correctly the way in which the data is formatted by the transimitting device before it is output to the transmission line.

The data is proceded by a start - bit, a level change in signal of "1" to "0", which initialses the clock circuit of the receiving DTE. After the reception of this start bit the DTE clocks in the data bits (either 5,6,7,8) depending on the transmission code used). Followed by the parity bit, if it is present and finally by a stop - bit or bits. After the stop bit the DTE resumes its idle state untill the reception of another startbit.

3.3.2 SYNCHRONOUS TRANSIMISSION

The data to be transmitted is checked out of the transimitting DTE into its DCE where, as with asychronous transmission, it is modulated, it is modulated before being output to the transimission line. Upon reaching the receiving DCE the data is demodulated into sychronous with it. This is done in order that is can be successfully shifted the register of receiving DTE.

3.4 ERROR CHECKING

Error checking has an important role in the successful transportion of data, as during the transportaion process, data can pass a number of elements, such as a thunder, storm, interference by power cashes e.t.c.; that can cause a certain amount of distortion resulting in the possibility of the data being connected before it has reached its destination.

There are a number of methods that can be used to check the correctness of data transmitted between two devices. The type of error check used is largely dependent upon the operating mode of the devices ,i.e

- Asychronous
- Sychronous
- Packet.

3.4.1 ERROR CHECKING IN ASYNCHORONOUS MODE

There are three different methods available to check that the error free transportation of data take place, these are;

- Vertical Redundancy check (VRC)
- Frame check
- Echoplex check

3.4.1.1 VERTICAL REDUNDANCY CHECK (VRC)

In vertical redundancy checking an extra bit is added to each character in oder to check the number of "1" bits contained in the character. This bit forms a partiy in conjuction with the data bits of the character and that reason is more commonly known as the "parity Bit".

The character can be checked for;

- Even parity, where the total number of "1" bits in the character are even
- Odd parity, where the total number of "1" bits in the character are odd.

Upon reception of the transimitted character, the receiving device checks the parity of the received character. If this parity is incorrect a transmission error is signalled.

3.4.1.2 THE FRAME CHECK

The frame check is used in conjunction with devices operating in start-stop mode. In any start-stop mode, every character transfered is packed between start and stop bits. The detection of a start - bit initiates the reception of a data character. The receiving device also expects at least one stop - bit to follow the data bits of the character. It is the checking of these start and bits that determines whether the data has been transfered corretly.

3.4.1.3 THE ECHOPLEX CHECK

This method is only possible if the transmitting device is keyboard/VDU oriented and has an "ECHO MODE" facility. If this is the case, then the data is transmitted ot the receiving device e.g a host computer, immediately after it is typed in via the keyborad. The data is processed by the receiving device and also echoed back to the VDU of the transmitting devices to see if any error occured.

3.4.2 ERROR CHECKING IN SYNCHRONOUS MODE

There are two different methods, available for devices operating in sychronous mode. This is in order to accommodate the different types and therefore sizes of transimssion code used. The two methods are;

- Longitudinal Redundancy check (LRC)
- Cyclic Redundacy check (CRC)

The longitudinal redundancy method is only on devices operating in a 7 - bit ASC11 code as it makes use of the parity bit, and the cyclic redundancy check method is used on devices operating in the 8 bit EBDIC code.

3.4.2.1 THE LONGITUDINAL REDUNDANCY CHECK (LRC)

The longitudinal Redundancy check is not used on its own but in conjunction with the vertical Redundancy check. The function of the LRC is to perform an error check on each transmitted block of characters.

This is accomplished with the use of a block check character (BCC). The BCC is calculated from all of the characters contained in the block. Each bit of the BCC is the parity (odd or even) of the data bits in the corresponding horizontal row.

A BCC is generated by the transmitting devices during the transmission of the character block and is itself transmitted at the end of the block. At the receiving devices a corresponding BCC is generated during the reception of the character block. The two BCC's are then compared and will be the same if no errors have occured.

3.4.2.2 THE CYLIC REDUNDANCY CHECK

In the cylic redundancy check a block of data is recognised as a stream of transmitted bits. These bits are entered into a cylic shift Register, also known as a CRC Generator, where a mathematical operation is performed on the stream.

The result of this operation, called the CRC code, is transmitted along with the bit stream to the receiving devices where they are both entered into another cylic shift register, known as a CRC checker, that checks the data for errors.

The theory of operation behind the CRC methods is based on the division of a bit stream by a constant (see figure 3.5). The quotient of this division is discarded and the remainder is transmitted as the CRC code.

3.4.3 ERROR CHECKING IN PACKET MODE

This mode uses the cylic Redundancy check, the only difference is that the result of the mathematical operation performed on the bit stream is known as the frame check sequence (FCS) as opposed to the CRG code.

3.5 THE TRANSMISSION SPEED

The transmission speed is dependent on the quality of the transmission line. The numbers of ways in which the transmission speed can be expressed are given below;

- The number of characters transmitted per second
- The number of bits transmitted per second
- The number of elements transmitted per second

$$\frac{\text{Bitstream}}{\underset{\underset{\text{polynomial}}{\uparrow}}{\text{Constant}}} = \text{quotient} + \underset{\underset{\text{CRC}}{\uparrow}}{\text{remainder}}$$

Figure 3.5 CRC-Code Equation

The maximum number of elements to be transmitted is stipulated by the owner of the transmission line (normally the natural telephone (company), and is expressed in terms of Bauds.

In an asynchronous device using ISO-7 code and operating at a speed of 110 bits/sec. A character is comprised of the following;

- 1 start Bit
- 7 Data Bits
- 1 Parity Bit
- 2 stop Bits.

Which gives a total of 11 bits per character. By dividing the bit speed, 110, by the number of bits per character 11, the character speed is obtained in this instance 10 characters per second.

3.6 CONNECTION MODES

In general a system can operate in one of two possible connection modes,

- Simplex
- Duplex

The selection of either connection mode is dependent upon the application of the system, in which a system can be initially divded into two categories,

- Interactive
- Non- interactive.

3.6.1 NON-INTERACTIVE SIMPLEX CONVECTION

In a non-interactive system, communication is required in one direction, from device A to device B. This is the most basic form of communication possible and is achieved using the simplex connection mode.

As can be seen from figure 3.6, both stations consist of a single channel, the only difference being the function of DCE's. The DCE of station A performs a modulating function, and the DCE of station B performs a demodulating function.

3.6.2 INTERACTIVE DUPLEX CONNECTION

The Duplex connection is used in interactive systems as it allows the possiblity of communication in either direction, This means that the DCE's within the system have to contain two channels, one for transmitting and one for receiving.

There are two types of Duplex connection mode,

- Half Duplex,
- Full Duplex.

3.6.2.1 HALF DUPLEX

If the transmission line consists of a single channel, communication is only possibly in one dierction at any time, i.e if station A is in transmit mode, station B will be in receiving mode and vice- versa.

Interactive communication is made possibly under these

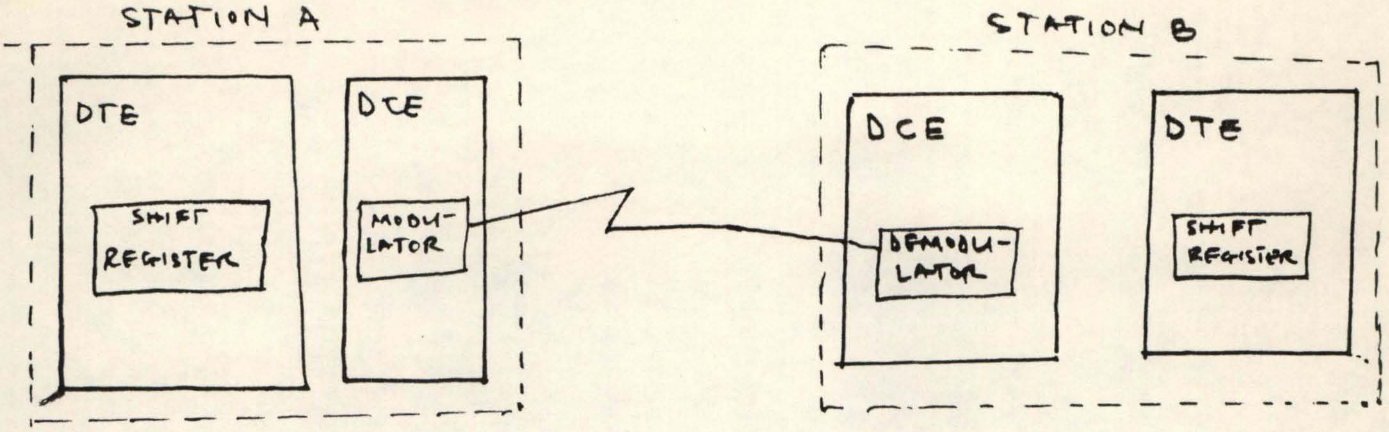


Figure 3·6 A simplex Connection

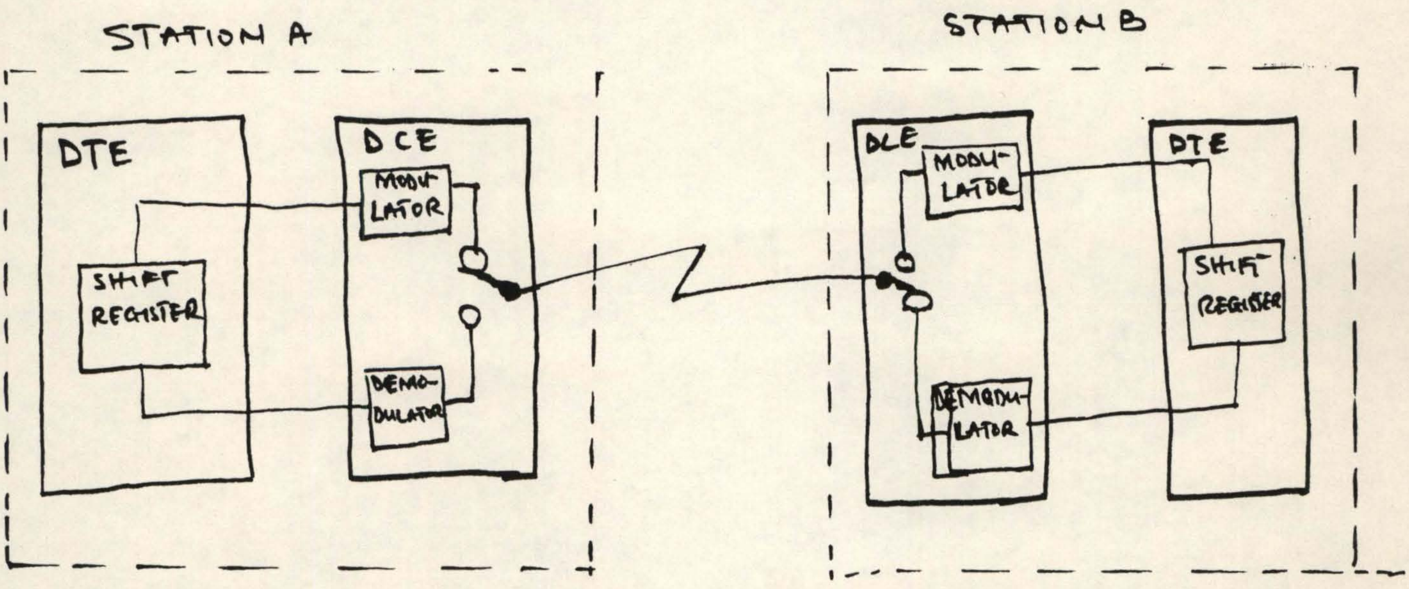


Figure 3·7 A Half Duplex Connection

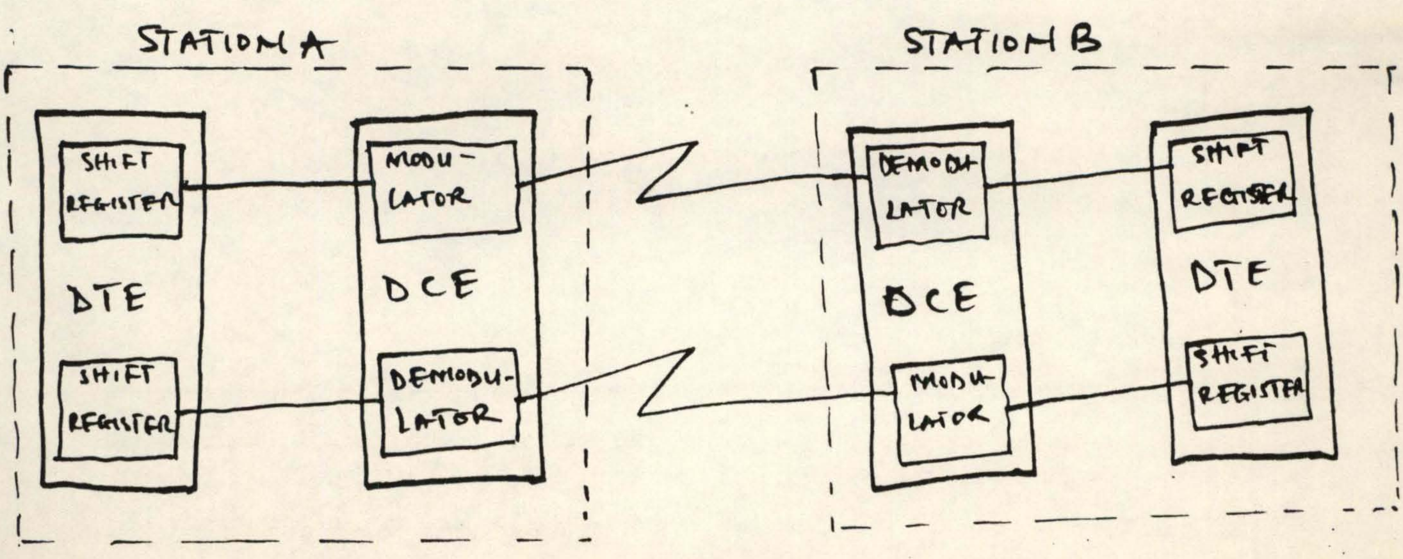


Figure 2·8 · A Normal Full Duplex Connection circumtances using a half Duplex connection. In this type of connection the DCE's are connection to the transmission line via a bult in switching circuit. This circuit can switch between either channel depending upon whether it is in transit or or receive mode (see figure 3.7).

3.6.2.2 FULL DUPLEX

If the transmission line contains more than one channel, the full Duplex connection mode can be used. In this mode simutaneous communication is possible between stations as there are seperate channels within the transmission line for transmitting and receiving (see figure 3.8).

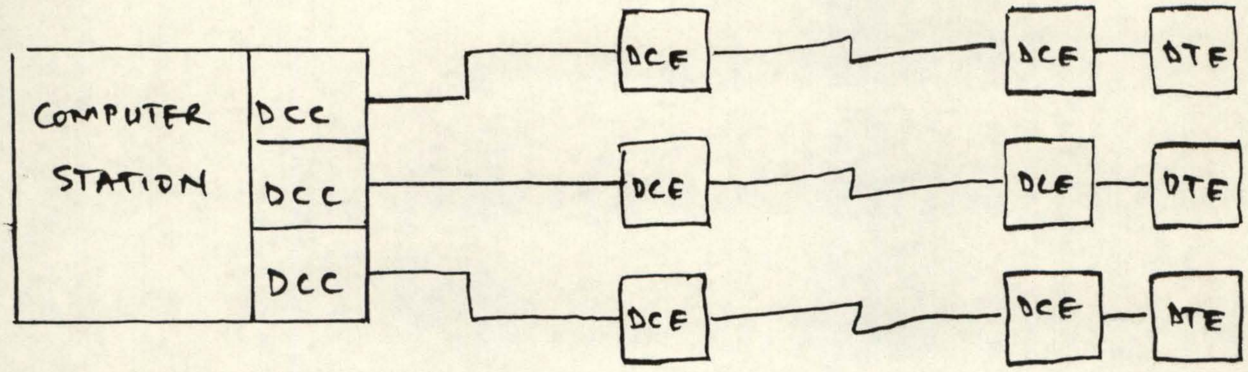
3.7 CONNECTION TYPES

There are three basic types of connection,

- Point to point
- Multi- point
- Loop

3.7.1 POINT TO POINT CONNECTION

The first and most straight foward connection type is known as the point to point, and is a direct connection between two devices. The point to point configuration can be used within a system containing a number of devices (see figure 3.9)



DCC = DATACOM CONTROLLER

Figure 3-9 A System Connected Using Point-To-Point

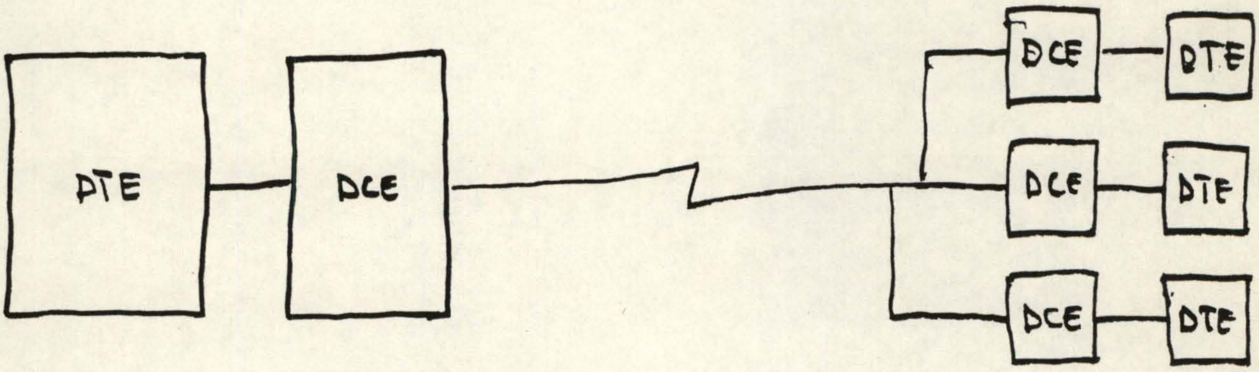


Figure 3-10 A Multi-Point Connection

3.7.2 MULTI - POINT CONNECTION

In a multi-point connection a number of device can be connected together via a single transmission line (see figure 3.10).

3.7.3 LOOP CONNECTION

This connection type can best be descibed as s serial multi-point. It is mostly found in banking systems where there is a primary device (A) connection to a number of secondary device (B,C, and D). (see figure 3.11)

3.8 DATA TERMINAL EQUIPMENT AND DATA TERMINATING EQUIPMENT INTERFACE

The success of data communication is only possible if the communicating device are compatible with one another. Therefore a certain amount of standard station is necessary in order to ensure that the succesful transfer of data takes place.

There are a number of Natural and International Organisations that have produced standands for data communication, a few of which are listed below;

- Comite consultant Internationla de Telegraphic et Telephonis (CCITT)
- International standards Organisation (ISO)
- American Natural standards Institute (ANSI)

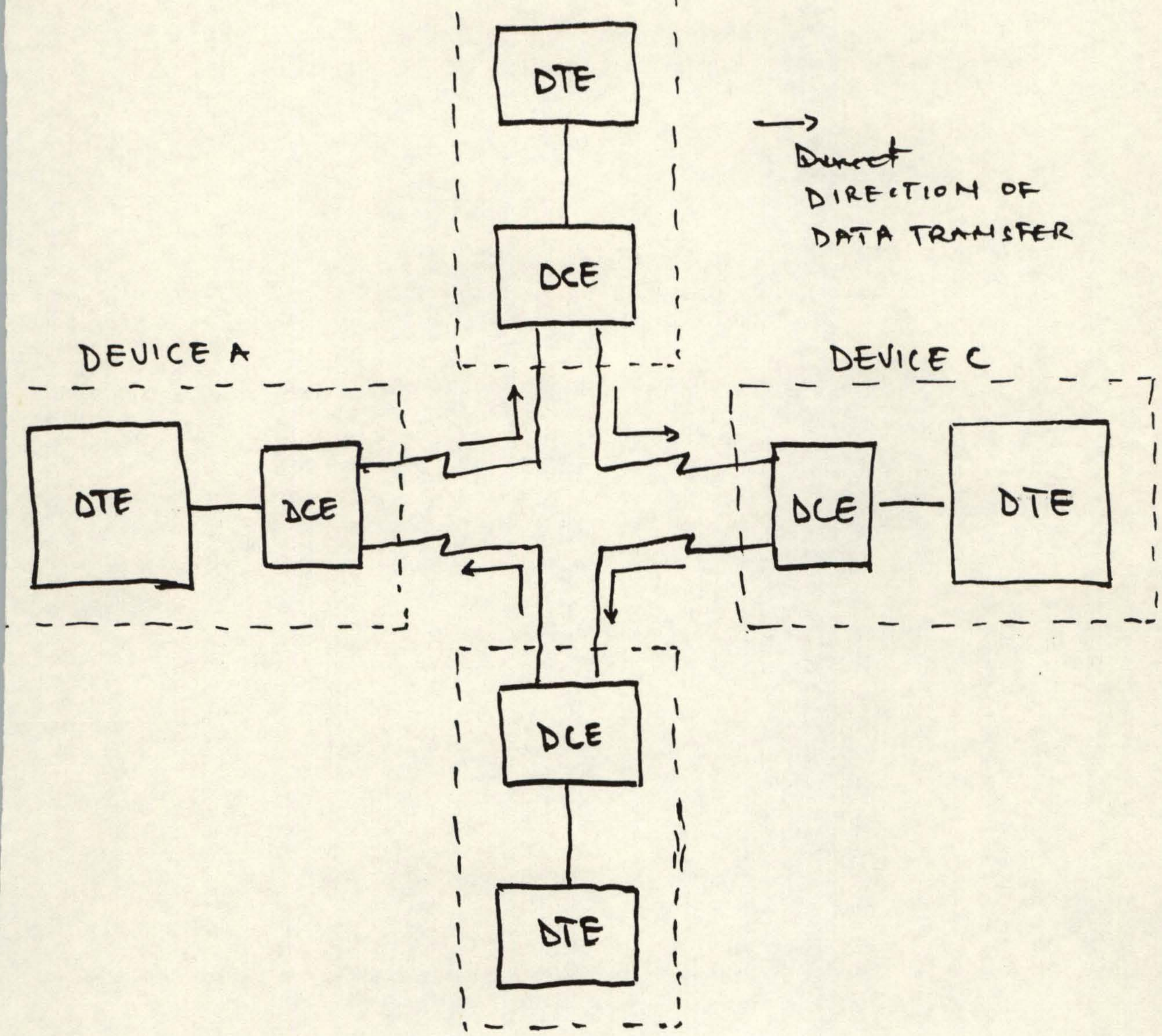


Figure 3·11 The loop Connection

- Electronic Industries Association (EIA)
- European Computer Manufactueres Association (ECMA)

The CCITT has produced two sets of standards for data communication, the V-series and the X-series recmmendations. The V-series is for data communicated via telephone Networks and the X-series is for communication vi dedicated Data Networks.

3.9 PROTOCOLS

Communication between a DTE and DCE is accomplished via an interface - (see figure 3.12).

If two devices (DTE's) are to communicate succesfully with one another there has to be certain amount of control over the flow of the transmitted data. This is accomplished by use of transmissiom control characters. These characters are separate from the data that is transfered and not have a printable representation.

These transmission control charaters alone are sufficient to control the data communication, some formal language is required to define how the control should be effected, when and how the control characters should be used and in which order e.t.c.

This formal language is commonly known as the protocol. A basic example showing the function of the protocol is given in figure 3.13

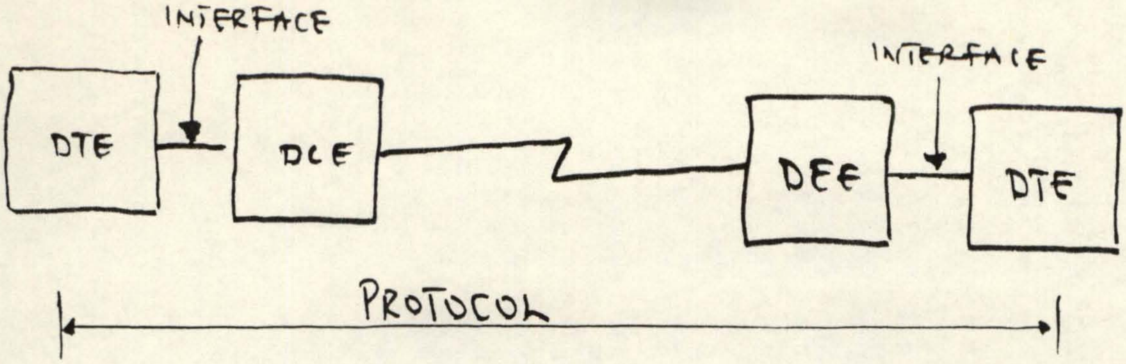


Figure 3.12 Difference Between Interface And Protocol

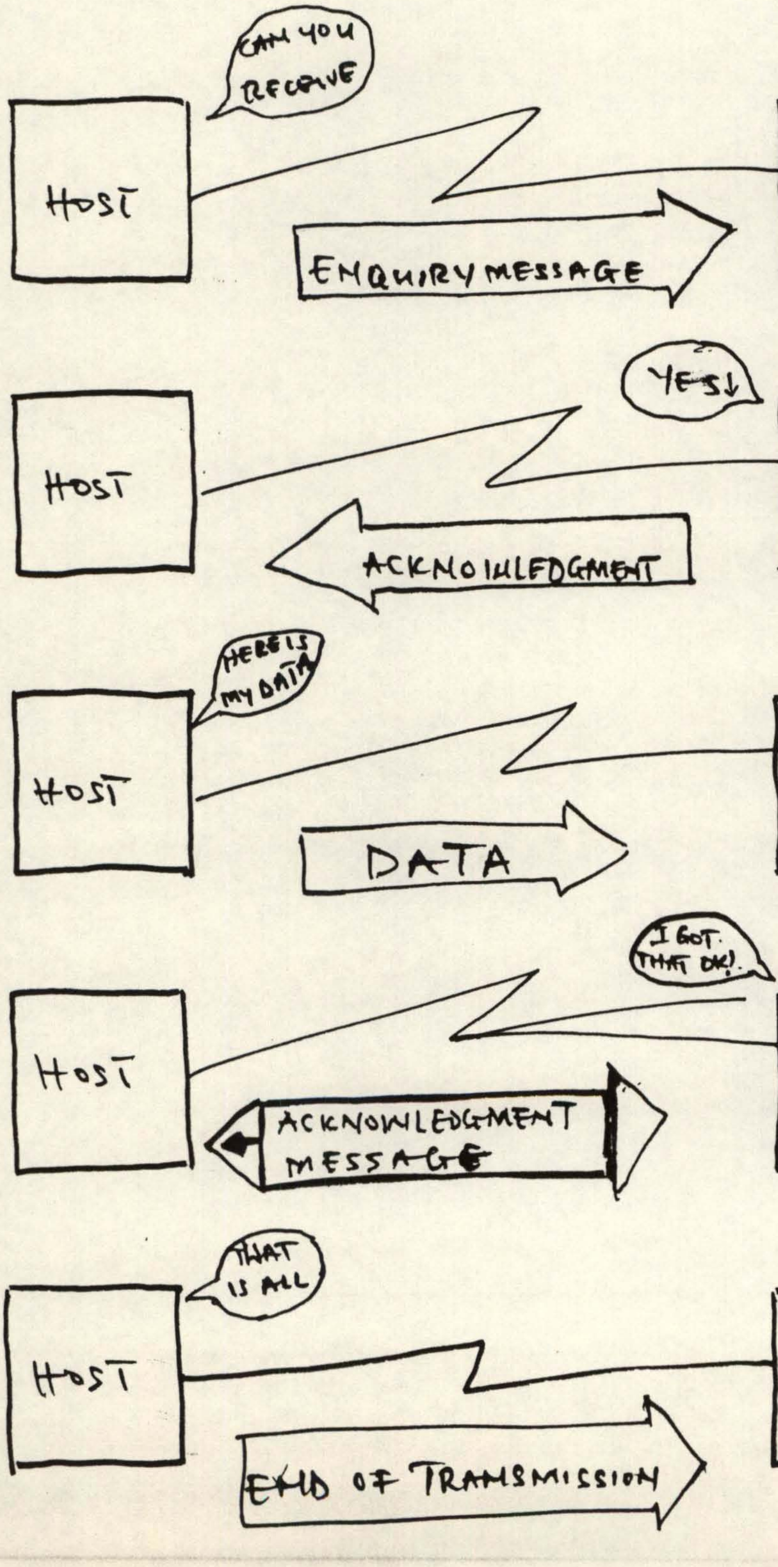


figure 3.13 An Example of A Protocol

CHAPTER 4

SHARED MEDIA IN NETWORKING

In a networking system, particularly in local networks, there are various forms of shared media. Sharing a medium is mostly about access control. The web of wires and interfaces becomes rapidly more complex as a network becomes more complex. The main subject of the present chapter is the study of an alternative way of joining a set of machines together by sharing a single medium. There are several ways of sharing a medium, we can calssify according to the way in which a medium gains access to the medium, and use of Time Divsion Multiplexing and frquency Divsion Multiplexing {TDM and FDM},contention, and Token.

4.1 FRQUENCY DIVSION MULTIPLEXING (FDM)

In a local system, where each device on the network has an individual transmitter and receiver associated with it, and where there is dedicated frquency slot for each of these devices to transmit and receive messages in the system is refered to as having a frequency division multiplexed bus' structure. In FDM, the frequency spectrum is divided into logical channels with user having exclusive possession of his own frequency band. By splitting a wideband channel into many-narrowband channels, then if a physical channel has a usable bandwidth of WHz and is split into M equal FDM subchannels, each subchannels has a W/MHz avaliable and thus can send W/M samples per second of data.

4.2 TIME DIVISIONED MULTIPLEXED (TDM)

In TDM, each transmitting device is given the total bandwidth of the transmission medium but only for a short time. It can be seen that there are two types of TDM from figure 4.1. We have sychronous time divisioned multiplexed and Asychronous time divisioned multiplexed.

In a sychronous time divisioned multiplexed system there exist fixed equal width time slots, which the units in the network can use to insert their messages into. The users then take turn to access the transmission medium, each periodically getting the entire bandwidth for a little bust of time.

4.3 CONNECTION ACCESS

The simplest form of connection access is usually refered to as simple Aloha. The term "Aloha" is used because the method was originally used on the Aloha Network in the early 1970's. On the Aloha networks, a group of stations shared a single radio channel to provide access for terminals distributed across the Hawqrian Islands to central computer. When a terminal attached to a station has a line input ready it transmitted it in a packet on the radio channel. If there was no other transmitted then the packet is likely to get through. However if another station also transmitted a

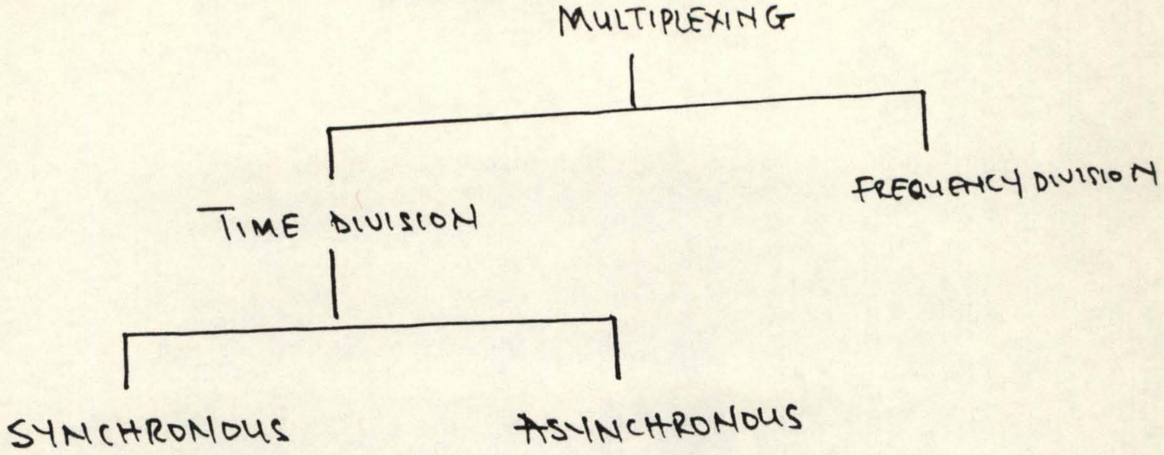


Figure 4·1 Medium Access Control Protocols

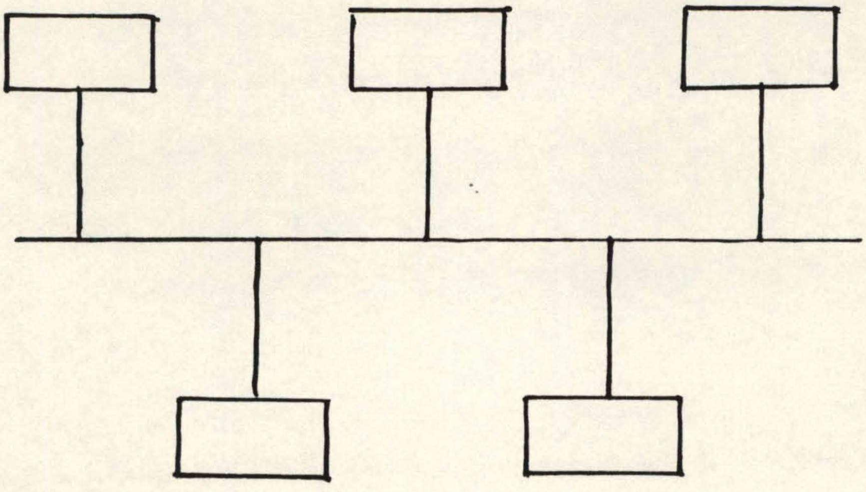


Figure 4·2 Common Bus Connection Via Ethernet packet in such a fashion that it overlapped in time, even by as little as one bit, then both packets were totally destroyed. When this happended, both stations would wait for a randomised time and transmit. The hope was that transmissions would eventually succeed in missing each other.

The term Aloha methods has come to general applied to any methods in which access to a shared medium is made in this random contention fashion. The essential character is that the packets are sent "blind" without first "looking" at or "listening" to the medium in order to take avoiding action.

4.4 CARRIER SENSE MULTIPLE ACCESS (CSMA)

In the Aloha channel a collission is only detected after the event, sometimes long after. If a station in this area has packet to transmit, it first listens to the channel to hear what any other station is transmitting with a delay of at most three bits. Thus if the channel is guite, then the station may start to transmit with high probability that the packet will not collide with another. This initia sensing for the already present signal of another station gives the methods its name; carrier sense multiple Access-CSMA.

Thus contention for the channel only takes place during the short time at the start of the packet. Once transmission is past this window, and its signal has started to reach all other stations, then it has seized the channel, the transmission is save, and all other stations will be deferring any output until the channel goes quiet again.

4.5 ETHERNETS

The CSMA protocols are great improvement in the Aloha protocol, as we might expect from our earlier discussion. With all the CSMA protocols, there is the small window when two or more stations may start to transmit before they see that the start of the other transmission.

With carefully designed cable systems, it is possible for a transmitting station to see a disturbance generated by another stattion transmitting at the same time that is similar in magnitude to the applied signal. In this way it can detect a collision, and we can abort the wasteful transmission. Such a system is termed carrier sense multiple Access with collision Detention CSMA/CD for short. Mostly it is known as informally as "Ethernet", the name assigned by the originators, Metcalfe and Boggs. Metacalfe and Boggs decribed the ethernet in a paper in 1976.

An ethenet is constructed by joining a set of stations onto a common piece of cable as in figure 4.2. In a given basic description of what this means it is sufficient to describe it as a 'listen while talk' system, where not only do the individual stations listen on the network while they are transmitting, but they also listen on the network while they are transmitting' conparing what they transmit with what they receive in this way they can therefore detect any other device transmitting at the same time.

Figure 4.3 shows a part of an ethernet with three stations and one reporter. We can see that each station is connected to the network through an interface and a transceiver and the purpose of the repeater is to connect two individual segments together.

4.6 RING SYSTEMS

A ring-based communication systems is constructed such that the stations or nodes on the network are joined together by active interfaces connected onto a transmission loop. In this way a message originating at one node enters the ring, is transmitted bit-serially to the adjasent node and passes from node to node until it reaches its destination. The destination node receives it, acts on the message then passes it on with a positive or negative acknowledgement. Finally the entire message continues around the ring until it returns to the originating node which then removes it from the network.

Messages in a ring-based system typically consist of a header, a time gap and data portion of the message with its own cyclic redundancy cheak. The header lenght and time gap are such that any node receiving the message has the time to

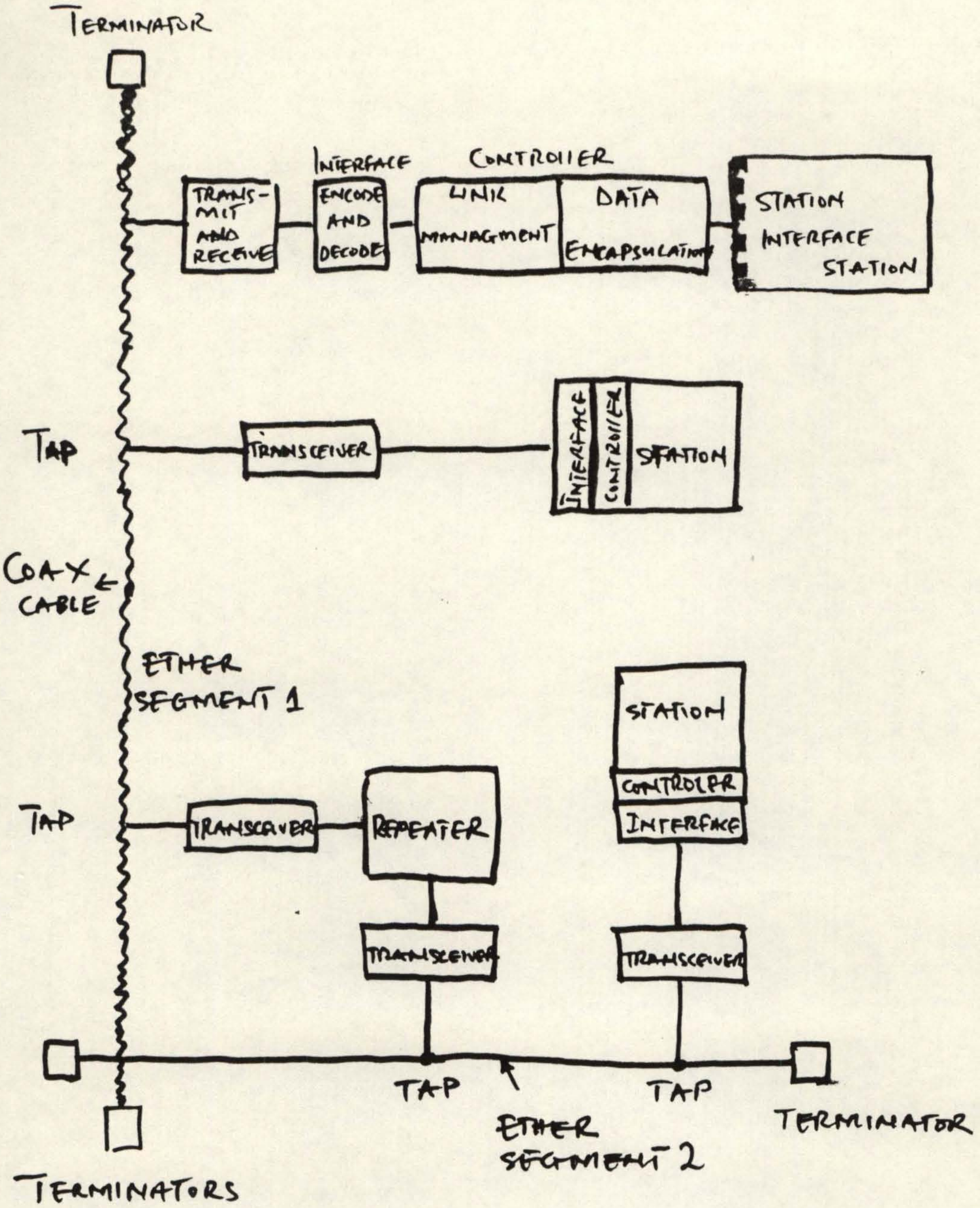


Figure 4·3 An Ethernet System.

check the header for corrections, determine whether it is the destnation for the message, then other pass the message on or receive the data portion od the message.

4.6.1 The Slotted Ring

The slotted ring system allows more than one packet on the ring at a time, each of the packets being slotted into a number of fixed size packets. The general principle of slotted ring is that the data transmitted on the ring are divided rigidly into a number of slots from stations to station. Each packet originating in the system contains a bit that indicates whether the slot is full or empty. When a station wishes to transmit it simply wants an empty slot to come around, makes it full and puts its data in the slot. The contention problem in sloted ring is simply solved by the slot. The contention problem in sloted ring is simply solved by having the remote stations wait for an empty packet to arrive.

The cambridge ring is a form of slotted ring system in that a system with no data to transmit waits for an empty packet to arrive and fills it with data and destination address.

4.6.2 The Token Ring System

Most ring networks tend to use the token ring type of system. The 'token' referred to in the name is a special distintive bit pattern or software mark that circulates through the network according to a predetermined algorithm, such that only the terminal with the token is permitted to send any message. In these system the station which holds the token must pass it on within a short time. Token passing may be such as a fully distributed polling system, in that the devices wishing to send messages have to wait until they receive permission in the form of token.

4.6.3 THE FDDI RING

The fibire Distributed Data Interface FDDI ring is another kind of token ring. FDDI is designed to be very fast ring that can have distributed physical extent.

FDDI allows multiple packets from multiple sources to be in transit at the same time, but achieves this using just one token. When a station has data to transmit, it waits for a token to come past, and captures it. It transmits several packets on the ring. The receiving station(s) copy the packet from the ring, but set it circulated back to the sender. The sender is responsible for removing the packet from the ring. The receiver(s) copy the data from the ring, and indicate that the packet has been recognised and copied by setting the appropriate bits. However, the sending station does not retain the token, it transmitts it immidiately following the packets it has sent out. In this way the token cirulates head up against the proceding data and allows the ring to be kept busy.

4.6.4 Token Bus

This type of medium sharring is topologically the same as the Ethernet. All stations are joined togther by a single passing wire, and each station taps into the wire. As with ethernet, any transmission by any station will be heard by all the other stations competing for access in ethernet fashion, access to the bus is regenerated by the passing of an access token ring among the stations.

Station are organised into a logical ring, and they pass an access token from one station to the next in the logical ring. As each station receives the token it may use it to transmit its waiting packets, and it must then pass the token onto the next station in the logical ring. In a logical ring the token is passed from station to station in order of the station numbers. On bus networks, including the token bus with its logical ring, every station talks to every other one, and hear every other one.

CHAPTER 5

NETWORKING ROUTING

The are various issues involved in suppling the basic network sverice. These issues are to do with suprouting data through the network and delivering it to its intended destination. We shall see how the route of a particular packed is determined both from its destination address and also from the topology and traffic in the network itself. Also,the two main approaches to the provision of network sverice, the datagrams and virtual calls is also discussed.

5.1 NETWORK ADDRESS, ROUTES AND TOPOLOGY

The various ways that data is transmitted, how errors occur, and the ways of detecting transmission errors and connecting them has been discussed. Now, we shall see how these basic elements may be combined to from the systems that are commonly called "Computer Networks".

The uses of network are attached to it in order to send data to each other and that the data will be passed accross the network in packeds. A user is a very general term, and includes individual terminal users or sample terminals and large multi-user mainframes servicing sveral hundred terminals.

For a packed to reach the intended receipient,the receipient need to be identified in some way. Every network user will be assigned a unique address. The sender of packets of data will attach the appropriate address to the packet before sending it out onto the network. The network will use the address to deliver the packet, the receipient uses the address to accept only packets intended for itself.

5.2 DATAGRAMS AND VIRTUAL CALLS

Datagram is an individual unit or packet of data together with a destination address. This is shown in figure 5.1. Datagrams are out onto the network one by one, and the network will interpret the destination address and try to deliver in a different order or may be lost sometimes and may de duplicated, currepted a mis directed.

A vitual call service parallels a telephone calls. An association is established between two users, one which calls the other. The two users then exchange data along the virtual call or connection, and then finally one or other initiates the disconnection of the call.

5.3 ROUTING DATAGRAMS

The topology of the network determines the routing of datagrams. The easiest type of routing is the degenerate ease of the shared medium. The medium could either be a ring or a bus, and access to it could be either by means of token or by contention. All shared medium have the common property that every packet is received by every user of the network, therefore there is no problem of working out a route, everything is broadcast everywhere. It then becomes merely the degenerate task of the receivers ignoring all the

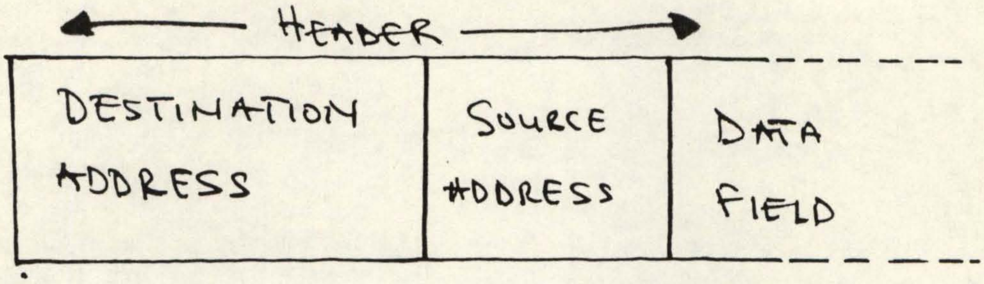


Figure 5.1 A Simple Datagram.

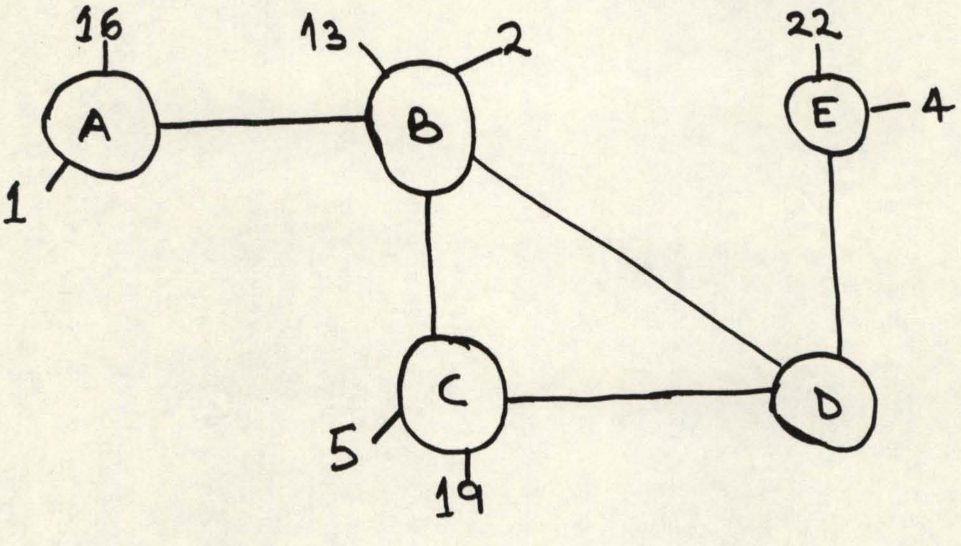


Figure 5.2 A Simple Network

packets not meant for itself.

Figure 5.2 shows a network with a set of five "Nodes". A to E connected by a set of point-to-ponit links. The links between the nodes are point-to-point links. In each nodes, the controlling program examines the destination address on the packets, and the uses some algorithem to chose the next link down which to send the packet towards its destination.

A possible way of implementing a network like of figure 5.2 is the setting up of a "routing table that contains ten entires, one for each destination address. In node A the entries for addresses 1 and 16 would indicate the specific links to those destinations, while all the other eigth destinated, would indicate the link connecting to node B. Also, node B would indicate that the datagrams for destinations 1 and 16 should be sent down the link connecting to node B. Also node B would indicate that the datagrams for destinations 1 and 16 should be sent down the link to node 4, destinations 13 and 2 should go down their specific links, 5 and 19 should go to node C, and the rest to node D. The routing tables for all five nodes can be contructed in a similar way.

In constructing these routing tables, we have taken the topological diagrams in figure 5.2 and worked out the shortest route from whenever we are to give destination. The mainteance of the routing tables will become more difficult as the networks get larger and lager. If there are a network with a 100 nodes and a thousand subscribers, then we will have to keep a routing table with a entires in each of the hundred nodes - 100,000 entries in all, and each time a subseriber joins the network all 100 tables must be updated.Considering instead the relabelled network in figure 5.3. Here we see that the addresses have been allocated in a two tier manner. All users on node D have the first part of their addresses 6, and no other users attached to other nodes have 6 as the first part of their address. The address is in two hierarchically related points-a node number and a line number. Thus, when trying to figure out the route to a specific destination, the algorithm goes like;

```
     if Destination _ Node _ Number = My_ Node_ Number
     then
          - packet is in the right node; look up the
          - destination in the line table
     else
          - packet is still in the wrong node; look up
          - the next segment of the route in the node
            routing table.
```

The advantages is that the network of 100 nodes and 1000 users, each node has one lookup table with 100 entries to find the destination node, and another with 10 entries to reach the ten locally attached users in this node. Also when new users join the system, the local lookup table needs to be modified.

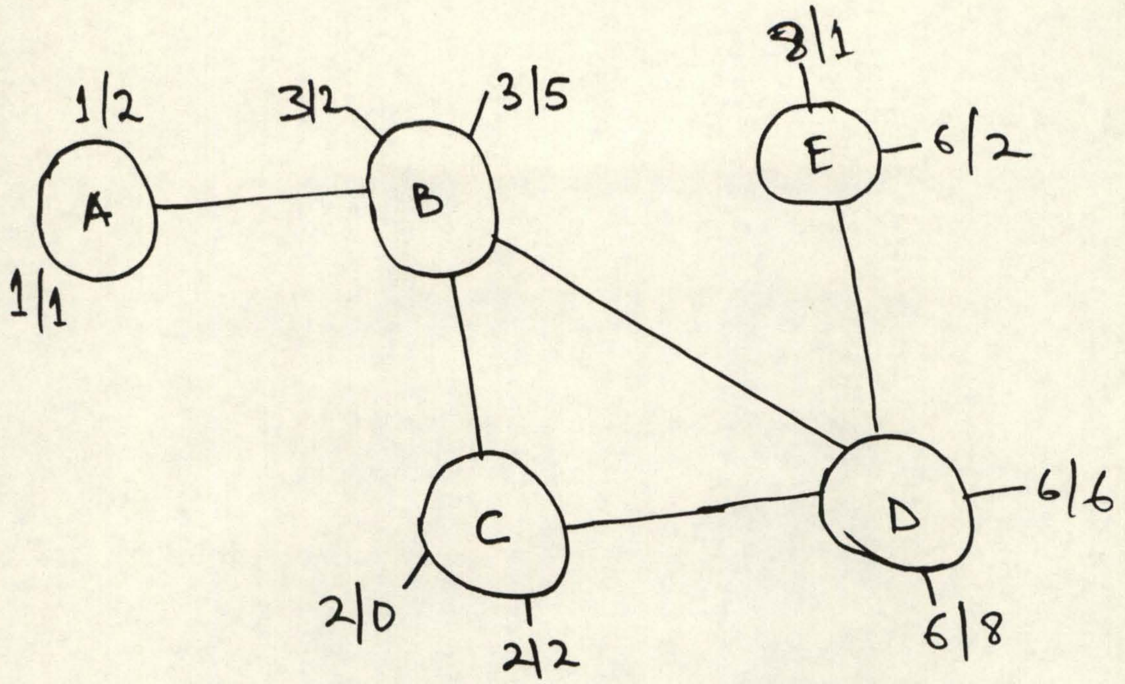


Figure 53 Two-Tier Addresses

5.4 VIRTUAL CALL NETWORK

figure 5.4 shows a simple network with user S attached to node A at address 1 2 3 4 5 6 7 and R attached to address 7 8 9 2 3 4 5. Suppose S wishes to estabish a virtual call to destination R. A call request is sent to node A specifing the requested destination and a label "Lsa" by which it wishes to identify this virtual call future. The point of specifying virtuals calls, and Lsa distinquishes which one in future messages. Lsa is unique link between S and A. In X.25, Lsa is the logical channel identifier.

The call request packet is "channel to 7 8 9 2 3 4 5 from 1 2 3 4 5 6 7 using label Lsa. When a call request packet arrives at node A, a control block will be allocated for the new virtual call. Amongst the information stored in this control block will be the label Lsa, and an identification of the link back towards S. Then A will examined the dsetination address "7 8 9 2 3 4 5", and work out the next link in the chain by means of routing tables. It identifies the link, and enters both the new label and new link in the control table for the virtual call. Finally, a new, modified connect packet is sent out onto B; connect 7 8 9 2 3 4 5 from 1 2 3 4 5 6 7 using lab ". The labelfor the virtual call changes as the call progress step-by step and link-by link through the network. The process is repeated with allocation of control block, the resolution of the next leg of the route, and the allocation of the next link, until the destination is reached. See figure 5.5.

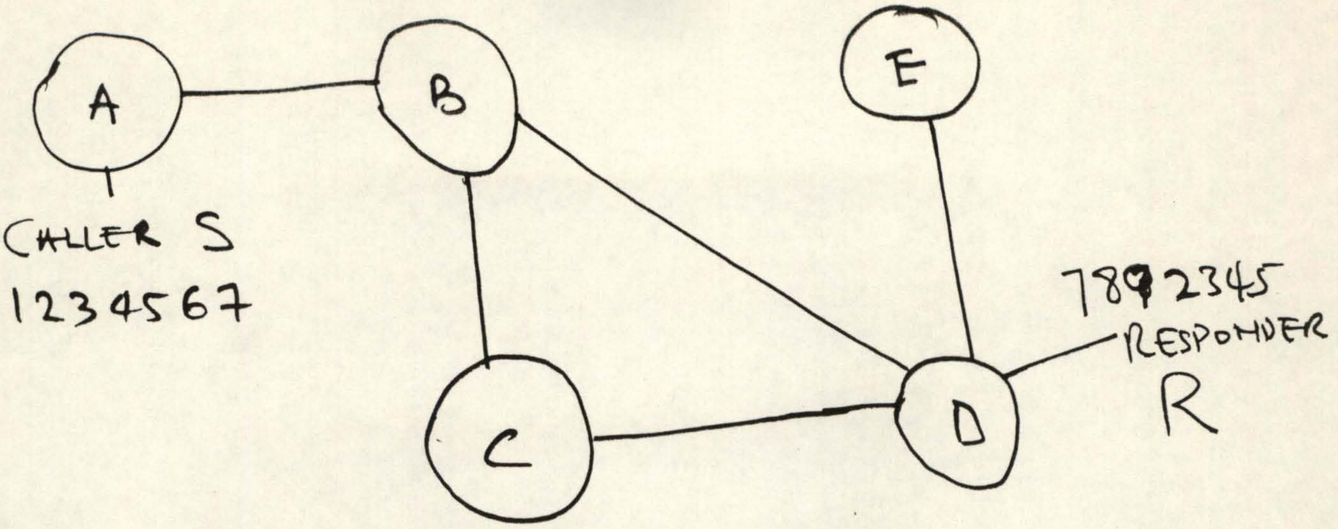


Figure 5.4 A Virtual Call Network

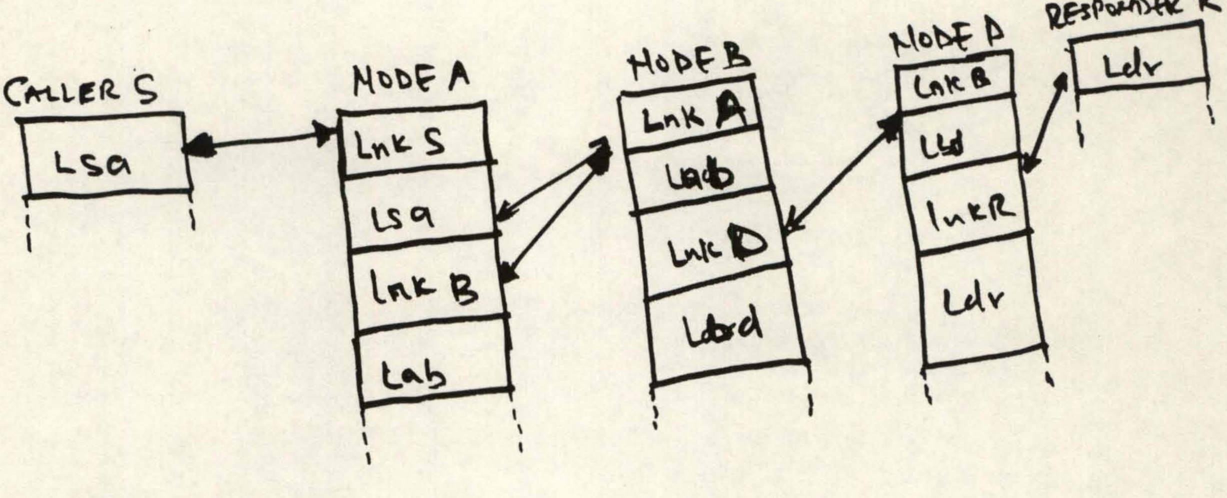


Figure 5.5 Linked Tables Node-to-Node

CHAPTER 6

NETWORK SERVICE AND INTERFACE

In the last chapter the principles involved in atually building the network itself out of constituent pieces were well explained. This is done by detailed examination of the two most inportant network services, X.25 and TCD, together with their protocoles. Also explained is the ISO transport services and brief summary of ISDN facilities.

6.1 X.25

X.25 is one of a set of standards produced by the international body, the CCITT. The X.25 is also blessed by ISO as 1S 8208. It is essential to realise that X.25 is primarily a defination of an interface to a network. (see figure 6.1). X.25 is the standard that describes the protocol across the link between the data circuit terminating equipment (DCE) and the Data terminal equipment (DTE) for Public switched networks.

6.1.1 The X.25 PROTOCOL

X.25 is built on the top of a single point-point link. This connects the user to the network, and is run with error checking protocol. X.25 provide virtual call service and allows the multiplexing of many virtual calls over a single link. Multiplexing allows the X.25 user to run multiple virtual calls with many users over the single X.25 link.

6.1.2. CALL CONNECTION in X.25

Virtual calls, including those in X.25, have three main phase. First the call is set up. If the set up is successful, there is a transfer phase, and then finally the call is cleared or disconnected. The call setup and clearing is best understood with a specific example. In figure 5.2 we see an x.25 network with two users A and B. If A establishes a virtual call to user B. Fisrt A chooses a new logical channel identifier (LCI), because each virtual call on the X.25 link is allocated a label to identify the call. The LCI has a local significance between DTEA and the corresponding DCE in the X.25 network, and it has relationship with LCIs in use at B or anywhere else. It construct a call request packet with a header as in figure 6.3, a type of 0001011 for table 6.1, and the required destination address, its own address, and some other parameters. This is sent across the X.25 interface to the DCE.

The DCE at A then communicates in some unspecified way with the DCE at the destination using whatever internal protocols that are appropriate. This causes the DCE at B to generates an incomming call packet to send to the corresponding DTE B must chose a new similar to the original call-request packet, but DCE B must chose a new LCI that is locally unique on its own X.25 link to user B. When the incomming call request arrives at B, the user

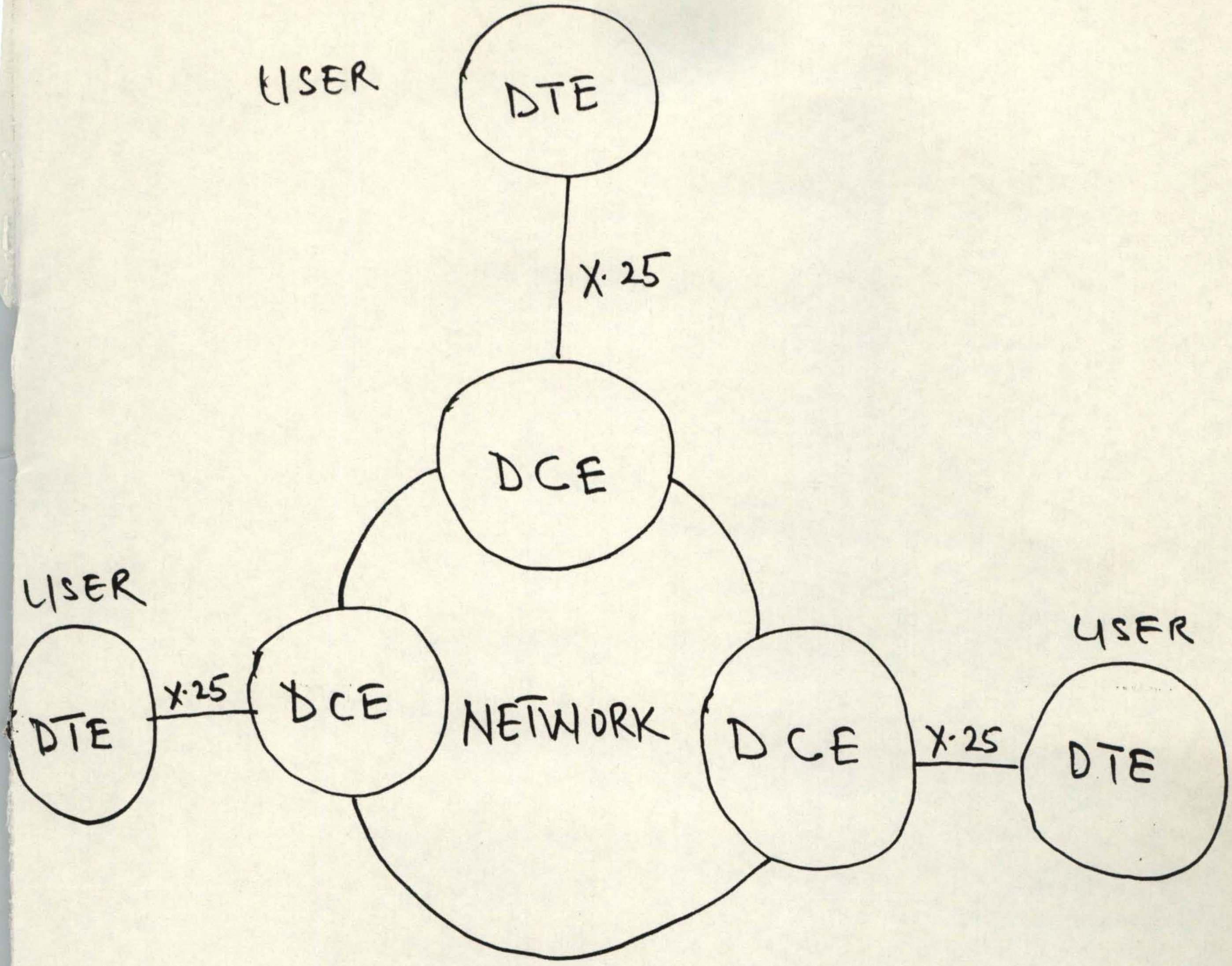


Figure 6·1 The Basic Role of X·25

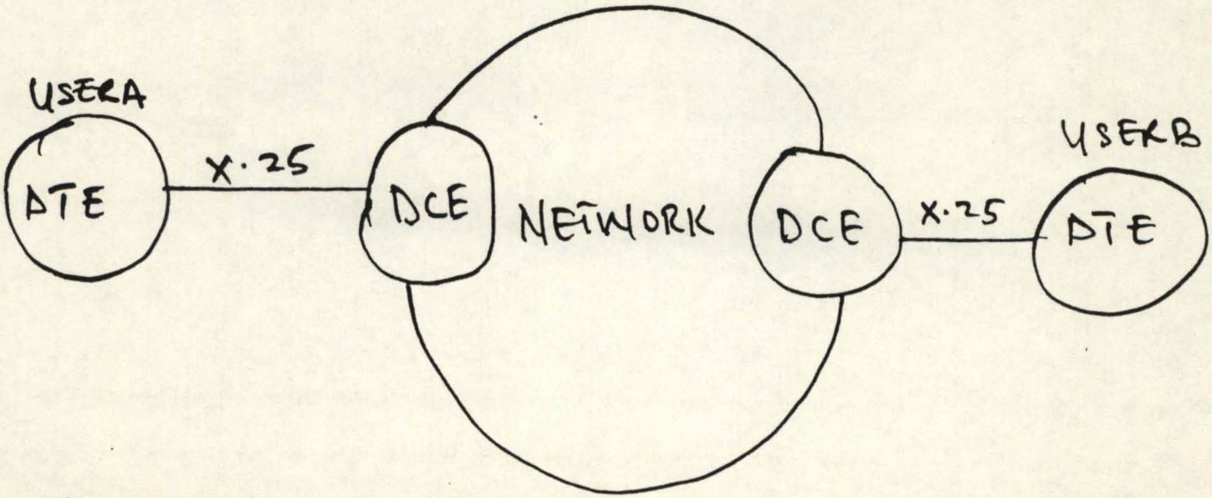


Figure 6·2 The Basic Model

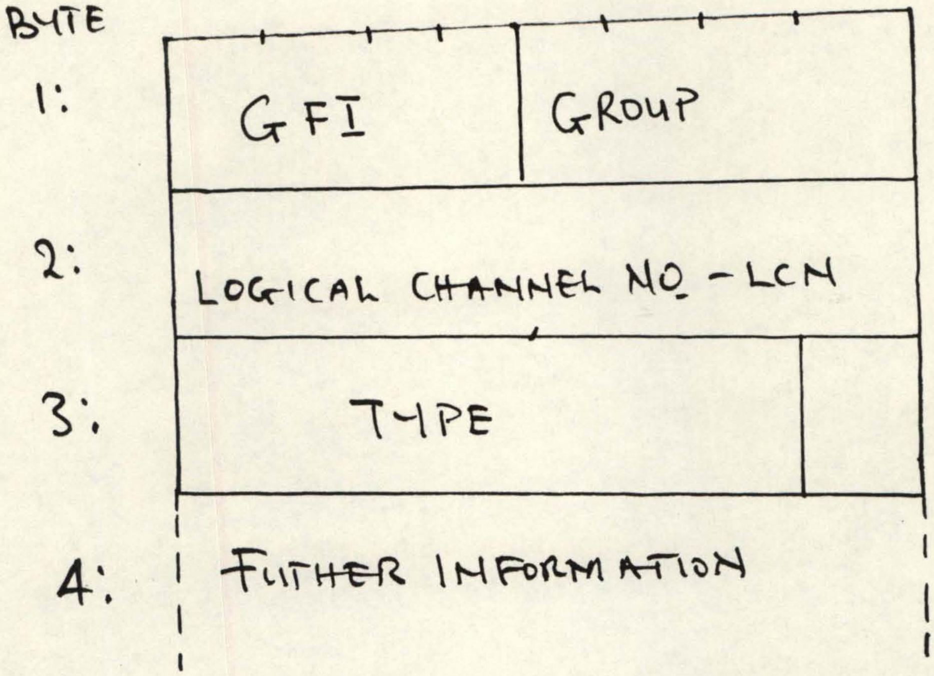


Figure 6·3 The General Format OF X·25 Packets decides whether to accept the call. If it decicks to proceed, then it will generate a Call-Accept packet. When the DCE at B receives this accept packet, it communicates suitably with the other DCE at A, and the DCE will then emit a call-connected packet to the original caller at DTE A. Once the call has been established, data is exchanged using the data type from table 6.1

6.1.3 RESET

The other operation that may take place during the data state is the RESET. The RESET operation is an attempt to recover from various error situations such as the detention of the loss of a packet, a protocol violation, an error in an unplementation, or a desire by higher level protocols to return to some well defined state.

The RESET operation causes flow control to reintialise, packed in transit to be disconnected, and so on. There are two main types of RESET, one is when a user request a reset and when the network detects an error. In the first case the RESET is propagated to the far end of the connection. The RESET confirmation is propagated back, and the RESET is complete.

The final important function of X.25 is that of call clearing. It is identical to those of RESET. As with RESET the call clearing process destroys data in transit and can be initiated at any time either by the network or by the

FROM DTE TO DXE	FROM DXE TO DTE	87654321
Call Request	Incomming Call	00001011
Call Accept	Call Connected	00001111
Clear Request	Clear Indication	00010011
Clear Confirmation	Clear Confirmation	00010111
Data	Data	xxxxxxx1
Interrupt ~~Confirm~~	Interrupt	00100011
Interrupt Confirm	Interrupt Confirm	00100111
Receive Ready	Receive Ready	xxx00001
Receive not Ready	Receive not Ready	xxx00101
Reject	Reject	xxx01001
Reset Request	Reset Indication	00011011
Reset Confirmation	Reset Confirmation	00011111
Restart Request	Restart Indication	11111011
Restart Confirm	Restart Confirm	11111111
Diagnostic	Diagnostic.	11110001
Registration Rqst.	Registration Rqst.	11110011
Registration Rqst	Registration Conf.	11110111

Table 5·1 Packet type Identifiers in X·25 users , however, the final effect is that the call is cleared rather than being just re-initialised as with a RESET.

6.2 THE ARPANET TCP

The ARPANET Transmission Control Protocol- TCP is the protocol invental by the ARPA community for use on the ARPA network. TCP implements a connection - orented services that lives on top of a datagram services.

The function of TCP is to open and maintain a connection between two entries, transfer data, and then finally to clear the connection down.

6.2.1 The TCP PROTOCOLS

Datagrams may be currupted while the connection is in progress or while it is being set up. To recover from these errors, TCP uses a sequence numbering scheme. It provides a two way simultaneous flow data- full duplex. Each flow of data has an associated independent sequence number each and every byte of data is numbered in ascending order. In effects, each byte is transmitted individually from the sender to the receiver and acknowledged individually by the receiver. Should a byte lost in transit, then the sender will wait for a certain time for an acknowledgment, and then retransmit the byte, and will persit in this until the byte is finally acknowledged.

6.2.2 CONNECTION MANAGEMENT

The other main area of TCP is the management of connection process. The mechanism was presented in a paper by Dahal and Sunshine (1978). The entity wishing to establish a connection could send a call-Request to the other party, the other party could then reply either in the affirmative, or may simply reject the advances of the caller. In this circumtances this would indeed be all that was required. However datagram services may currupt data. One of the more challenging problem that caused is when a packet is unduly delayed. When such a delay is combined with a computer that "crashes" and restarts, then the scope of confusion is considerable.

Dahal and Sunshine deviced a mechanism whereby this confusion could be avoided by making the handshake slightly more complex. The fundamental device is to use a new, unique identifier that can be attached to the call request packet. A suitable method is to time stamp with resolution small enough so that no two call request packets from the same starting point can even contain the same time. This call-Request carries the time start stamp and the call-Accept will carry this unique brand back. On receipt back by the instigator of the call, the stamp is checked, and if it does not agree with original value sent out on the call-Request, then remedial action is taken.

In TCP, the unique starting point is called the initial sequence Number - ISN. Since this is unique, this ISN is also used as the unique stamp in the call request packet, and is returned on the call accept packet. The estblishment of a connection involves each end emitting a call-Request to the other end specifies on ISN, and receiving a call-Accept confirming the ISN from the other end.

Now, when an invalid sequence is detected, the TCP uses the device called RESET. When either end of the connection receives a packet that it decides is a clear violation of the protocol, i.e not intended for the current connection it should send a RESET.

6.2.3 DISCONNECTION MANAGEMENT

TCP approach to disconnection is different from that of X.25, the disconnect or close is a logical marker that follows the data, and keeps its place at the end of the segment at which it is transmitted. Thus it is not distruptive and no defence action against the destruction needs to be taken. If A and B are transimitting data, A can decide that it has finished sending data to B and send close. However B can still continue updating its receive window and notify B of this to acknowlege the receipt of the data, and further movement of this foward edge of the window that is neccessary to allow the flow. Eventually, the reverse leg from B to A will be closed too.

Finally, TCP is defined on top of an underlying Internet Protocol- IP. IP allows datagrams of various lenghts to be sent across mixture of diverse networks that together make up the internet. The IP datagram contains 32-bit source and destination address, and allows for the fragmentation and reassembly of datagrams at intermediate steps on the journey across the internet should this be necessary.

6.3.0 THE ISO OSI SEVEN LAYER MODEL

The task of implementting communications systems to cope with the problems encountered in the real world is very large indeed. The task is too large to be dealt with as a single task. In order to make things manageable, the task has to be broken down into a number of sub-tasks. Each of these can be thought of as a self contained task. One such subdivision is the ISO seven layer model. This is particularly important as it forms the basis of the 'open systems' interconnection network protocols usually known as OSI Protocols.ISO stands for the International Orgaisation For Standardisation of a standard organisation heavily involved with the standardisation of network protocols.

OSI specifies a set of protocols that can be used to implement a network at some levels, especially the lower levels, there are several alternative protocols that may be employed. This allows networks to different sets of interworking with other OSI networks.

6.3.1 LAYER 1 - THE PHYSICAL LAYER

The physical layer deals with the most fundamental aspects of network connection. Connection types, connnection pin-outs, electrical signallying and signally conventions. The standards for the physical layer specify how to design drivers and receivers for the interface, what type of cable to use to write devices together and precisely how the interface operates. The most important physical layer standards relevant to packet switched networks are X.25 and X.20 bis.

6.3.2 LAYER 2 - THE LINK LAYER

The link layer is responsible for transporting information from the higher level protocols across the physical layer interface between two devices connected together. The link layer provides mechanisms for detecting errors in the information transfered. This may be in the form of 'currupted data ' possibly due to electrical noise coupling into the link wiring. The link layer has to include mechanisms to detect such errors and construct them in a way that is transparent to the higher level protocols. The OSI link layer protocol for packet switched networks is known as ' X.25 level 2'

6.3.3 LAYER 3 - THE NETWORK LAYER

The network layer is used to establish connectors between end point devices across a networks or interconnected networks. The network layer must include an 'address' concept, so that devices can identify each other. The network layer controls the transfer of information from the higer level protocols across connection. The OSI network layer protocol for packet switched network is 'X.25 level 3'

6.3.4 LAYER 4 - THE TRANSPORT LAYER

The transport layer provides a standard interface between the higher level protocols and the underlying lower levels of the network. The transport layer is needed because different network and link layers may have different characterities . These need to be hidden from the higher levels if inter-networking between different types of network is to be possible.

6.3.5 LAYER 5 - THE SESSION LAYER

The session layer uses the transport services to provide the mechanism for transmitting information and so does not have to worry about the messing details of the network and the link layers. It provides support for the information transfer between applications.

6.3.6 LAYER 6 - THE PRESENTATION LAYER

The presentation layer deals with the way in which the information being transfered is represented. The presentation layer incoporates a 'transfer syntax' to define rules for how the information is to be represented in such a way that any OSI application can understand the information.

6.3.7 LAYER 7 - THE APPLICATION LAYER

This layer provides the ultimate in high level support for the application using the network. It includes facilities like file transfer, job transfer and message handling support. Support is also included for interactive use of network in the form of virtual terminal (VT) support.

6.4 ISDN

There have been many changes in the technology of Telephone services for a whole variety of reasons. In particular, rather than the circuit being anatogue end-to-end it is normal for the speech to be digitised and for the vast majority of the transmission between exchanges to take place with purely digital signals. Since the service delivered to the customer is analogue, then the normal way of transmitting data is to use modems to convert the digital signals in the computer or terminal into the analogue signals that must be transmitted along the telephone wire. At the exchange, these analogue signals are digitised and switched between the exchanges. Clearly this is not ideal situation. For this and many other reasions, the whole of the telephone system is being revised, and a system called integrated services digital network - ISDN is being introduced. Modern use of wide- area networks is still dominated by slow speed terminal access and mail, and ISDN services will make a large impact in that area. However, ISDN is only just starting to appear, and by the time it is widely available, the major use of networks will certainly have moved beyond simple terminal access to the more demanding bulk data transfer which is clearly the main use of fast local-area networks. Already wide-area networks are providing ever faster transmission speeds. ISDN will have to compete directly with fast local networks for the higher performance applications

CHAPTER 7

INTERNETWORKING

The devices that interconnect the networks are usually called gataways. Gateways allow communication between two networks that have different sets of addresses.

7.1 GATEWAYS

In figure 7.1 there are three gateways. Gateways 1 and 2 are simple gateways that interconnect two networks. Gateway 3 connects all the three networks. The problems that gateways face and sometimes sovle are many and varied. It may be because the networks having different technologies or differentsets of addresses or may be because they are run by different orgainsations that have seperate budgets and phylosophies.

7.2 ADDRESING DOMAINS

Gateways allow communication between two networks that have different sets of addresses. For example in fig. 7.2, we have two networks A and B that have overlapping sets of addresses [1 2 3 4] and [2 3 4 5]. Any address only has meaning within its own context or domian. However, a user of network A, say X at address 2, can communicate with a user Y at address 3 in network B, and it is possible using only the domain address above.

It is not possible for user X to find address '3' to network A or she will get it interpreted locally within A's domain.

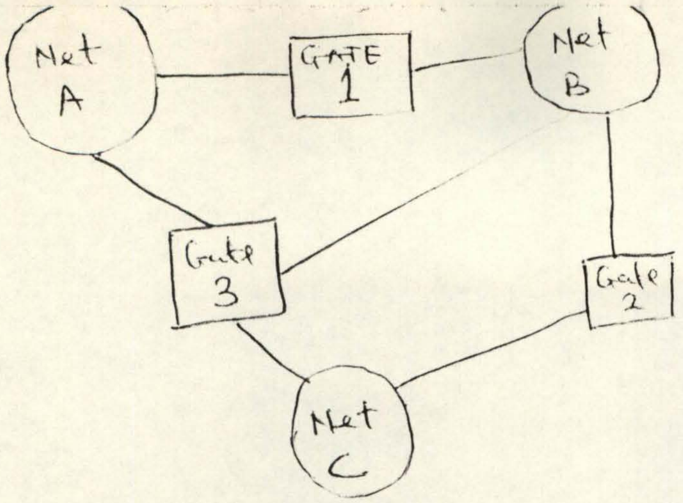


Figure 7.1 Networks Joined via Gateways.

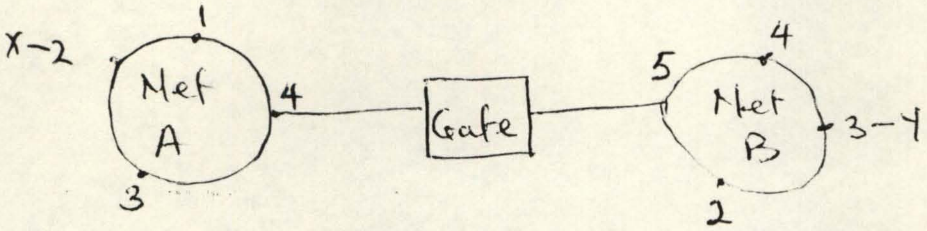


Figure 7.2 Networks with Conflicting Addresses.

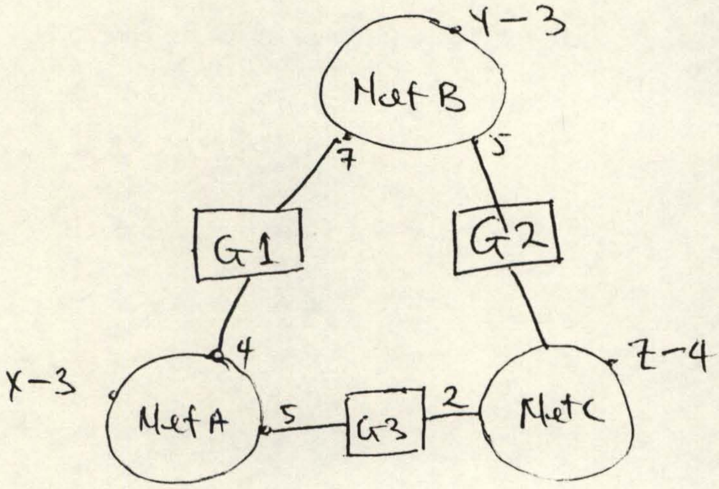


Figure 7.3 Third Party Addressing.

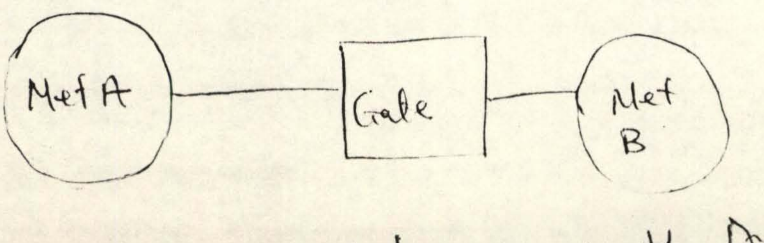


Figure 7.4 Networks with Differing Packet Sizes.

It will not get to the remote destination intended. Therefore, to communicate to address 3, but on network B", there must be a mechanism for saying it. A straight forward way is to form a compound address. First, the address of the gateway within the local domain, and then the other address on the other side of the gateway. Thus the user at X will generate an address like "4,3" and feed this to network A. The first part of address "4" will be used to reach the gateway . The gateway then retreives the rest of the address from Y to X is "5,4". The important thing is that the address of the gateway G, but from the other side, in the other domain.

7.3 THIRD PARTY ADDRESSING

It is also possible for a user X to create a job that uses a file at Y, and transfer the job to Z to be executed. To address this type of job, considering internetwork in figure 7.3, thus as it passes through gateway G3 on the way to Z, the refrence address [4, 3] is prefixed with G3's address in the domain of network C, giving a new address (2, 4, 3)

The new job has now been transfered to :

```
BEGIN <JOB>

-------------------------
-------------------------

EXECUTE FILEPRO INPUT = FILE  @ [2, 4, 3]

-----------------------
-----------------------
END {JOB}
```

7.4 PROTOCOL MAPPING

Gateways way be used to join networks that run different sets of protocols. Gateway may be used to interconnect a datagram network on the side to virtual call network on the other. At another level, a gateway may attempt to map two higher level protocols to each other, allowing file transfer to make place.

This type of gateway is extremely useful, following the networking of the different types of technology available for local and wide area networks, and allowing wide variety of differing networks to work together.

7.4.1 MAPPING AT THE PACKET LEVEL - PACKET SIZES

It is generally easy to map at the packet level. If there are two different types of technology that we wish to gateway together, it is generally straight foward to take a packet from one type of technology and transmit it onwards across the other.

However, there are still few possible problems, even with such an apparently trivial task, for example, packet sizes and addressing. Considering figure 7.4. Suppose that network A is capable of working with packet sizes up to 512 bytes long. There is no problem with sending a packet from A to B, but suppose a packet from network B that is 350 bytes long arrives at the gateway destined for network A. Obviously the 350bytes will not fit into the smaller

128 bytes packets in network A. It is not possible to just put the first 128 bytes into a packet in A, and discard the remaining 222 bytes.

There is a solution, but it depend on the amount of "control" or "influence " that can be exerted on one or other network. If a network is under our control, it means that we can change the protocols in use on the network.

It is possible to split the long packets from the network B up into smaller fragments that fit the packets on network A. The gateway should be able to do this and the users of network A must be able to use the fragmented packets from the gateway.

CHAPTER 8

SECURITY IN COMPUTER NETWORKS

As computers become more pervasive and important, the information that they process and pass from one to another across networks becomes more critical. Secure data is basically that which should not be generally available. Personnel information and financial records fall into this category .

Secure data is held in databases in computer systems which may be connected to a communication network. In many cases, it is difficult to control access to the network and therefore the host computer system on the network must protect themselves against attack from intruders. This is what is meant by 'access control', only those people who need to access the data should actually be able to access the data. Unauthorised attempts to access the data should not only be detected and prevented, but also signaled to the operators of the system so that they are aware of these attempts.

Access controls usually use some form of password protection to provide security. This means that somebody wishing to access secure data must provide the correct password before access is granted. Passwords are efficiently the keys to the safe.

A second aspect of security in computer network is relevent when secure data has to be transfered accross the network. In many cases, it may be impossible to guarantee that it is not possible for someone to gain access to one of the communication links and monitor the data flowing on the link. In such cases, it may well be up to applications using the network to take measure to ensure that no such attempts will result in useful information being obtained and that any attempts to alter the data in transit can be detected and rejected.

Data in transit in computer networks may be made secure by using 'data encryption'. This means that the data is first specially encoded in such a way that only the intended receiver is able to reconstruct the information. Any unauthorized intruder would not be able to deduce anything from the encrypted data.

8.1 CONTROLLING ACCESS

A threat to access control is when an intruder searches the memory of a computer or its filestore looking for useful information. Often in computer networks, the computer's memory may not be cleared between running tasks for different users. If the intruder is lucky, the previous task that used the memory now occupied by his task left some important information lying around in memory. This is a classic way of locating other users passwords and, in extremely unfortunate cases, large chunks of the file containing all of the valid passwords for the host computer may be able to access all of the data stored within the computer.

8.1.1 USER NUMBERING AND PASSWORD

The most basic form of access control that the host computer system can have is the 'user number and password 'system. A user calling into the computer is first asked for a user number and then the password associated with user number. The user number may be public knowledge. The host computer checks the user number / password combination against a file of valid user number/password pairs.

If the combination is found within the 'validation file',the user is granted access to the system. The host computer may still restrict the priviledges that the user has within the system. The validation file may also contain a list of previledges associated with the user number that the user cannot change.

Although this type of system is for preventing unathorised access when the consequenses of a security breach are not particularly serious, there are a number of problems with this system. Firstly, the validation file of user number/password combinations is liable to attack by intruders. In many cases it is not acceptable for even the system managers to be able to access this file in order to read its contents.

The validation file can be protected against attack by use of a 'one way cipher'. This means that when the validation file is created, the entries are not stored as the user number/password combinations themselves but as an 'encryted' version. The fact that the cipler used to produce the encrypted form is one way means that it is imposible to reproduce the original text from encrypted form in the file When the user supplies a number/password the combination is first encrypted using the same one-way cipher that was used to generate the validation file originally. If the encryted form is found within the file, the user is granted access to the system.

This methods of encrypting the validation file avoids the problem of unathorised access to its contents as the contents are meaningless. One unfortunate side effect of this is that if a user forgets a password, there is no way of finding out what the password was. The only thing to do is to create an entry for a new user number/password combination.

There are three well known technigues for obtaining user number and passwords. One technique is to monitor the network links or other parts of the communication network. Eventnally, user number and passwords will be seen and can be recorded for future use by an intruder. Actually, Ethernet networks are particularly vulnerable to this kind of attack because any node on the network can monitor every data packet on the Ethernet cable. Since most PCS and workstations can easily be fitted with an Ethernet interface and run software that monitors the data on the network, a program could be written to check for user number and passwords and store them in a file for later collection by the intruder.

The second methods of obtaining user number and passwords is to write a program that may massguerades as the genue login sequence. All that program actually does is to collect user number and passwords; for later collection by the intruder. When the user log-in, the fake log-in program says something like 'system down until futher notice!. The third method is to search distributions in areas where there are hard copy terminals. Very often, users enter their user number and passwords combination in such a way that it can easily be read.

8.1.2 QUESTIONNAIRES

Another method of identity verification makes use of information known to the authorised user but unlikely to be known to others. On first introduction to the system the user is asked a series of questions relating to such apparently irrelevent things as name of schools headmaster, colour of grandmother's syes, name of favourite author or football team, e.t.c rather than to the more usual component of cirriculum vitae, place and date of birth, maiden name of wife e.t.c. The selected items are such that the user is likely to find them easy to remenber, but an intruder is likely to find them difficult to discover. On later visit to the system for access, the user is asked a selection of questions to which the system has stored the answers. Correct replies allows the desired access. Greater security can be obtained if during access session, the system asks further questions from time to time; this would detect a session, take over in some way by an intruder.

8.2 DATA SECURITY

The weakest link in the system is the communication network itself. The network may cover a large geographical area and use public communications services. This generally means that the physical security may well be impossible. There are many situations however, where data must be transfered with high security.There are two separate requirements for data security. The first security where the actual information itself must be kept secret. Even if the intruder is able to gain access to information on the network, it must not be form that is useful. The second is for data anthencity. Hence the object is to ensure only those authorised can send specific data specific data across a network, usually with the aim of modifing the data base information.

One technique that an intruder can use is 'passive wire tapping' in this case, the intruder moitors the information flowing on a communication link. The aim is to extract useful information from either the information itself or statistics about the information. The technique is also known as eaves dropping. It can be protected against by encrypting the information before transfering it across the network.

8.3 CRYRTOGRAPTHC TECHNIQUES

A cipher is the method used to encode the data in a secret' form. The process of encoding the data with a particular cipher is known as encrypton. The reverse process of extracting the original information from the encrypted data is known as decryption. The original information is knwon as 'plain text' while the encrypted form of the plaintext is known as ciphertext.

Figure 8.1 shows how the information flows in a communictaion system protected by crytographic techniques. The plaintext information for the transmitter flows to first onto the encryption device. This may be a separate hardware system, or else part of the software system with the computer system.

The encryption device employs some encryption alogorithm to the plaintext to generate the ciphertext. The Ek symbol indicates that E is encryption algorithm while k specifies the particular 'key' that is used to encrypt the information. The ciphertext is then transmitted across the communication networks to the information receiver. Before the information is passed through the decryption device. The

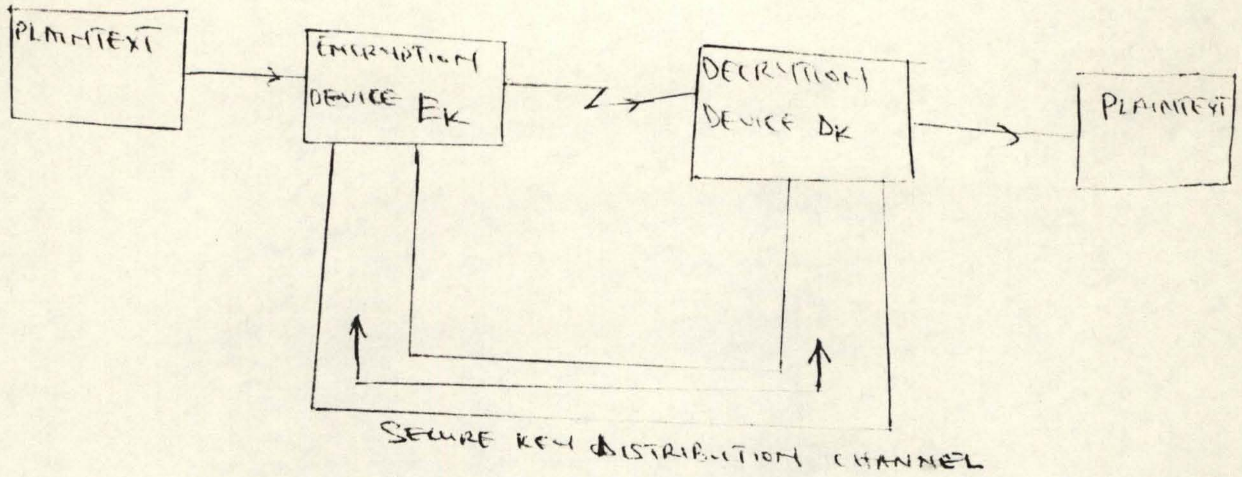


Figure 8.1 Information Flow

symbol Dk indicates that D is the decyption alogorithm while k specifies the key.

8.4 ENCRYTION ALGORITHMS

The purpose is to provide a very brief overview of some of the common algorithm used with cryptographic systems.

8.4.1 TRANSPORTATION CIPHERS

The concept in transportation ciphers is to rearrange the letters in an information message in such a way as to hide the information message. All the characters in the message remain the same; it is just that the ordering of the character is different.

8.4.2 SIMPLE SUBSTITUTION CIPHERS

The idea here is to replace each character in the set of characters used in the plaintext with another in the set of characters used in the ciphertext.

An example is shown below;

Plaintext; A B C D E F G H I J K L M N O P Q R S T U V
W X Y Z

CIPHERTEXT; Z Y X W V U T S R Q P O N M L K J I H G F E
D C B A

Using this simple substitution cipher, the message;

THEMANAGINGDIRECTORWILLBECOMMINGTOMORROM

becomes

GSVNZMZTRMTWRIVXGLIDROOYUXLUNRMTLNIILD

Which at first sight at least hide the information content pretty well.

CHAPTER 9

IMPLEMENTING ENTERPRISEWIDE NETWORKING

Careful planning management, and backup underpin the implementation of LAN to LAN corporate networking. Local area networks (LANs) are installed by many organisations to overcome particular business or communication problems. The result is that despite the fact that a substantial investment in LAN equipment has been made by companies, there is no overall control or management being exercised by either corporate data processing or telecom groups.

In addition, many organisation are looking to reap extra benefits from their existing LANs by interconnecting them to provide a company wide infrastructure that supports the widest possible connectivity between the attached devices for electronic mail, file transfer, data base sharing, and so on (see fig. 9.1). For smaller companies operating within a single site who do not have large data bandwidth requirments, the installations of simple bridges between the existing LANs is all that is required.

For larger organisations, however, who wish to connect together many LANs at numerous sites, this is not a task to be undertaken lightly. A problem on a departmental LAN might result only in a minor crisis where as a problem on large interconnected LAN network could prevent a company from

ENTERPRISEWIDE NETWORKING

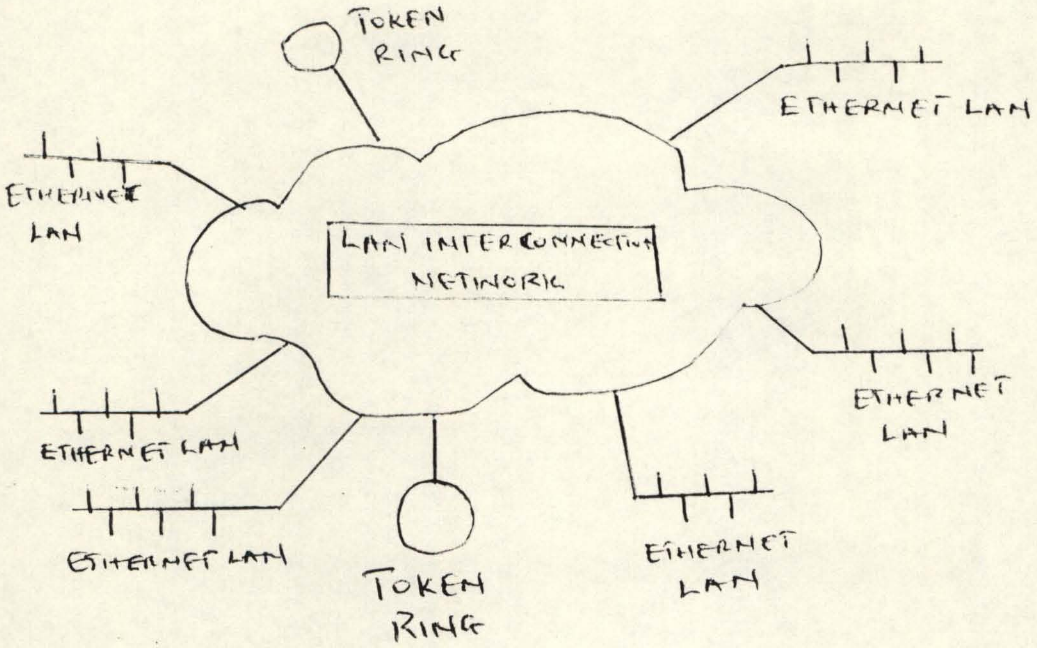


Figure 9·1 Interconnection of LANs to provide a companywide infrastructure.

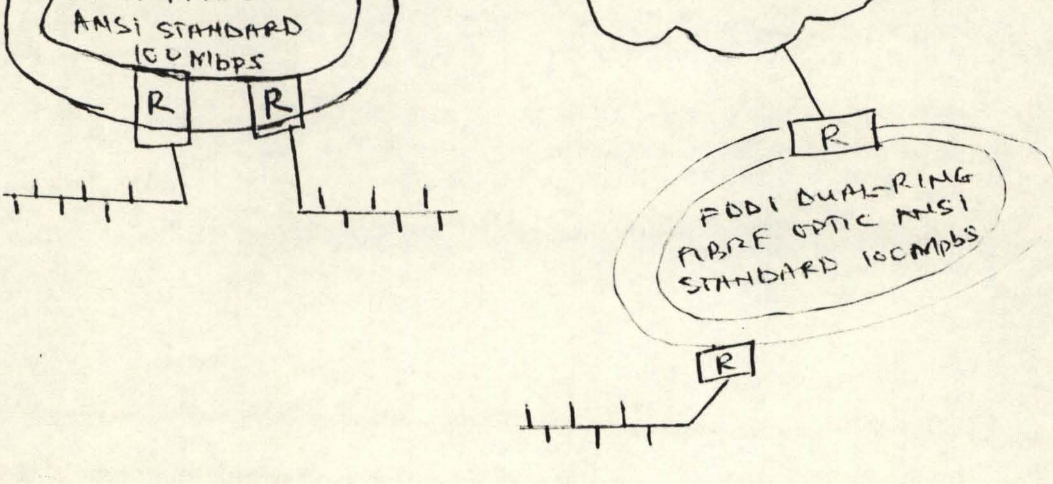

R
R
R
X·25
FDDI DUAL-RING FIBIRE OPTIC ANSI STANDARD 100 Mbps
R
R
R
R
FDDI DUAL-RING FIBRE OPTIC ANSI STANDARD 100Mbps
R

figure 9·2 Interconnecting sites with Routers and X·25 networks doing business. It is essential that a company develops a clear strategy for the planning and choose an experienced and reputable supplier as a partner to undertake the task.

9.1 "LOCAL" LAN

At the local level, existing LANs may be interconnected by local bridges or routers to provide inter-LAN connectivity. An alternative is to install an additional LAN to provide the backbone for the corporate network. This gives rise to a hierachical topology that is much easier to manage. An excellent medium for this backbone to allow growth and increase banwidth requirements is optical fibre. One standard is dominant for this application; Fibre Distributed Data Interface (FDDI).(see figure 8.2 and figure 8.3)

9.2 FDDI

This standard, which was first proposed by sperry and Burroughs (now unisys) to the ANSI standards commitee X3T95 in 1983, is now being implemented by most computer and LAN hardware suppliers as the next generated LAN technology. It provides an increase in performance over existing Ethernet and token Ring systems.

Based on a double fibre ring, FDD1 offers the resiliance of a backbone system. Operating at 100Mps, it provides some 80Mbps of bandwidth available for user data; at least twenty folds increase on the 3 - to 4 Mbps throughout typically

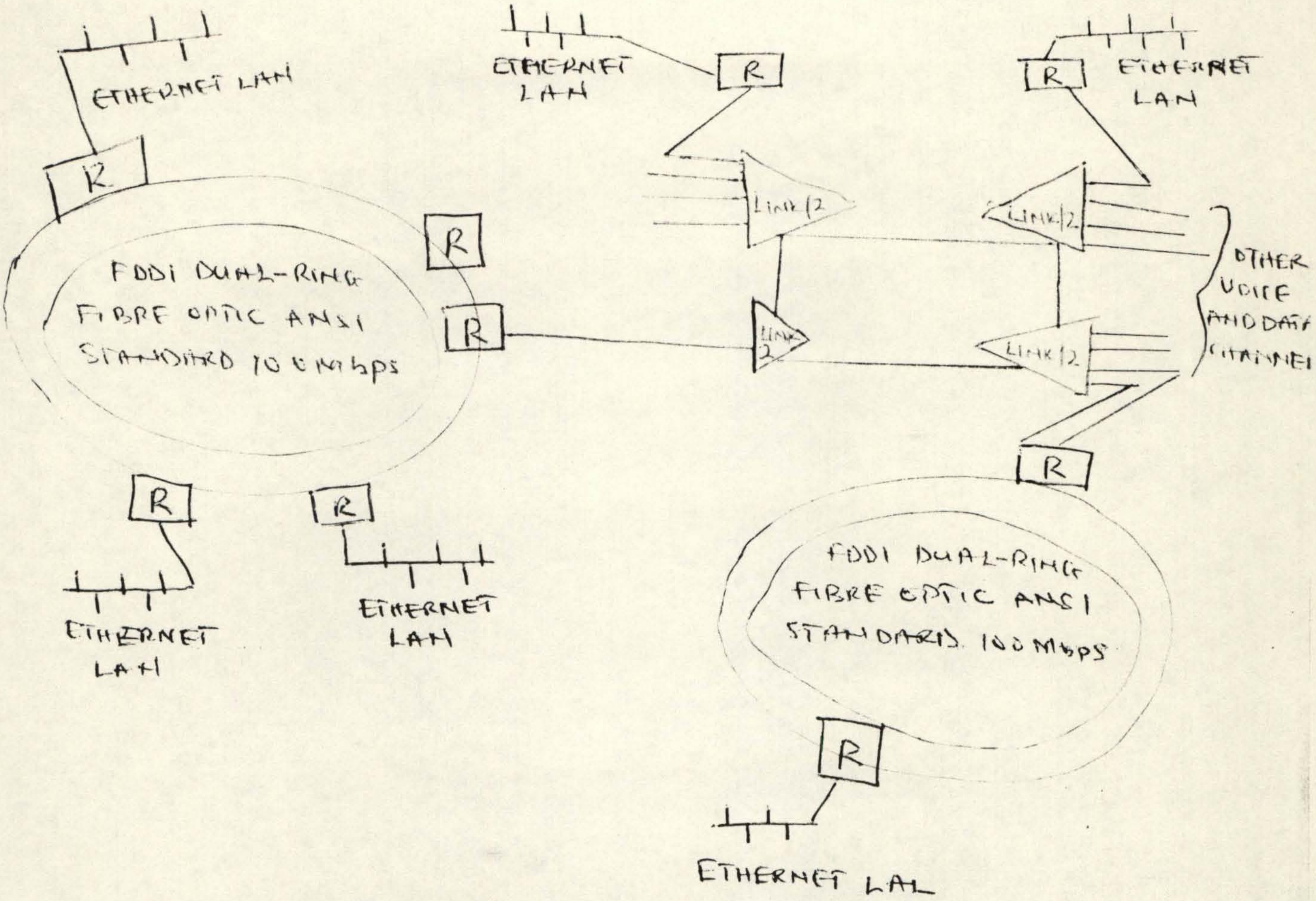


Figure 9·3 Interconnecting sites with routers and a LINK/2 network.

quoted for an Ethernet system. The LED light sources and fibre defined in the FDDI media specification allow for up to 2km between stations, while the overall specifications provides for up to 500 dual - attached stations on the main ring. With this capacity, the backbone can be installed on the largest of sites.

9.3 IMPROVED RESILIENCE

FDD1 netwrok resilience and manageability can be improved by an additional device called a concentrator, which provides the capability to connect workstations directly to the 100Mps FDD1 using only a single attachment connection, and is much cheaper than the dual attachment requried to provide the resilience on the main ring.

9.4 AN OPEN SOLUTION

To provide a truly open solution, the network protocol should conform to the ISO/OSI model and standards. The upper layer protocols of which are still being developed. The non-OSI protocls is to use TCP/IP until the ISO standards mature to the point where they are more widely implemented. An internetwork based on TCP/IP routers can be used to link LANs not only locally to a FDD1 backbone, but also remotely, using leased lines or existing X.25 or other data networks.

9.5 BANDWIDTH DEMAND

Where LANs are distributed over many remote sites. It is important to get some assessment of the bandwidth required to handle the intersite traffic. The demand for bandwidth in LAN environments is increasing. For example, with the advent of windows 3.0, average pc users will perhaps be utilizing 4 - Mbyte 386- based opposed to the 640k Dos of a few years ago.

In a LAN envirnment, where diskless workstations are becoming popular and a central file service provides secunty of all data with the entire system controlled by a MIS department, the file server and the network can present a bottlneck in terms of file transfer. RAM disks on a local workstations can be very effective in increassing the performance of program in this environment, although the initial upload of the program module or data file is still limited by the bandwidth.

9.6 CABLELESS LANS: THE NETWORK OF THE FUTURE

Network users can eliminate the time and expense requried to install conventional cabled LANs by choosing systems that utilize infared light or the radio spectrum to transmit data. Cableless local area networks open a world of new possibilities for network managers. They greatly ease the work required to install a network, particularly in order buildings that were not built with cabling needs in mind.

These systems also enable users to move or reconfigure their networks, a critical advantage considering that in many applications, networks must accommdate freguent major reconfigurations.
The advantages of rapid, indexpensive LAN installations are obvious when compared to the work reqaired to install traditional cabled networks. Most firms utilize outside contractors to install or route their network cabling. This is time consuming, frustrating process that entails providing precise specifications, selecting a reliable contractors, managing the project, and waiting for a convinient time usually night or weekends during which to install the cabiling.

As a result, conventional cable networks typically consume 30 to 90 days from initial planning to actual installation or longer in difficult applications. Cableess networks can be installed in on matter of hours, often by users themselves.

In addition, approximately 30 percent of LAN networks must be relocated or rearranged annually. Conventinal cables routed through ceilling, floors, and walls are usually abadoned each time. Cablesless system can be moved as needed, providing many years of additional services and significantly reducing overall costs of operation. Three different cableless technologies are currently available for

LAN environments: Intrared light, speed spectrum radio, and microwave radio.

9.6.1 INFRARED LAN NETWORKS

Infraced light can be used as a data transmission medium. Infared transmission method uses a technique that has been called directed point-to-point technology, in which the infrared light is focused into a narrow beam. This delivers the highest amount of infrared power to the receiving devices. Coverage within a building can be precisely defined by users, and the propagation of infrared light signals is a well-understood technology. High data transmission rates with low error rates are possible.

In January 1991,the industry's first token Ring - compatible LAN system based on infrared light was introduced. It achieves data transimssion rates of 4mb over distances of up to 80 feet.

9.6.2 SPREAD EPECTRUM RADIO LANS

Spread spectrum radio is a technique where by data signals are transmitted as RF energy confined to spectrum of frequacies. Curent spectrum technology operates at speeds up to 2Mbps over frequencies between 902 and 928 MHZ.

9.6.3 RF MICROWAVE LANS

Oue vendor, Motorola, has recently announced cabless LAN product that operates in the radio (microwave) frequency range. The wider bandwidth avalable in this spectrum makes higher data transmission rates possible.

CHAPETR 10

IMPLICATIONS OF COMPUTER NETWORKING IN AN ORGANIZATION
(A CASE OF STUDY OF NATIONAL OIL AND MARKETING PLC)

Computer are being distributed for use by funetional business units and departments. Concurrent with that trend is a signitreant decentralization of many data processing functions which, until recently, were within the domain of the management information systems department.

To examine the implictions of computer networking in an organization, a case study of National OIL and Marketing Company PLC will be used. Personal visits and interviews were conducted during the course of this project.

10.1 A BRIEF HISTORY OF THE COMPANY

The company markets refined products and other by products of petroleum. The company has installations at Apapa, Benin, Kano, Porthcurcourt, Oregun, and their market layout spreads over the country. The company started bussiness as far back as 1927, importing kerosene in drums just for lighting purpose.

In 1938, if feamed up with mobil to form a company called OIL storage company, Apapa,(OSCA) both of them hadfairly large drums stroage installation around Apapa, but were marketing products in drums. But this time it wasn't only kerosine it included some quantity of petrol and lubericant; because at that time in Nigeria some vehicles had been introduced by the colonial administrations. The products were marketed through some commercial houses, namely UAC used by mobil and GBO used by shell.

In 1952 the two company splited and went its own way. The office at 38/39 Marina is the head office, but the heart of the company is at Apapa because it harbours the main ware house, the formulations plants. In 1957 the company started chemical products marketing, mainly insectiside for the cocoa plantations in west Africa.

In 1989 government decided to sell off 20 of its 60% and the company went public,and of course about a year ago an ordinary resolution was passed at the annual general meeting to change the name of the company from National OIL and Chemical Marketing Company LTD to National OIL and Chemical Marketing PLC.

10.2 MANAGEMENT INFORMATION AND COMPUTING DEPARTMENT (MIC)

The company established their data processing department in 1970 as computer department but in 1989, the name of the department was changed to Management Information and Computing (MIC).

Every organisation requires the making of decisions, the coordinating of activities, the handing of people, and the evacuation of performante directed toward group objectives.

evacuation of performante directed toward group objectives. In the early stages of the development of computer hardware in the 1950's the technology improved so repidly that management had difficulty in appreciating the capabilities of computer Electronic data processing, with its emphasis or entry, processing, and output of data, quickly enable managers to handle such routine activities as processing payrolls and accounts receivables of the company.

Data processing has provided volumes printouts of internal data, such as account and financial data, production shedules inventions of raw materials, work in process and finished goods, sales by teritory, products and customers.

A significant number of the functional responsibilities traditionally performed by the MIC department will be shifting to the user. The current MIC responsibilities are shown in the typical contralised MIC organization chart in figure 10.1

In this chart, at present the MIC manager normally has five major line functions reporting to him these major line function are information, system development, technical support, quality control and operations.

System development section is usually responsible for the design, programming, maintenance of applications systems. The operations organisation is also usually divided into three functional activities, data entry, schedulling and

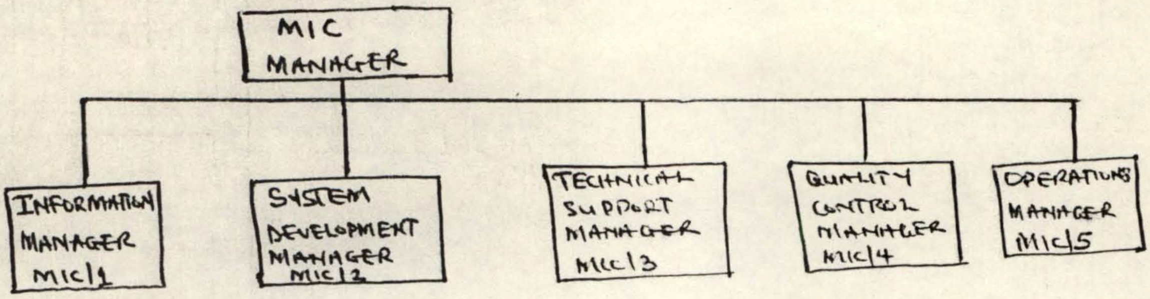

MIC MANAGER
INFORMATION MANAGER MIC/1
SYSTEM DEVELOPMENT MANAGER MIC/2
TECHNICAL SUPPORT MANAGER MIC/3
QUALITY CONTROL MANAGER MIC/4
OPERATIONS MANAGER MIC/5

Figure 10·1 : Typical MIC Organisation Before Implementation of Computer Networks.

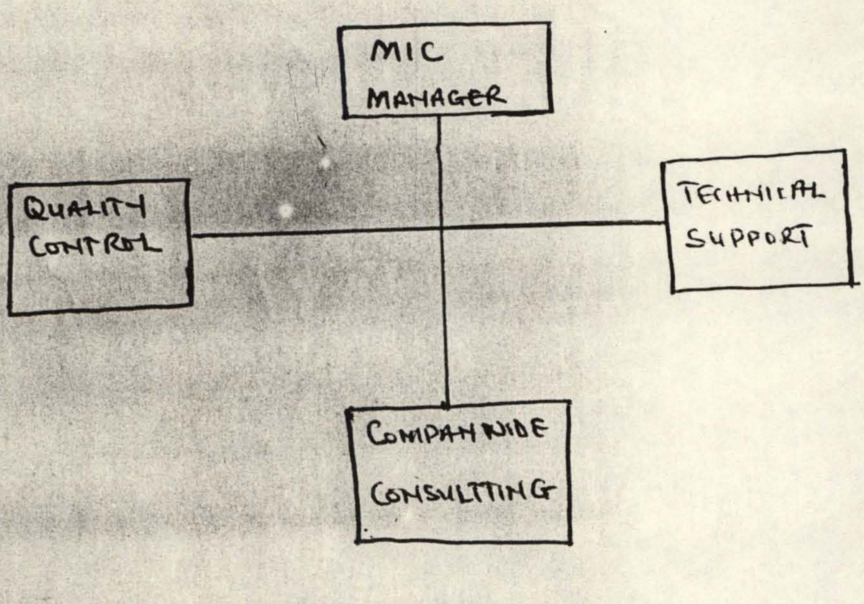


Figure 10·2 : Typical MIC Organisation After Implementation of Computer Networks.

unput/output contro, and computer operations, whiel run actual production work.

Technical support usually consists of highly skilled technicians required to maintain the operating system software. They also provide technical advisory services to MIC in such areas as data base and data communications control software and new computer equipment acqusition.

The quality control function establishes and monitors system standards including system justification procedures, project management techniquies, and system and acceptence testing mechanisms.

Although the structure of a particular MIC organisation may differ somewhat from the one described here, the functions, though not distinct, will still be present.

10.3 THE ORGANIZATION IMPACT OF COMPUTER NETWORKING ON THE MIC FUNCTION

Given the structure described above, significant changes are likely to occur within the next 3 to 5 years. These changes in each of the functions described next will be proportional to the growth in use of network.

10.3.1 MIC MANAGER

The department will become smaller in number of systems development and operations personal. Many of the development personel will migrate to the user areas.

The function will become more oriented toward controlling and coordinating overall system activities while providing a strong quality control capability with emphasis on total system planning.

The MIC manager's role will change from being a line management executive in change of a large number of people, to one that is analogous to that of a corporate controller.

The job qualifications will change. The MIC manager will be more oriented toward managing a matrix organisation of staff-oriented experts, rather than a line organisation. Also the MIC manager will be more innovative, less of a caretaker and more planning oriented. He will also be more a member of the company's general management.

10.3.2 OPERATIONS

The data entry function, as part of the data processing function will disappear and, with it, the keypunch operator. Almost all the data will be entered by the user through intelligent terminals.

The input and output control balancing function will be incorporated in computer programs. The internal auditors will assure management that the users are properly using the processing control features.

Operation of the remote computer will be a responsiblty of the user in accord with corporate-wide proceedures, so that data may be periodically accessed by the control computer

10.3.3 SYSTEM DEVELOPMENT

The systems analysts, currently responsible for designing systems, will either move into the user organisations, generally taking over line management responsities as well as participating in the development of computer applications, or will become staff consultants in the new MIC organization. Current programmers will become more technically proficent and join the technical support function or they will be attached to other organizatined units at lower pay seates.

The systems manager will become an architect who operates as an adjunt to the corporate planning group. It will be his function to determine the sets of information that operating management will have to access in order to implement and monitor the strategic plans of the management group.

10.3.4 TECHNICAL SUPPORT

The personnel will become more oriented toward mincomputer and microprocessor software support in addition to enlarging their knowledge of data base and data communication control software. Although the computer performs all the calculations for a given task, the software organises how the package which monitors the consistency of the organisation total data resource. Their technical advisory services will be provided primanlly to remote users rather than to MIC staff.

10.3.5 QUALITY CONTROL

This area of the MIC department will be the most rapially increassing in importance. In the past, there has been a tendency to use it as a testing ground for personnel whose career paths were cut off in other MIC functional areas. It should now become a high-profile position for the most qualified individuals who will review new systems development prject at designated checkpoints.

The personnel will become more directly responsible for administration and coordination in many areas including:

- data security and processsing controls
- decision to have one remote location develop an application for use by several locations, instead of duplicating development cost.
- interface synchronisation between linked application systems, e.g order-invoicing, sales and accounts receivable
- providing and monitoring documentation and testing

In sumary, it appears that the MIC function will become more of an in-house consulting group and less of a services bureau/software house as computer networking take hold, tending toward the organisation structure shown in figure 10.2

10.4 THE ORGANISATIONAL IMPACT ON THE USER

A significant number of data processing functions will be transfered to the user as computer networking come to function. The user will become responsible for the daily operation of the system, including data entry, input/output control, and schedulling of the equipment.

The most effect on user management in taking over system operations will be:

- User management will have to become more knowledgeable about computerized data processing and its economics
- Users will initially have more work to handle. This situation should be transistent. In almost all cases, direct on line data entry and information accessibility should eliminate redundant paper handling and manual proceedures to the point that a more productive, smaller work force results.

The other area of organisational impact on the user is related to systems development responsibilities. A new breed of user may be readily justified by the increase return on the system investment that will result from the user's being held responsible for the systems success.

10.5 STAFFING IMPLICATIONS

With the implementation of computer networking system, the power of the computer is brought directly to the system user. The result is that many long established system users must now think of a computer system as much more than the punched cards and printouts they once used. Now the computer system consists of CRT displays, keyboards, disks diskettes, modems, communication lines processing and printers. This change in concept provides a new challenge for the system user. The task of allevating the technological shock while simutaneously sustainning the current level of services is of paramont importance. Minnimizing the impact of this change can be accomplished through wise planning and strong user involvement from the inception in the system development cycle.

Traditionally, line management were only end-users of computer sytems, submitting input data to data processing and receiving from them printed output. The computer operations requried to process the data and produce the system output were centralized in the data processing department. With the introduction of computer networks, the traditional three functions of data entry, data control, and equipment operation are now extended to the user departments.

Now user line management must cope with data entry deadlines and schedules. Data control functions, such as batching and banlancing of input data, and reconcillation and distribution of system output, are now an essential part of the system user's daily business routine.

In addition to operation of the equipment, transmission of data to the host system, and recaption of data from the host system, the system user must be prepared to develop operating schedules for his own environment, furthermore he must participate in the development of the overall network operation schedules.

Data processing staff must relinquish the functions previously mentioned. However, as resident authorities on these functions they must impact expertise to the system users, prior to the implementation of the network system. The data processing staff must also develop the necessary network support tools to minimize user operational problems after network implementation.

10.6 USER STAFF SELECTION AND TRAINING

The most important person involved in the network is the network coordinator. The objective of the network coordination function is to ensure that effective day-to-day operation of the network is maintained while continuing to meet the organisational objectives in network processing.

10.6.1 NETWORK COORDINATOR FUNCTIONS

The major functions that must be performed by the network coordinator include the following:

- Management of systems and data processing staff supporting the operation of the network system.

- Support of system user staff in the field branch locations for day-to-day operations, and identification and resolution of problems.
- Coordination of data transmission and processing schedules in conjuction with the host system and field branch office staff.
- coordination of hardware and software maintenance

The position of network coordinator in the most vital factor determine the success of the network operation. The network coordinator must bring two basic sets of skills to the job. The first is an intimate understanding and knowledge of the organisations business process. This knowledge is mandatory to sustain an adequate communication with field branch office staff, and to provide a proper perspective on their operational problems. The second skill is a sound technical knowledge of computers and data communication to ensure an adequate level of service to the system users, to understand the ramifications of technical decisions, and to deal with the hardware vendor.

Finding a person who possesses these two sets skills is usually an awesome undertaking. Typically the person selected as Network coordinator brings to the position one set of skills only. The person rarely has a background in the business process and the technical aspects of data processing and data communications.

10.6.2 System Development Activities

The various activities undertaken by the system user committee during system development provide firsthand experience and training for them. Those activities for which the system user assumes primary responsibility are as follows.

- Development of user functional Requirements- These requirements describe how the system will become from an external point of view, i.e from the operations viewpoint. Users provide most input to this report, which is the first produced by there project team. The users should also be acquainted by the data processing concepts, and the data processing people with the aplication concepts. These requirements will outline sereen formats operator prompts, and alternate execution paths for each of the preceeding elements.

- Development of system introduction mannual, operational mannual, and training kit- the introduction mannual is used to introduce system users in general to the network system, and to assist the training team(s) in training the operators at each field location. The operation mannual documents the routine and non-routine operational procedures for use by field branch personnel. The system training includes a complete training program that uses the preceeding two mannuals as reference texts.

- Development of Acceptance Testing Proceedures- When data

- Development of Acceptance Testing Proceedures- When data processing personnel are writting the necessary computer programs, user project team members can begin the development of the acceptance testing procedures. In addition to the traditional application acceptance test where data are prepared in advance, processed through the system, and compared to expected known results, many other accptance tests must be planned and prepared. They include

  - Ease of operation and general system flow-tested through actual operation of the system by an operator.
  - Data communications-tested through live transimission and reception of data, and through simulated communication failures and errors such as breaking the data communication link during transmission.

10.6.3 Network Support Development Activities

During the development of the network , however, an addtional event, the establishement of the network support site must take place. The network support site is operated by the network coordinator and contains a computer terminal similar to every other site or node in the network. Its establishment involves consideration of not only the physical environment but also the necessary procedures for operational coordination and support of the distributed network. The network support site is best situated at the organisation's head office.

A dedicated HOT-LINE telephone is requried for exclusive use in providing operator problem assistance. for a nationally distributed network, this HOT-LINE must be manned during business hours at all network locations.

The network support procedure that must be developed include the following:

- Documentation Maintenance- These procedures address the chanelling of documentation changes through the network coordinator, the distribution of documentation dates, and the publication and distribution of a network newsletter.

- Equipment and Software Failure- These include procedures for recording equipment and software failures, classifying each failures, documenting a recovery technique, incorporating the technique into a standardized formal procedure, and distributing this procedure throughout the network.

- Software Maintenance and Testing- These are proceduring for initiating host application, terminal application, terminal system, or telecommunications software maintenance, for testing the changes and for distributing and implementing the maintenance changes.

Through an indepth involvement in the development of user requirements, user manuals and the training kit, and acceptance testing procedures; the establishment of the network support site; and the actual conducting of the acceptance tests, system users on the project team acquire the training necessary for implementation and operation of the network system.

10.7 THE CONVERSION AND IMPLEMENTATION PROCESS

Once training is completed, conversion and implementation can begin, Numerous activities must take place prior to the conversion and implementation. The first major activity is installation planning, which must take place well in advance of equipment installation.

Topics that must be considered during installation planning are listed below:

- check that adequate space exists for the equiment
- check that the electrical power requriments of the equipment can be met.
- check that humidity and temperature range at the site falls within acceptable limits for the equipment.
- Determine where the modem and dataphone, if requried, will be installed.
- check to see that a telephone is located near the equipment to permit voice communication while operating the equipment.

If a checklist and guidelines are developed, then installtion planning can be done by the system user. Furthermore, the resulting successor activities, such as ordering the modem, dataphone, and telephone, and supervising their installation, can also be adequately handled by the system user.

Once the system user has established operator identification codes, and access passwords, these can be passed to the data processing department for incorporation into both host and terminal software. The data processing department should also ensure that there is a sufficient number of telecommunications ports available at the host location, that the host system modem is installed, that the remote numbers are assigned, and that sufficient direct access storage space at the host system has been allocated. The data processing department is also responsible for the initialization of diskettes or disk cartridges and the copying of all system and applicatuion software needed for system operation onto the proper diskettes.

The trainer arrives at the site either the day of, or day after equipment installation, and performs various inspections and tests. After clearing up any outstanding items and fully checking out the equipment, the tranier begins the traning program.

Upon completion of the program, and after all files have been either converted or created by the data processing department, parallel or live operation is begun. When a smooth transition from the old system to the new system has occurred, the process begins again at another site.

10.8 OPERATIONAL SUPPORT

Once the network system is operational, the network coordinator and his staff manage the network with the aid of user documentation and the network support activities.

The most important tool is a message broadcast program that permits the composition of a message at the network support site terminal, and the transmission of that message to any or all remote locations in the network. The broadcastting of the message can be done on a point-to point basis with every remote location.

A second software tool is one that permits the distributions of software updates using the data comunication facilities. The alternative is the creation of software disk cartridge(s) or diskette(s) for every site, and distributing them by mail or courier service. This task is a risk because volume created on one terminal can be unreadable on another. The distribution of software updates can be done either through the host system or on a point-to point basis with each remote location. This eliminates repetive creations, and the problem of volume incompatibility between terminals because each terminal creates its own volume.

In the final analysis, the true value of these tools is realised when they are used to support a well- prepared and well - organised network coordinator and staff. The partnership between user and data processing, so necessary to the development of a successful system, must continue to ensure the successful operational of network.

CHAPTER II

CONCLUSION AND RECOMMENDATION

This project has presented an overview of the concepts involved in computer communication networks. The usability of many data processing application can offen be increased by placing the computer power at the location at which results are needed. Many remote computing options have become available because of advances in computer communication processing, which is blending of both the computer and the electronic components technologies.

With ultimately increased intelligence and ease of use, computer and communications will be better able to assist man. Applications of computer networks are virtually limitless. They cover widely differing areas, such as scientific research, banking, library services, medical services, weather forcasting, and e.t.c.

It is hope that this project will be very useful to the information scientist who wants to know how to put to work to his advantage the best that current technology can offer. In this era of a growing confluence of communications and computing, this project will be useful for computer scientists, programmers, engineers, and network designers as well as managers in order to understand the concepts used to design efficient and viable communication networks. It will also help in concise description of the various network components, strategies to put them together and approaches to analysis and improve network behaviours, and help to analyse the implications of an enterprisewide computer networks in an organisation.

REFRENCES

AHUJA , V. "Design and Analysis of Computer Communication Networks", McGraw Hill, 1987

ALAN , B. "New Information Technology ", Ellis Horwood, 1984

BARNETT , R. and MARYNARDSMITH ,S., "Packet Switched Networks: Theory And Practice", Johnwesley, 1988

CHORAFAS ,D., "Designing and Implimenting Local Area Networks", McGrawHill, 1984

DAVIES ,D.W and PRICE W.L, "Security For Computer Networks",Johnwesley, 1989

DEASINGTON ,R.J, "X.25 Explained: Protocol For Packet Switching Networks2nd ed; Ellis Horwood, 1989

HUTCHINSIN ,D. , "Local Area Network Achitectures", Addinsion Wesley 1989

RUSSELL , D. "The Principles of Computer Networking", Cambrdge University Press , 1989

SENN , J . A , "Analysis and Design of Infomation System-2nd ed" , McGrawHill , 1989